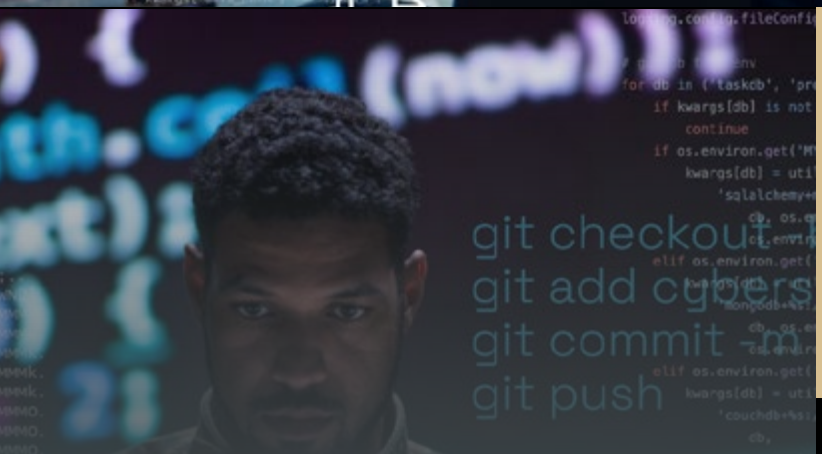
ÉDITION 2024

GUIDE MÉTIERS CYBERSÉCURITÉ

260 PAGES D'INFOS ET DE CONSEILS POUR TRAVAILLER DANS LA CYBERSÉCURITÉ

PAR GUARDIA CYBERSECURITY SCHOOL



65 FICHES MÉTIERS DE LA CYBERSÉCURITÉ

100+ TÉMOIGNAGES & CONSEILS DE PROFESSIONNEL·LE·S

TOUT SAVOIR SUR LES

- MISSIONS
- COMPÉTENCES
- FORMATIONS
- SALAIRES...

19,90 €

9 782958 497118

UN GUIDE ÉDITÉ PAR GUARDIA CYBERSECURITY SCHOOL

Première école d'informatique dédiée à la cybersécurité en France et accessible post-bac. L'objectif de Guardia Cybersecurity School est de former les futurs talents français experts de la sécurité numérique qui sauront protéger nos entreprises et institutions. Co-créé avec les entreprises du secteur, le programme pédagogique par projet est au plus proche des besoins du marché et des entreprises. Il est conçu pour former des techniciens opérationnels et agiles, capables de maîtriser les évolutions technologiques.

> www.guardia.school

Conception et Réalisation

Directeur de publication : Valérie Dmitrovic

Directeur de création : Jonathan Ruiz, Franck Weber

Chef de rédaction : Romain Charbonnier

Les Partenaires

Omen

Sogeti x Intel

Fulllife

Bollé

Maxnomic

ISBN 978-2-9584971-1-8

EDITO

Le secteur de la cybersécurité offre de belles perspectives d'avenir pour toute personne souhaitant travailler dans ce domaine et voulant s'investir dans des missions passionnantes, innovantes et à fort enjeux. Pour cela, **le besoin en formation est capital !**

Le dernier rapport de l'Agora du FIC (plus grand salon européen sur la cybersécurité) met en évidence l'importance de la formation pour **subvenir aux besoins de 500 000 créations de postes dans la cybersécurité.** Pour les experts, l'indépendance des Etats européens est liée à notre faculté à former les jeunes aux métiers de la cybersécurité.

L'industrie de la cybersécurité est de surcroît l'un des secteurs les plus innovants, la plupart des métiers étant à haute technicité.

Nous vous proposons dans ce **guide les fiches de 65 métiers** parmi les plus représentés dans l'industrie de la cybersécurité.

Pour chacune : une description du métier, les missions les plus fréquemment réalisées, une liste des compétences à maîtriser, ainsi que les qualités et les avantages de la profession.

Ces fiches ont été réalisées **en collaboration avec des professionnels** en exercice pour mieux comprendre et appréhender la réalité de leur quotidien.

VALÉRIE DMITROVIC
DIRECTRICE GÉNÉRALE DE GUARDIA CYBERSECURITY SCHOOL

SOMMAIRE

65 FICHES DES MÉTIERS DE LA CYBERSÉCURITÉ ET DES CONSEILS DE PROFESSIONNELS. DÉCOUVREZ POUR CHAQUE MÉTIER : MISSIONS, FORMATION, NIVEAU D'ÉTUDE, COMPÉTENCES, SALAIRES.

REMERCIEMENTS

CE GUIDE N'AURAIT JAMAIS PU VOIR LE JOUR SANS LES TÉMOIGNAGES ET LE DÉVOUEMENT DE CES NOMBREUX PROFESSIONNELLES ET PROFESSIONNELS DE LA CYBERSÉCURITÉ. EN NOUS RACONTANT LEUR QUOTIDIEN, LES RÉALITÉS, AVANTAGES ET INCONVÉNIENTS DE LEURS MÉTIERS, NOUS AVONS PU CRÉER 65 FICHES PRÉSENTANT 65 MÉTIERS DIFFÉRENTS DU SECTEUR DE LA CYBERSÉCURITÉ. C'EST EN ÉTANT AU PLUS PROCHES DES PROFESSIONNELS DU SECTEUR QUE GUARDIA CYBERSECURITY SCHOOL PEUT PROPOSER UN ENSEIGNEMENT AU PLUS PRÈS DE LA RÉALITÉ DE L'INDUSTRIE ET UN ACCOMPAGNEMENT POUSSÉ VERS LA PROFESSIONNALISATION DE SES ÉTUDIANTS ET DIPLÔMÉS.

ROMAIN CHARBONNIER

Journaliste

Expliquer, raconter, vulgariser, prendre de la hauteur sur des sujets économiques (tech, jeu vidéo, économie sociale et solidaire, environnement, vie des entreprises, sport, culture, tourisme, etc.) caractérise le travail de Romain Charbonnier.

Recherche de l'information, analyse, synthétisation, entretien sont ses méthodes de travail afin de fournir des contenus éditoriaux qualitatifs.

Journaliste Lyonnais depuis plus de 10 ans, Romain Charbonnier nous a été d'une grande aide pour la rédaction de ce guide des métiers de la cybersécurité. Il a su synthétiser les témoignages et interviews des professionnels interrogés pour aboutir aux 65 fiches du guide.

Son travail nous permet aujourd'hui de proposer un éventail complet du paysage professionnel de l'industrie de la cybersécurité à destination des futur·e·s étudiant·e·s et professionnel·le·s du secteur.

Redouane Khenache
Consultant Analyste SOC
SQUAD

Daniel Diaz
Analyste SOC
CYBERPROTECT

Guillaume Celosia
Head of OT/IoT Security
CMA CGM

Amandine Durand
Lean Compliance Designer
COMPLEYE.IO

Olivier Velin
Gestionnaire crise de cybersécurité
DEVOTEAM

Cyril Bras
RSSI
GRENOBLE-ALPES MÉTROPOLE

MERCI À EUX ET À TOUS CEUX QUI, DE PAR LA NATURE DE LEURS MÉTIERS, ONT TÉMOIGNÉ ANONYMEMENT.

04

ANALYSTE DE LA MENACE CYBERSÉCURITÉ

Niveau d'études : Bac+5

Spé Conseillée : Maths ou NSI

Employabilité : Bonne

Salaire débutant : 3 500 €

Code ROME : M1802 - Code FAP : M2Z

L'ANALYSTE DE LA MENACE CYBERSÉCURITÉ ASSURE LA SURVEILLANCE DES SI D'UNE ENTREPRISE OU D'UNE ADMINISTRATION. A LUI DE VEILLER À L'INTÉGRITÉ ET À LA CONFIDENTIALITÉ DES DONNÉES D'UNE ENTREPRISE.

Compétences

Travailler en tant qu'analyste demande de mettre en pratique une série de compétences acquises en formation puis au fil des expériences. Elles sont donc fondamentales.

· Bonne connaissance des enjeux et des métiers de l'organisation
· Capacité de compréhension des menaces cybersécurité
· Capacité à exploiter des sources ouvertes de manière sécurisée
· Mise en place de plans de veille sur un ou plusieurs secteurs déterminés
· Détection, qualification et analyse d'informations pertinentes
· Veille géopolitique et géostratégique
· Capacité de synthèse des éléments analysés
· Capacité à s'intégrer dans des réseaux pour pratiquer une veille technologique
· L'anglais

Salaire

En France, l'analyste de la menace cybersécurité touche en début de carrière en moyenne entre 3 200 et 3 500 euros brut mensuels.

Un analyste de la menace cybersécurité confirmé pourra gagner entre 4 000 et 5 000 euros brut annuels.

Aux États-Unis, un analyste de la menace en cybersécurité peut être rémunéré en moyenne 86 000 dollars annuels.

Missions

Ses missions sont d'une part, de détecter toutes les menaces et activités suspectes ou malveillantes sur les différents systèmes d'information, d'autre part, de faire de la prévention au sujet des cyberattaques et autres menaces potentielles sur le système d'information d'une entreprise.

L'analyste de la menace cybersécurité étudie l'évolution des motivations et des modes opératoires des attaquants afin de permettre à l'organisation d'ajuster sa stratégie de cybersécurité.

De plus, il assure la maintenance et la mise à jour des dispositifs de sécurité d'une organisation.

À un niveau plus opérationnel et technique, il fournit aux CERT/CSIRT et aux SOC (Security Operation Center) des renseignements fiables et contextualisés leur permettant d'adapter et d'améliorer leurs moyens de prévention, de détection et de réponse à incident.

Les missions de l'analyste cybersécurité se recoupent en quatre grandes activités, à savoir :

La collecte et l'analyse de données :

· Collecter, qualifier, organiser, recouper et analyser des données brutes issues de différentes sources (dark web, renseignements open source, média sociaux, CERT, etc.)
· Entretenir des échanges avec des réseaux d'homologues français et internationaux

Les activités de renseignement (threat intelligence) sur le contexte des menaces cybersécurité :

· Comprendre les enjeux et le contexte de la cybermenace, réaliser une veille sur les menaces émergentes
· Qualifier les menaces pouvant viser un type d'organisation, étudier le niveau d'exposition aux risques
· Apporter un support dans la compréhension des incidents rencontrés

L'amélioration des moyens de détection :

· Analyser les techniques d'attaques et les modes opératoires connus
· Améliorer les capacités de détection

La capitalisation et le partage :

· Rédiger les alertes et les rapports d'analyse permettant de mieux comprendre les menaces pesant sur l'environnement
· Produire des documents d'analyse permettant d'alimenter les outils de détection
· Mettre à jour des bases de connaissances
· Partager, lors d'un incident ou d'une crise de cybersécurité, l'état de la compréhension de la menace et les hypothèses probables concernant l'évolution de l'incident ou de la crise

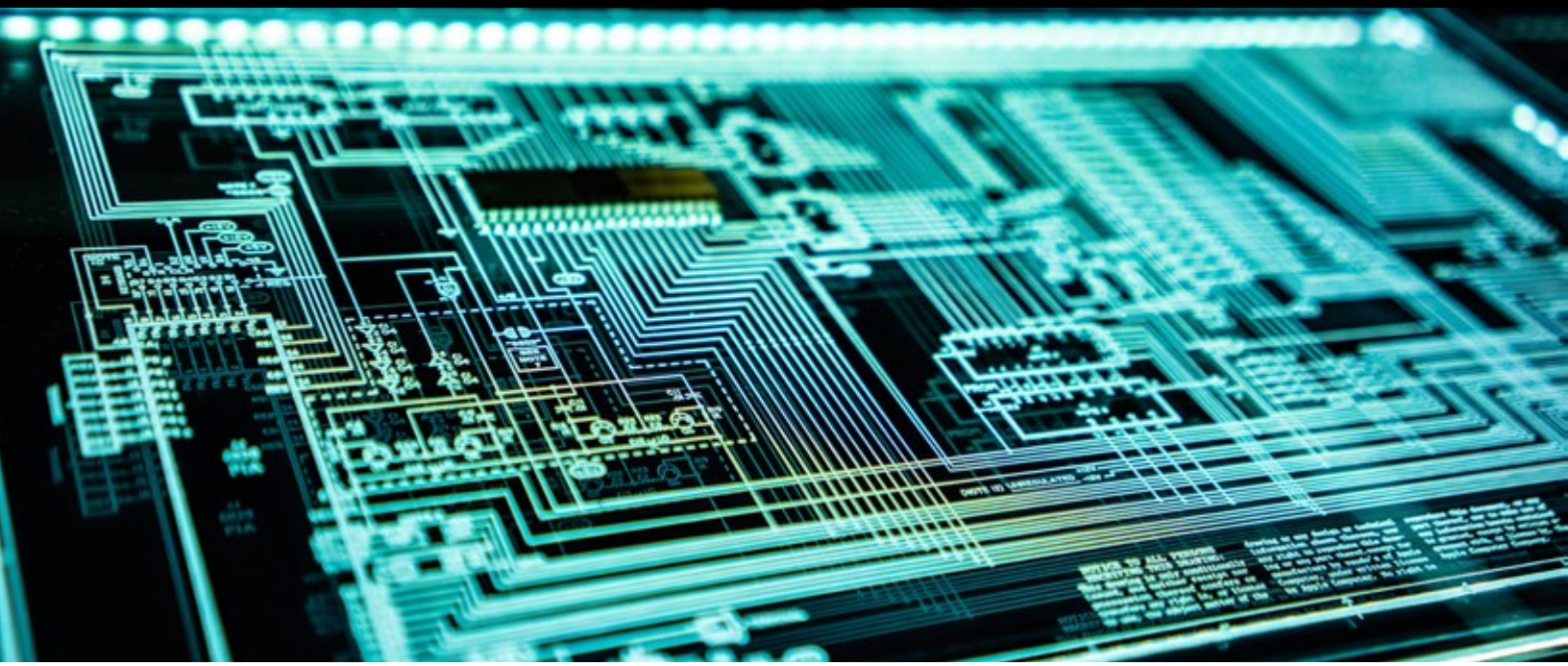
L'AVIS DU PROFESSIONNEL

« Avec l'évolution de la transformation numérique, l'intérêt de protéger l'information devient de plus en plus indispensable. Dans 5 ans, ce métier sera parmi les métiers les plus demandés mondialement. »

Redouane Khenache
Consultant Analyste SOC
SQUAD

QUALITÉS

· Rigueur
· Capacité à travailler en équipe
· Capacité à résister à la pression



Freelance

L'analyste de la menace cybersécurité peut exercer en tant que freelance. Après quelques années en poste pour acquérir de l'expérience, se lancer dans le grand bain de l'indépendance est tout à fait envisageable.

A savoir qu'exercer en freelance, c'est faire preuve de plus de rigueur, de professionnalisme et d'expertise qu'en étant salarié.

L'analyste de la menace cybersécurité peut également faire le choix de rejoindre un cabinet d'experts en cybersécurité qui le positionnera sur plusieurs missions.

Le tarif journalier moyen d'un analyste indépendant peut varier entre 400 et 600 euros.

Avantages et inconvénients

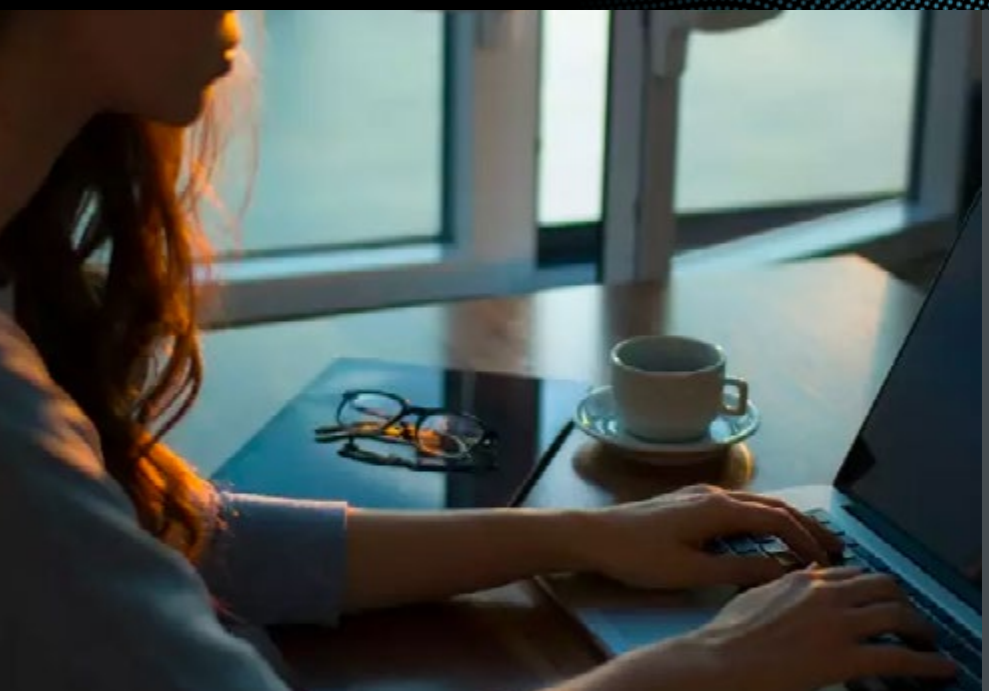
Choisir de faire sa carrière en tant qu'analyste cybersécurité, c'est avant tout s'engager dans un métier passion qui est en première ligne de la lutte pour la cyberdéfense. Un métier qui a le vent en poupe.

Du côté des inconvénients, le rythme des projets peut être très dense. Il est plus élevé sur la phase de test de la solution en amont mais reste soutenu dans la phase d'exploitation. Il peut être en forte hausse en période de nouvelle méthodologie d'intrusion et changement de technologie ou de produit.

« UN BON ANALYSTE SOC EST CELUI QUI CONNAÎT LE MAXIMUM DE FAILLES UTILISÉES ET LES PRATIQUES SUIVIES PAR LES HACKERS »

« Il faut être doté d'une grande capacité d'écoute et d'analyse pour comprendre le besoin client et y répondre. Il faut également faire preuve d'une bonne capacité d'adaptation à plusieurs aspects de la cybersécurité et à plusieurs technologies, afin de pouvoir maîtriser plusieurs sujets rapidement. »

Daniel Diaz
Analyste SOC
CYBERPROTECT



FORMATION

En intégrant le Master of Science, le métier d'analyste SOC n'aura plus de secret pour vous. Le cœur de la formation sera orienté vers les techniques d'attaques et sur les différentes méthodes à mettre en place pour protéger l'information et le système.

Au travers de projets liés à la recherche de failles, à l'analyse d'attaques ou à la mise à jour des moyens de détection, vous deviendrez un Guardian, élément indispensable à la sécurité de votre entreprise.

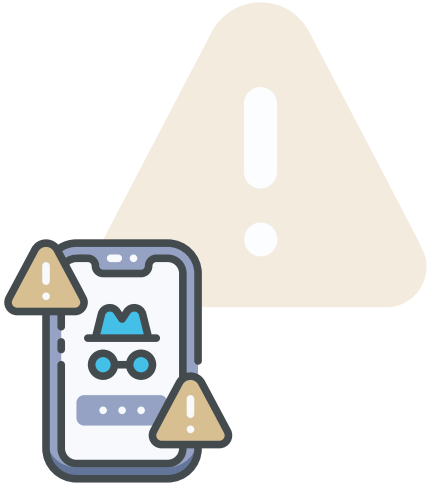
Évolution de carrière

L'analyste cybersécurité est le garant et le gardien de l'intégrité et de la confidentialité des données informatiques de l'entreprise. Aussi, les entreprises ont bien compris l'intérêt de se doter en interne d'un analyste de confiance, auquel on pourra confier davantage de responsabilités, qui pourront l'amener par exemple à évoluer vers un poste de responsable du SOC.

Où travailler ?

L'analyste de la menace cyber peut exercer dans divers types d'organisations. Dans les secteurs industriels, pour des sociétés de services ou dans le secteur public. Ou encore :

- Editeurs de logiciels et entreprises informatiques
- Secteur bancaire
- Secteur des télécommunications
- Sociétés de conseil en technologies



L'AVIS DU PROFESSIONNEL

« Le métier d'analyste SOC m'a immédiatement intéressé car il permet de voir tous les scénarios d'attaques possibles et les différentes méthodes pour protéger l'information et le système informatique en général.
Pour pouvoir bien mener les tâches d'un analyste SOC, le consultant doit avoir un bon esprit d'analyse et être méthodique. Mais la qualité la plus importante pour n'importe quelle mission, notamment en sécurité, c'est l'épistémophilie (NB = soif de comprendre, grande curiosité). »

Redouane Khenache
Consultant Analyste SOC
SQUAD

02

ANALYSTE DU SECURITY OPERATION CENTER

Niveau d'études : Bac+5

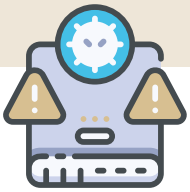
Spé Conseillée : Maths ou NSI

Employabilité : Très Bonne

Salaire débutant : 2 900 €

Code ROME : M1802 - Code FAP : M2Z

L'OPÉRATEUR ANALYSTE SOC A POUR MISSION LA SURVEILLANCE DU SYSTÈME D'INFORMATION D'UNE ENTREPRISE AU SENS LARGE AFIN DE DÉTECTER TOUTES LES ACTIVITÉS SUSPECTES OU MALVEILLANTES. IL INTERVIENT AUSSI EN AMONT POUR FAIRE DE LA PRÉVENTION.



Compétences

Pour exercer en qualité d'opérateur analyste SOC, il est indispensable de posséder un socle de compétences informatiques solides orientées cyber-sécurité. Il est également nécessaire de connaître le cadre réglementaire relatif à la sécurité informatique :

· Sécurité des systèmes d'exploitation
· Sécurité des réseaux et protocoles
· Et en matière de cyberdéfense : pratique de l'analyse de journaux (systèmes ou applicatifs), de flux réseaux, connaissance d'outils et de méthodes de corrélation de journaux d'événements (SIEM), des solutions de supervision sécurité, des techniques d'attaques et d'intrusions, des vulnérabilités des environnements
· Scripting

Salaire

A l'heure où le sujet de la cybersécurité touche toutes les sphères professionnelles, les entreprises sont de plus en plus nombreuses à se doter d'un SOC.

En France, l'opérateur analyste SOC en début de carrière touche en moyenne entre 2 600 et 3 200 euros brut mensuels.

Un opérateur analyste SOC expérimenté peut être rémunéré jusqu'à 48 000 euros brut annuels. À l'international, en Suisse par exemple, un opérateur analyste SOC peut gagner jusqu'à 100 000 CHF par an.

Missions

Les SOC sont composés d'analystes, d'ingénieurs en sécurité, ainsi que de managers supervisant les opérations de sécurité. Les équipes SOC travaillent étroitement avec les équipes d'intervention afin de s'assurer que le problème de sécurité soit bien réglé une fois qu'il a été découvert.

L'opérateur analyste SOC identifie, catégorise, analyse et qualifie les événements de sécurité en temps réel ou de manière asynchrone sur la base de rapports d'analyse sur les menaces. Il contribue au traitement des incidents de sécurité avérés en support des équipes de réponse aux incidents de sécurité.

Lorsque le système est compromis par une intrusion, l'analyste SOC évalue les dommages subis et apporte son aide pour concevoir une solution technique afin de rétablir le service en coordination avec d'autres acteurs de l'entreprise (administrateurs informatiques, computer emergency response team/CSIRT).

Il s'assure du maintien à jour des dispositifs de supervision de la sécurité comme le SIEM (Software Information Event Management), principal outil qui fait le lien en temps réel entre des événements et incidents pour en évaluer la dangerosité.

L'analyste SOC joue également un rôle en termes de prévention auprès des utilisateurs. Il veille au respect des bonnes pratiques et apporte ses conseils sur toutes les questions relatives à la sécurité.

Les missions quotidiennes de l'opérateur analyste SOC sont les suivantes.

Détection des menaces :

· Identifier, analyser, qualifier les événements de sécurité en temps réel
· Évaluer la gravité des incidents
· Notifier les incidents de sécurité

Réaction face aux menaces :

· Transmettre les plans d'action aux entités en charge du traitement et apporter un support
· Faire des recommandations sur les mesures immédiates
· Accompagner le traitement des incidents par les équipes d'investigation

Mise en place des usages et des outils :

· Contribuer à la mise en place du service de détection (SIEM, etc.)
· Contribuer à la définition de la stratégie de collecte des journaux d'évènements
· Participer au développement et au maintien des règles de corrélation.

Veille et amélioration :

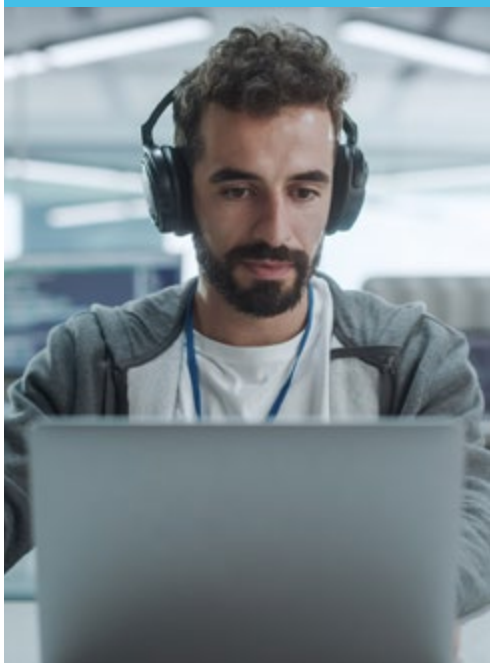
· Collaborer à l'amélioration continue des procédures ; construire les procédures pour les nouveaux types d'incidents
· Contribuer à la veille permanente sur les menaces, les vulnérabilités et les méthodes d'attaques afin d'enrichir les règles de corrélation d'événements

Reporting et documentation :

· Renseigner les tableaux de bord rendant compte de l'activité opérationnelle
· Maintenir à jour la documentation
· Recherche de compromissions (threat hunting)

QUALITÉS

· Capacité à travailler en équipe
· Capacité à définir des procédures
· Autonomie et organisation
· Capacité d'analyse et de synthèse
· Rigueur, sens de la méthode
· Qualité rédactionnelle
· Communication et expression orale



C'est quoi un SOC ?

Le SOC, pour Security Operation Center, désigne dans une entreprise l'équipe chargée d'assurer la sécurité de l'information. Le SOC est une plateforme qui permet de superviser et d'administrer la sécurité du système d'information au travers d'outils de collecte, de corrélation d'événements et d'intervention à distance.

L'objectif d'un SOC est de détecter, analyser et remédier aux incidents de cybersécurité à l'aide de solutions technologiques et d'un ensemble de procédés et de démarches de sécurisation du système informatique dans son ensemble.

Le SOC veille à ce que les failles et incidents de sécurité soient identifiés, analysés, compris et contrôlés. Concrètement, les SOC surveillent et analysent l'activité sur les réseaux, les serveurs, les terminaux, les bases de données, les applications, les sites Web et autres systèmes, à la recherche de comportements anormaux qui pourraient être le signe précurseur d'un incident ou d'un compromis en matière de sécurité .

L'organisation du SOC :

Elle doit permettre de répondre à différentes missions. Le SOC s'organise donc en 3 couches distinctes :

Le niveau 1 (opérateurs) relève les alertes et fait un premier diagnostic. C'est ici que l'opérateur analyste SOC intervient.

Le niveau 2 (analyste sécurité) réalise l'analyse détaillée des alertes, communique vers les équipes concernées, accompagne le traitement des incidents et, dans quelques cas, peut mettre en place des remédiations.

Le niveau 3 (experts sécurité) prend la relève du niveau 2 pour les analyses approfondies ou nécessitant une compétence pointue. En s'appuyant sur l'analyse de risques, le responsable du SOC va proposer et implémenter des uses-cases en s'appuyant notamment sur un catalogue de use-cases couvrant de nombreuses menaces. Si le use-case n'est pas déjà présent dans le catalogue, il est chargé de le développer pour répondre au besoin spécifique.

Constituer un SOC présente l'avantage pour l'entreprise d'assurer la surveillance continue de ses systèmes et données et ainsi de pouvoir rester au fait des menaces qui pèsent sur son environnement.

L'outils de l'analyste SOC : le SIEM

L'Agence Nationale de la Sécurité des Systèmes d'Information ou ANSSI recommande le recours à un SOC (Security Operating Center) dans le cadre d'une politique de sécurité renforcée. Un SOC s'appuie sur les technologies SIEM (Security Information and Event Management) afin de gérer les évènements du système d'information.

Le SIEM est une technologie spécifique qui permet d'analyser les menaces. Concrètement, le SIEM permet à une entreprise de centraliser toutes les informations de sécurité en un seul outil. Les données collectées auprès des logiciels antivirus, des pare-feux, des serveurs, des protections anti-theft ou encore des systèmes d'exploitation en tout genre seront analysées dans un même outil, ne laissant place au hasard. Une telle technologie permet aux équipes de cybersécurité de surveiller et de traiter plus facilement en temps réel les problèmes concernant l'infrastructure IT. Les produits SIEM améliorent l'efficacité et la précision lors de la détection et de la réponse aux menaces. Sans solution SIEM, l'opérateur analyste SOC aura la tâche impossible de parcourir des millions de données cloisonnées et impossible à comparer.

Le choix de la solution SIEM au sein d'une organisation sera fonction des besoins de l'entreprise. Plusieurs aspects doivent être pris en compte au moment du choix de la technologie SIEM afin de se doter de l'outil le plus adapté pour sa propre structure.

L'opérateur analyste SOC et les équipes cybersécurité devront notamment hiérarchiser les sources de données et choisir un éditeur SIEM prenant en charge toutes les applications utilisées par l'entreprise.

Freelance

L'opérateur analyste SOC peut exercer en tant que freelance. La première option consiste à créer un statut d'auto-entrepreneur ou une société individuelle auprès de la Chambre de Commerce. Il sera ainsi possible de facturer ses prestations à tous types de clients. Il est également possible de rejoindre un cabinet d'experts en cybersécurité qui peut aider l'opérateur analyste SOC à se positionner sur plusieurs missions.

Le tarif journalier moyen d'un opérateur analyste SOC freelance peut varier entre 400 et 700 euros.

Évolution de carrière

La cybersécurité est devenue un élément stratégique pour toutes les organisations publiques et privées. Les entreprises sont de plus en plus nombreuses à se doter d'un dispositif de contrôle de la sécurité des données ou SOC.

L'opérateur analyste SOC sera amené à gérer de plus en plus d'incidents de sécurité et devra par conséquent développer une bonne compréhension des nouvelles menaces qui pèsent sur son périmètre. Pour suivre l'évolution des tendances, il pourra être amené à développer des compétences en machine learning et en threat intelligence afin de renforcer les capacités de détection.

Après plusieurs années d'exercice, l'opérateur analyste SOC pourra éventuellement évoluer vers un poste de responsable du SOC.

Comment le devenir ?

Pour devenir opérateur analyste SOC, il est nécessaire de préparer un diplôme de niveau Bac + 3 à 5 en informatique, avec une spécialité en sécurité des systèmes d'information. Le métier est accessible à partir d'une première expérience en ingénierie des réseaux et des systèmes.

A l'heure où le sujet de la cybersécurité touche toutes les sphères professionnelles, les entreprises sont de plus en plus nombreuses à se doter d'un SOC afin de pouvoir suivre et analyser en continu les risques et menaces potentiels de sécurité.

En France, l'opérateur analyste SOC en début de carrière touche en moyenne entre 2 600 et 3 200 euros brut mensuels. Un opérateur analyste SOC expérimenté peut être rémunéré jusqu'à 48 000 euros brut annuels.

Après plusieurs années d'exercice, l'opérateur analyste SOC pourra éventuellement évoluer vers un poste de responsable du SOC.

Où travailler ?

L'opérateur analyste SOC peut travailler dans les secteurs industriels, pour des sociétés de services ou encore dans le secteur public.

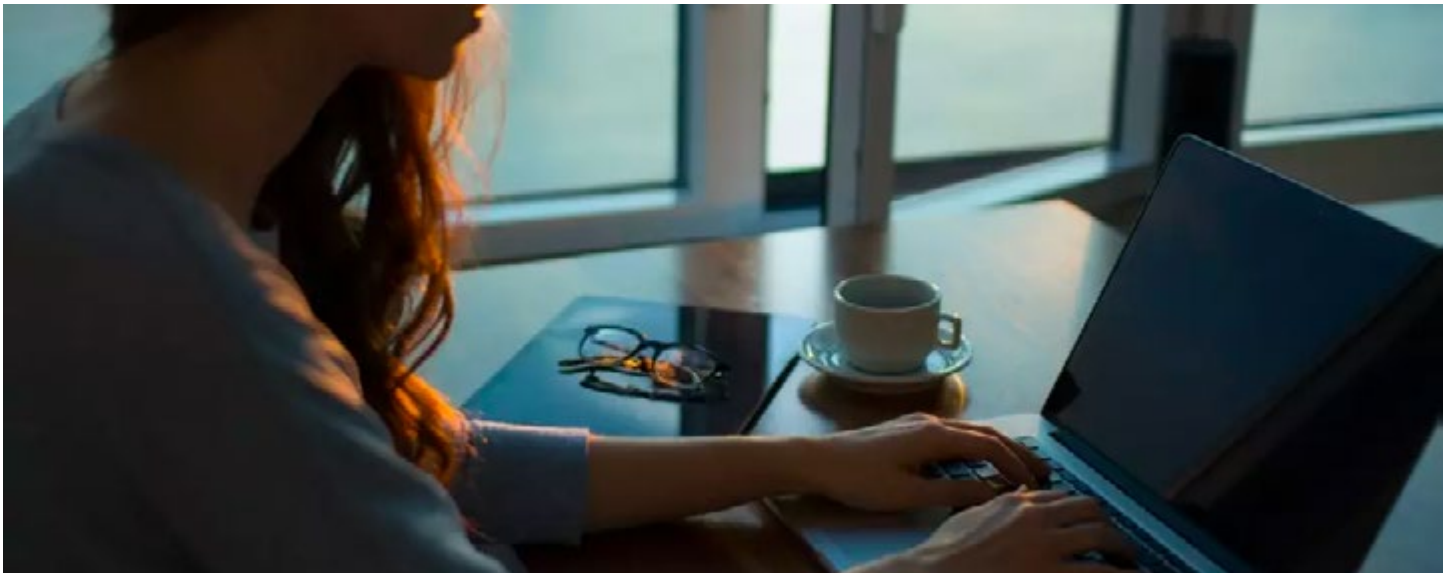
Voici un exemple d'entreprises et institutions qui font appel à des opérateurs analystes SOC :

· Editeurs de logiciels et entreprises informatiques
· Secteur bancaire
· Secteur des télécommunications
· Sociétés de conseil en Hautes Technologies

Avantages et inconvénients

Faire carrière en tant qu'opérateur analyste SOC, c'est choisir d'exercer un métier qui a du sens, puisque intégrer le SOC signifie être est au cœur de la stratégie de cyberdéfense de l'entreprise.

Du côté des inconvénients, il est possible de citer la pression liée aux responsabilités du métier. En effet, il est important de savoir garder son sang-froid car l'opérateur analyste SOC doit gérer et traiter des données extrêmement sensibles.



03

ANALYSTE DU CSIRT OU CERT

Niveau d'études : Bac+5

Spé Conseillée : Maths ou NSI

Employabilité : Bonne

Salaire débutant : 3 300 €

Code ROME : M1802 - Code FAP : M2Z

L'ANALYSE DES MENACES ET DES FAILLES DE SÉCURITÉ DEVIENT UNE PRÉROGATIVE POUR L'ENSEMBLE DES ENTREPRISES QUI SE VOIENT DANS L'OBLIGATION DE PROTÉGER LEURS DONNÉES ET LEUR PATRIMOINE NUMÉRIQUE FACE À DES ATTAQUES DE PLUS EN PLUS SOPHISTIQUÉES ET SOURNOISES.

Compétences

Devenir expert des réponses aux incidents de sécurité nécessite de posséder de solides compétences informatiques et des connaissances pointues en cybersécurité telles que :

· Maîtrise du système d'information, de l'urbanisation et de l'architecture du SI
· Analyse post-mortem (forensic) : connaissance des outils d'analyse et des procédures légales
· Cyberdéfense : pratique de l'analyse de flux réseaux, connaissance des techniques d'attaques et d'intrusions, des vulnérabilités
· Scripting

Études

Pour devenir expert réponse aux incidents de sécurité, vous devrez justifier d'un diplôme en informatique de niveau Bac +5 avec une spécialisation en cybersécurité.

Salaire

La rémunération d'un expert réponse aux incidents de sécurité varie selon le CSIRT au sein duquel il intervient.

Le salaire médian pour les experts réponse aux incidents de sécurité en France est de minimum 40 000 euros par an.

Un profil senior ou expert pourra prétendre à un salaire allant jusqu'à 75 000 euros annuels.

Missions

Dans un monde où les réseaux globaux prennent toujours plus d'expansion et une importance stratégique qui ne se dément pas, les systèmes d'information d'une organisation doivent pouvoir résister aux différentes menaces qui pèsent sur eux.

Pour sécuriser leurs systèmes et leurs réseaux, les organisations doivent pouvoir compter sur des gestionnaires capables de reconnaître les menaces et les vulnérabilités des systèmes existants.

C'est le propre de la mission de l'expert réponse aux incidents de sécurité.

Au quotidien, il met en œuvre des actions afin d'anticiper les incidents, les analyse, puis préconise des mesures d'amélioration visant à limiter les incidents futurs.

Voici en détail ses missions quotidiennes :

Anticipation des incidents :

· Réalise une veille sur les nouvelles vulnérabilités, technologies
· Alimente les bases de renseignement sur les menaces (threat intelligence)
· Maintiens et développe des outils d'investigation

Analyse des incidents :

· Collecte les informations techniques d'un large ensemble de systèmes d'information, réalise la recherche d'indicateurs de compromission
· Analyse les relevés techniques réalisés afin d'identifier le mode opératoire et l'objectif de l'attaquant et de qualifier l'étendue de la compromission
· Rédige des rapports d'investigation

Conseil :

· Préconise des mesures de contournement et de remédiation de l'incident (assainissement et durcissement)
· Préconise des mesures d'amélioration des capacités d'analyse (extraction des indicateurs de compromission)

Expérience

Il est entendu, compte-tenu de la nature sensible des missions inhérentes à son métier, que l'expert réponse aux incidents de sécurité occupera des responsabilités qui évolueront progressivement selon son niveau d'expérience et de maturité professionnelle.

Technicien I ou débutant :

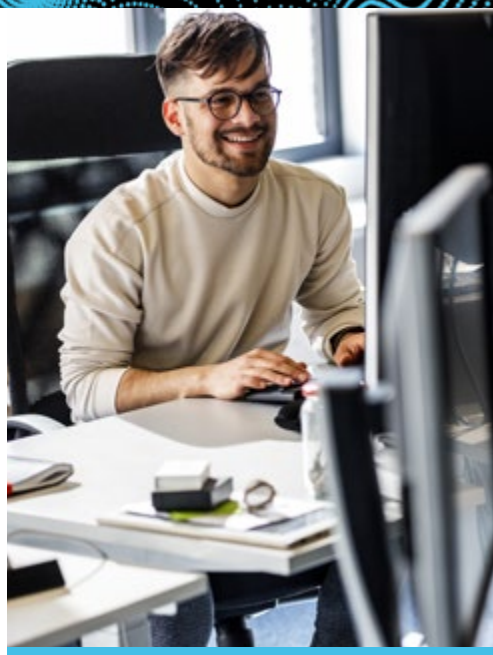
· Assume un rôle de soutien technique général en effectuant des activités, conformément aux procédures et politiques établies
· Assiste les techniciens plus expérimentés de son domaine d'activités
· Détient généralement 0 à 2 ans d'expérience pertinente

Technicien II ou intermédiaire :

· Assume un rôle de collaborateur dans la réalisation d'activités techniques et participe à la résolution de problèmes techniques
· Contribue au développement et à l'amélioration de méthodes et procédures de travail, peut contribuer au transfert des connaissances par l'encadrement et le coaching des employés moins expérimentés de son équipe
· Détient généralement 3 à 5 ans d'expérience pertinente

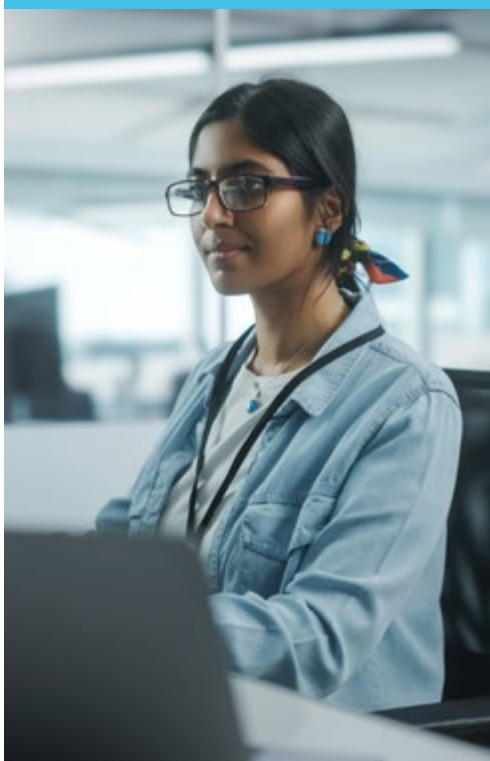
Technicien III ou titre principal :

· Assume un rôle d'expert technique et contribue à la résolution de problèmes techniquement complexes
· Influence les pratiques, méthodes de travail et procédures d'un point de vue technique et participe à leur développement afin d'en optimiser la qualité et l'efficacité
· Collabore avec différents intervenants internes et externes
· Contribue au transfert des connaissances par l'encadrement et le coaching des employés moins expérimentés de son équipe
· Détient généralement 6 à 9 ans d'expérience pertinente.



QUALITÉS

· Capacité de restitution et de vulgarisation pour des publics non techniques
· Rédaction de rapports adaptés à différents niveaux d'interlocuteurs
· Travail en équipe
· Capacité à résister à la pression
· Sens éthique



C'est quoi un CSIRT ou CERT ?

L'expert réponse aux incidents de sécurité intervient généralement au sein d'un CERT (Computer Emergency Response Team) ou CSIRT (Computer Security Incident Response Team).

L'équipe CSIRT ou CERT est une regroupement de personnel expérimenté, technique et non technique qui travaillent ensemble pour comprendre l'étendue de l'incident, comment il peut être atténué et, au final, comment y remédier.

Les tâches prioritaires d'un CSIRT ou CERT sont les suivantes :

· Centralisation des demandes d'assistance suite aux incidents de sécurité (attaques) sur les réseaux et les systèmes d'information : réception des demandes, analyse des symptômes et éventuelle corrélation des incidents
· Traitement des alertes et réaction aux attaques informatiques : analyse technique, échange d'informations avec d'autres CERT, contribution à des études techniques spécifiques
· Établissement et maintenance d'une base de données des vulnérabilités
· Prévention par diffusion d'informations sur les précautions à prendre pour minimiser les risques d'incident ou au pire leurs conséquences
· Coordination éventuelle avec les autres entités (hors du domaine d'action) : centres de compétence réseaux, opérateurs et fournisseurs d'accès à Internet, CERT nationaux et internationaux.

Où travailler ?

L'expert réponse aux incidents de sécurité peut intégrer l'un des CSIRT qui constituent ce réseau international, composé d'entreprises et d'institutions de tailles et profils très variés.

Voir la fiche métier « Gestionnaire crise cybersécurité » pour la liste des CSIRT/CERT en France.

Freelance

L'expert réponse aux incidents de sécurité peut exercer en tant que freelance indépendant. La première option consiste à créer un statut d'auto-entrepreneur ou une société individuelle auprès de la Chambre de Commerce. Il sera ainsi possible de facturer ses prestations à tout type de clients. Néanmoins, ce choix est encore plutôt rare, dans la mesure où l'expert réponse aux incidents est très souvent rattaché à un CSIRT pour exercer.

Avantages et inconvénients

L'expert réponse aux incidents de sécurité convoque quotidiennement l'ensemble de ses connaissances en cybersécurité (technique, veille, prospective) dans ses responsabilités. C'est donc un métier riche et complet .

Ce métier est à réserver aux profils qui ne craignent pas le stress et la pression car il faut savoir être réactif afin de pouvoir répondre au plus vite aux incidents de sécurité.

Comment le devenir ?

L'expert réponse aux incidents de sécurité analyse les activités malveillantes ou d'attaques au sein du système d'information de l'entreprise. Ce professionnel de la cyberdéfense est titulaire d'un diplôme d'informatique de niveau Bac +5 avec une spécialisation en cybersécurité et sécurité des réseaux informatiques. Le salaire médian d'un expert réponse aux incidents de sécurité en France est de minimum 40 000 euros par an. Ce métier est en plein développement au sein des organisations qui possèdent une structure de type CERT ou SOC.

04 ARCHITECTE CYBERSÉCURITÉ

Niveau d'études : Bac+5

Spé Conseillée : Maths ou NSI

Employabilité : Très Bonne

Salaire débutant : 5 000 €

Code ROME : M1802 - Code FAP : M2Z

L'ARCHITECTE CYBERSÉCURITÉ ANTICIPE, PRÉCONISE ET CONÇOIT LES ORIENTATIONS TECHNOLOGIQUES ET MÉTHODOLOGIQUES LIÉES À LA SÉCURISATION DES SYSTÈMES D'INFORMATION, AUTANT SUR LES PANS LOGICIELS QU'INFRASTRUCTURES.

Avantages et inconvénients

Faire sa carrière en tant qu'architecte cybersécurité est un métier valorisant pour qui souhaite être au cœur des enjeux techniques qui touchent à la cybersécurité. Cet expert de la sécurité informatique est en effet le chef d'orchestre du système d'information de l'entreprise. L'architecte cybersécurité est un ingénieur confirmé, mais aussi un manager et un gestionnaire.

La pression liée aux responsabilités du métier est l'un de ces inconvénients en revanche.

Salaire

En France, l'architecte cybersécurité en début de carrière touche en moyenne entre 40 000 et 60 000 euros brut annuels.

Expérimenté, il peut être rémunéré jusqu'à 80 000 euros brut annuels.

Aux Etats-Unis par exemple, un architecte cybersécurité peut gagner entre 92 000 et 222 000 dollars annuels.

Chaque rémunération va dépendre de l'entreprise-employeur, du niveau d'expérience recherché, et du lieu de travail.

Où travailler ?

L'architecte cybersécurité peut exercer dans les secteurs industriels, pour des sociétés de services ou encore dans les entreprises publiques.

Voici un exemple d'entreprises qui font appel à des architectes sécurité :

- Les éditeurs de logiciels et entreprises informatiques
- Les banques et les assurances
- Les entreprises de télécommunication
- Les sociétés de conseil en hautes technologies

Missions

L'architecte cybersécurité définit et structure les choix techniques en matière de sécurité des systèmes d'information en réponse aux besoins du client et veille à leurs applications. Il produit les livrables documentaires et les spécifications nécessaires.

Les missions de l'architecte cybersécurité sont déclinées en quatre grands sujets :

Préconisation

· Accompagner les chefs de projet dans le design de l'architecture, spécifier les différents paramétrages et définir les exigences techniques de sécurité pour intégrer de nouveaux systèmes ou faire évoluer des systèmes existants
· Conseiller sur le choix des solutions techniques et préconiser des architectures sécurisées pour un ou un ensemble de systèmes d'information s'assurer de sa conformité réglementaire le cas échéant
· Participer au choix des éditeurs et des fournisseurs de services SI sous l'angle sécurité
· Revoir régulièrement l'architecture existante, identifier les écarts et faire des recommandations d'amélioration de la sécurité
· Définir les stratégies de tests de validation sécurité et veiller au suivi des recommandations

Communication

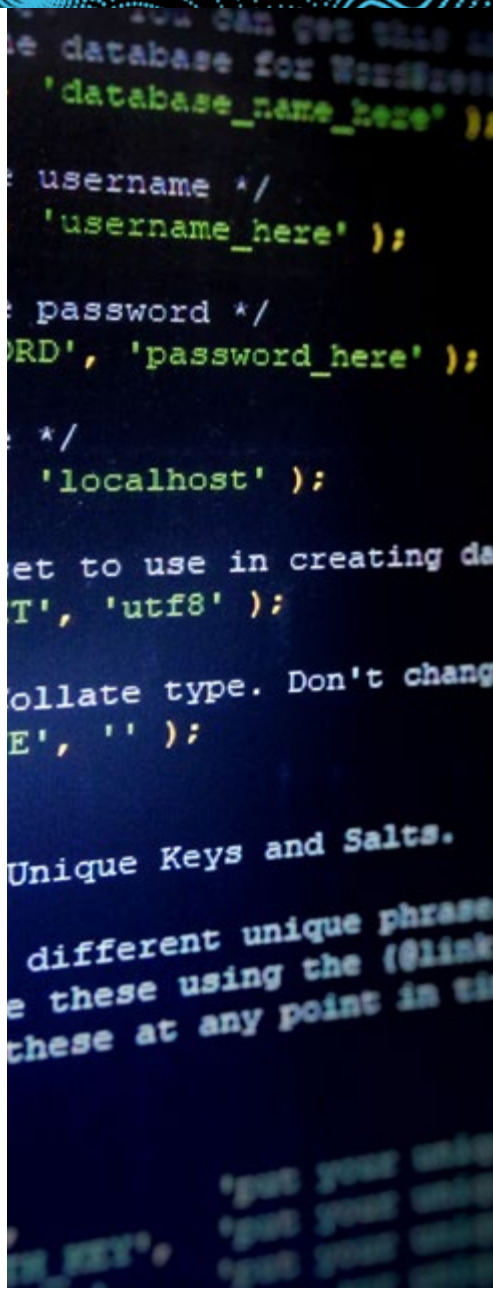
· Contribuer à la montée en maturité des architectes techniques et des urbanistes en matière de sécurité des SI
· Collaborer avec les spécialistes techniques de sécurité pour consolider une vue globale de la sécurité

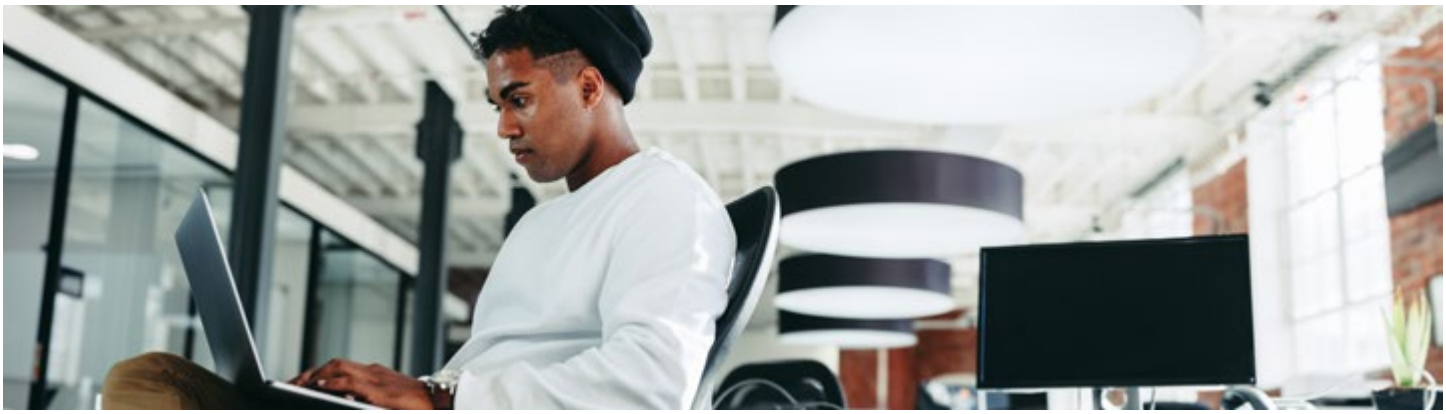
Conception

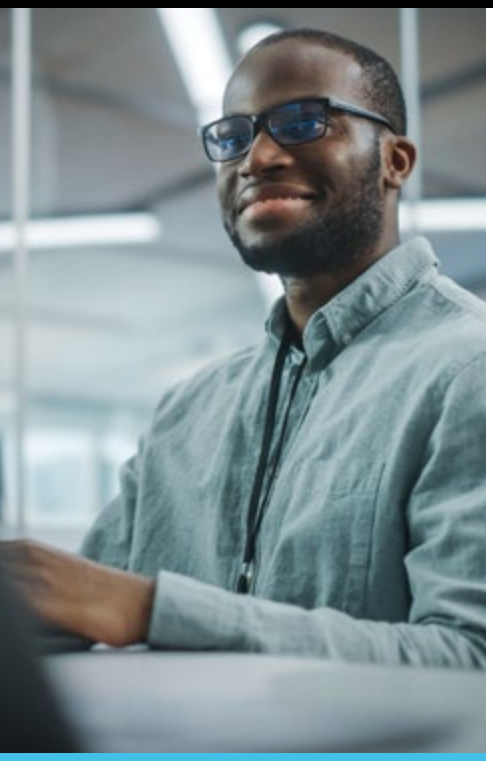
· Établir la stratégie des architectures de sécurité des SI en lien avec la stratégie globale métier et contribuer à la déclinaison des principes du modèle de sécurité globale
· Élaborer des modèles de référence pour les architectures
· Contribuer à la déclinaison des politiques de sécurité en standards de sécurité opérationnels

Conseil

· Conseiller sur l'utilisation et la combinaison des briques de sécurité existantes
· Analyser les risques de sécurité liés à l'introduction de nouvelles technologies ou de nouveaux systèmes d'information
· Assurer une veille sur les nouvelles menaces et en tenir compte dans la définition des architectures de sécurité
· Maintenir des relations avec les fournisseurs pour assurer une veille technologique sur les innovations et les outils de sécurité en vue de les intégrer dans les architectures de sécurité le cas échéant

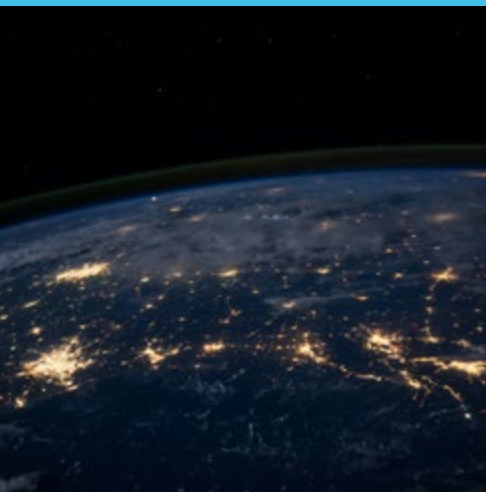






QUALITÉS

· Travailler en transverse au sein de l'organisation
· S'intégrer dans des réseaux pour pratiquer une veille technologique
· Prendre en compte les nouvelles méthodes de gestion de projet (méthode agile notamment).
· Manager une équipe
· Avoir un sens de l'intérêt général
· Résister à la pression
· S'approprier les enjeux métiers



Évolution de carrière

L'architecte cybersécurité doit être capable d'appréhender la complexification et la rapidité d'évolution des systèmes d'information, aussi bien sur un plan technique que fonctionnel. Il doit maîtriser les concepts d'architecture de sécurité dans des environnements en évolution (cloud, virtualisation, API…).

Avec le développement de l'IOT et des flux d'interconnexion avec l'extérieur, l'architecte cybersécurité est de plus en plus sollicité sur sa capacité à sécuriser un ensemble de socles ouverts et hétérogènes, en tenant compte des enjeux business de l'entreprise.

Ce métier fait l'objet d'une demande croissante liée au besoin de gérer des architectures de sécurité de plus en plus complexes face à l'augmentation des menaces.

Freelance

L'architecte cybersécurité peut exercer en tant qu'indépendant. L'idéal étant d'avoir quelques années d'expérience à un poste similaire en entreprise ou au sein d'un cabinet d'experts en cybersécurité. Organisation, compétences, qualités humaines et rigueur seront les quatre grands critères qui seront à prendre en compte pour lancer une activité freelance.

Le tarif journalier moyen d'un architecte cybersécurité freelance peut varier entre 500 et 800 euros.

Études

Pour devenir architecte cybersécurité, il est nécessaire de valider un Bac +5, via une école d'ingénieurs ou à l'université, avec une spécialisation en cybersécurité.

Ce métier est accessible à partir d'une expérience préalable d'au moins 8 ans en architecture technique des systèmes d'information.

Compétences

Exercer à ce poste demande un niveau d'exigence certain ainsi que la maîtrise de compétences indéniables. A savoir :

· Le système d'information, de l'urbanisation et de l'architecture du SI
· La sécurité des systèmes d'exploitation
· La sécurité des réseaux et protocoles
· La contribution des architectures à la sécurité : conception et modèles
· La contribution des architectures à la sécurité : intégration des systèmes
· Les connaissances des solutions de sécurité du marché
· La veille technologique cybersécurité et étude des tendances
· L'innovation cybersécurité
· La capacité de compréhension des menaces en matière de cybersécurité

Comment le devenir ?

Pour devenir architecte cybersécurité, il est nécessaire de préparer un diplôme de niveau Bac +5 en informatique avec une spécialité en sécurité des systèmes d'information. Il faudra également justifier d'au moins 8 années d'expérience en architecture technique des systèmes d'information.

L'architecte cybersécurité devra faire preuve d'une grande rigueur et d'une bonne résistance au stress, car il a en gestion et en suivi tout ce qui se rapporte au système d'information de l'entreprise.

Ce métier fait l'objet d'une demande croissante liée au besoin de gérer des architectures de sécurité de plus en plus complexes face à l'augmentation des menaces, notamment celles qui impliquent les objets connectés et l'IOT.

05

CHEF·FE DE PROJET CYBERSÉCURITÉ

Niveau d'études : Bac+5

Spé Conseillée : Maths ou NSI

Employabilité : Très Bonne

Salaire débutant : 4 000 €

Code ROME : M1802 - Code FAP : M2Z

LE CHEF DE PROJET DE SÉCURITÉ DES SYSTÈMES D'INFORMATION DÉFINIT, MET EN ŒUVRE ET CONDUIT DES PROJETS DE DÉPLOIEMENT DE SOLUTIONS ET D'OUTILS DE SÉCURITÉ, EN LIEN AVEC LES OBJECTIFS DE SÉCURITÉ FIXÉS PAR L'ORGANISATION.

Salaire

La rémunération d'un chef de projet sécurité varie en fonction de la taille de l'entreprise qui l'emploie et de son expérience.

En moyenne, un responsable sécurité débutant qui exerce en France touchera 4 000 euros par mois contre 6 000 euros pour un profil sénior.

En Suisse, le salaire annuel moyen d'un responsable de projet sécurité avoisine les 9 000 francs CHF.

Où travailler ?

Le responsable de projet sécurité peut exercer dans plusieurs types d'organisations. En effet, il peut travailler saisir l'opportunité de travailler aussi bien dans une entreprise industrielle que pour des sociétés de services ou dans le secteur public. Plus précisément :

- Éditeurs de logiciels et entreprises IT
- Banque, assurance, mutuelle
- Entreprises spécialisées dans les télécommunications
- Hôpitaux et centres de santé

Évolution de carrière

Au vu de la hausse et de la diversité des menaces cybercriminelles, le chef de projet sécurité est un professionnel de plus en plus recherché en entreprise.

Il pourra exercer en tant que responsable des systèmes d'information (RSSI) après avoir fait ses preuves plusieurs années en tant que responsable de projet sécurité.

La capacité à prendre en compte les nouvelles méthodes de gestion de projet (méthode agile notamment) est une compétence qui sera à développer sur ce poste dans les prochaines années.

Missions

Au quotidien, le responsable de projet de sécurité intervient sur 3 types de missions :

La phase d'analyse et de diagnostic qui consiste à :

· Définir les besoins permettant de répondre aux enjeux de sécurité en cohérence avec les enjeux métiers
· Réaliser les analyses des solutions de sécurité du marché
· Réaliser une veille sur les produits de sécurité et disposer d'une connaissance de ces produits afin de couvrir les risques
· Établir les spécifications fonctionnelles générales et rédiger les cahiers des charges pour des solutions de sécurité

Ensuite, vient la phase de conduite du projet au cours de laquelle il s'agit pour le responsable de projet de sécurité de :

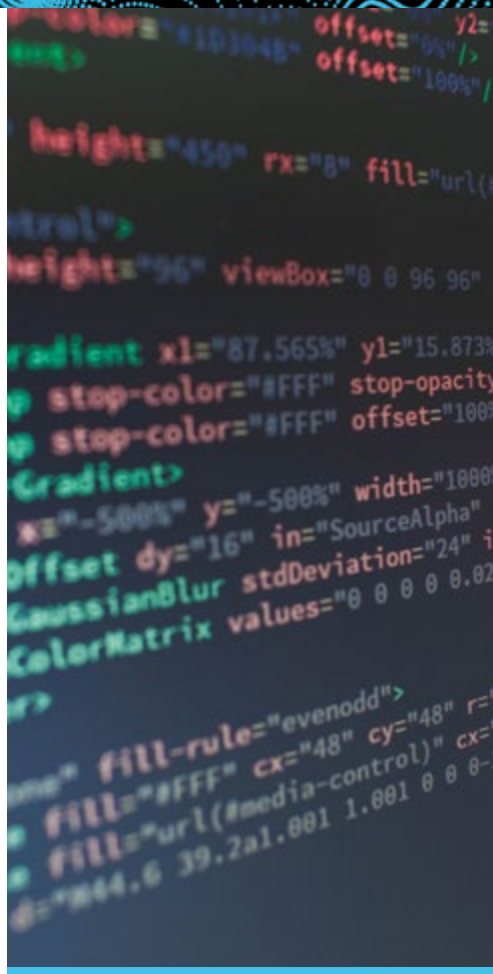
· Assurer le suivi des phases d'appel d'offres, réaliser l'évaluation et le choix des solutions, suivre la contractualisation
· Analyser les risques de sécurité liés au projet, proposer des mesures de sécurité si nécessaire
· Définir et superviser la réalisation des prototypes et de preuves de concept (POC) et des tests fonctionnels de la solution de sécurité choisie
· Prendre en main les solutions de sécurité étudiées (fonctionnellement et techniquement) lors des phases d'études
· Effectuer la recette des solutions de sécurité et apprécier leur conformité au cahier des charges
· Contribuer à la conception et à l'intégration des solutions de sécurité adoptées (incluant notamment les aspects d'architecture, de gestion des identités et des accès et de contribution à la stratégie de surveillance et de détection) et assurer leur suivi
· Participer à l'administration des dispositifs de protection, surveillance et contrôle des systèmes informatiques
· Évaluer de nouvelles solutions pour réduire les risques.
· Assurer les suivis des incidents
· Participer en condition opérationnelle, au maintien des dispositifs de continuité et de reprises mis en œuvre pour réduire les impacts en cas de dysfonctionnement ou de sinistre
· Contrôler la bonne intégration de la sécurité dans les projets et réaliser des audits internes ainsi que des tests afin d'apprécier l'évolution du niveau de sécurité des systèmes d'information
· Gérer le suivi des prestataires

Enfin, vient la phase de prévention où il doit :

· Formaliser et suivre l'avancement du plan d'action de réduction des risques des systèmes d'information (SSI)
· Accompagner l'utilisation des systèmes d'information par les équipes opérationnelles en rédigeant des normes, des guides de bonnes pratiques et des procédures qui respectent le cadre méthodologique du système de management de la sécurité de l'information
· Procéder à des actions de sensibilisation générale ou de sensibilisation ciblée auprès des utilisateurs du système d'information

Le responsable de projet de sécurité ne travaille jamais seul. Cet expert en cybersécurité doit en effet assurer la coordination des différents acteurs d'un projet afin d'en assurer le succès, tout en respectant la conformité du projet avec les besoins des maîtres d'ouvrage métiers. Ainsi, il est également un animateur, puisqu'il encadre une équipe de professionnels, informaticiens, développeurs et architectes sécurité.

Il prend en compte les conseils et expertises de son équipe afin de définir la stratégie de sécurité de l'information de l'entreprise. Il communique ensuite auprès de l'ensemble des parties prenantes tout au long du projet et alerte si nécessaire. Il anime les réunions de suivis et les comités de pilotage et communique les KPI (indicateurs) du projet.



QUALITÉS

· Un esprit d'analyse
· Un sens du service
· Une rigueur
· L'autonomie
· Une bonne communication
· Un bon relationnel
· Une bonne pédagogie
· Un sens de l'efficacité et du pragmatisme
· L'anticipation
· La réactivité et la disponibilité en cas de problème

Compétences

Exercer comme responsable de projet de sécurité informatique demande des compétences métiers, à la croisée de la gestion de projet, de la sécurité informatique et de la cybersécurité. Dans le détail, il doit connaître et maîtriser :

· Le droit et les réglementations en vigueur en matière de cybersécurité
· Lu système d'information et des principes d'architecture
· Les fondamentaux dans les principaux domaines de la SSI
· Les solutions de sécurité du marché
· La sécurité des systèmes d'exploitation, des réseaux et protocoles
· La gestion de projets et de portefeuille de projets
· Le pilotage de projets dans tous les domaines liés aux infrastructures
· La mise en œuvre une démarche d'audit
· L'accompagnement du changement et des évolutions d'un SI
· La manière de former et sensibiliser les utilisateurs
· La mise en œuvre d'une démarche qualité et de gestion des risques

Études

Pour devenir responsable de projet sécurité, vous devrez justifier d'un diplôme en informatique de niveau Bac+3 à Bac+5 avec une spécialisation en informatique.

Il vous sera demandé d'avoir une à plusieurs expériences dans le domaine de la gestion de projet cyber ou dans la gestion de projet informatique.

Certaines sociétés et entreprises exigent également des certifications en sécurité/produit comme par exemple la norme de sécurité ISO 27001 (appréciation des risques et anticipation des menaces, gestion des incidents).

Freelance

Le responsable de projet de sécurité peut exercer en tant que freelance indépendant. La première option consiste à créer un statut d'auto-entrepreneur ou une société individuelle auprès de la CCI. Il sera ainsi possible de facturer ses prestations à tous types de clients. Le responsable de projet de sécurité peut également faire le choix de rejoindre un cabinet d'experts en cybersécurité qui le positionnera sur plusieurs missions.

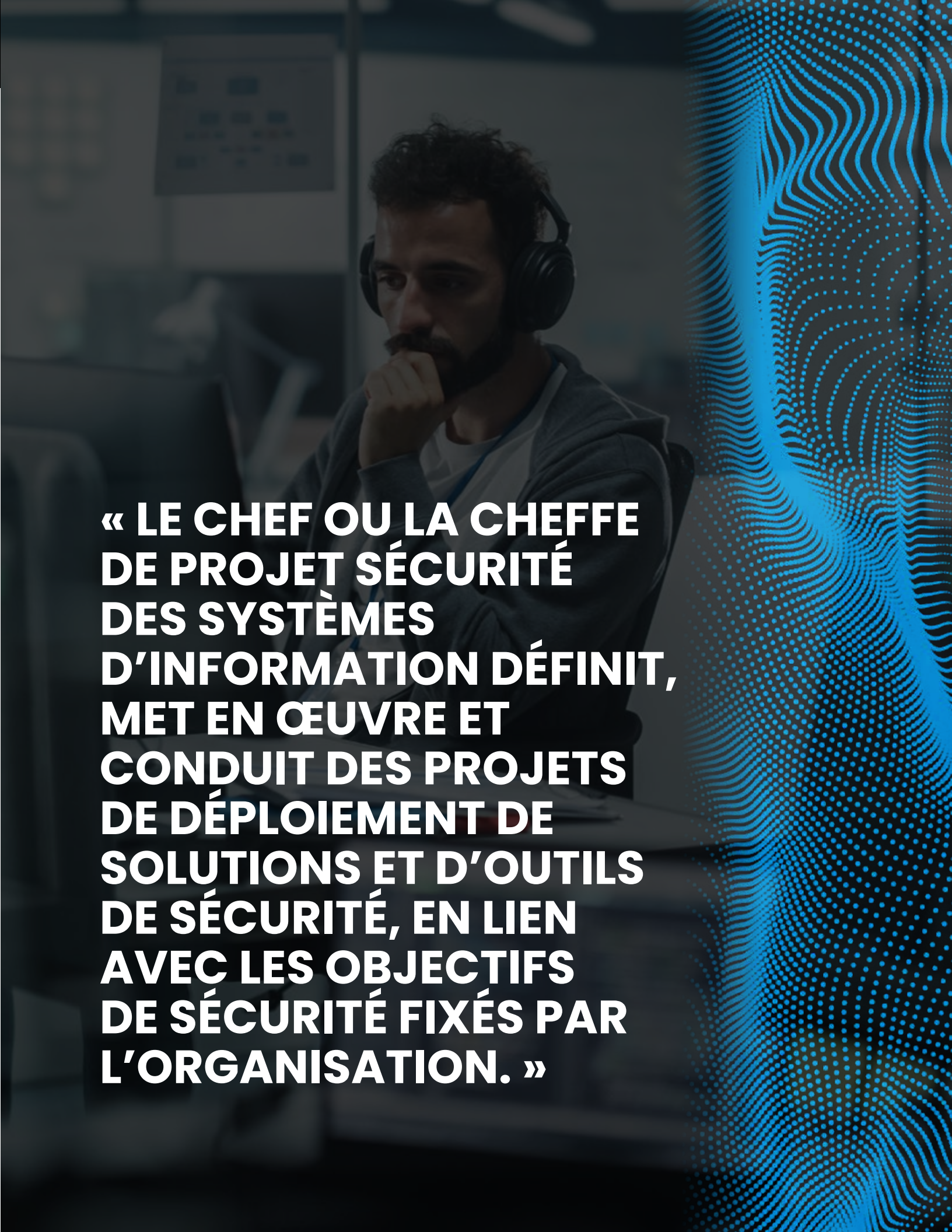
Le tarif journalier moyen d'un responsable de projet de sécurité freelance peut varier entre 600 et 1 500 euros, en fonction de ses expériences et références en entreprise.

Avantages et inconvénients

Si vous aimez la gestion de projet et le travail en équipe, le métier de responsable de projet de sécurité pourrait tout à fait vous convenir.

En effet, cet expert cybersécurité doit savoir s'adapter à son auditoire et ne pas avoir peur de s'exprimer auprès de cibles variées, direction, équipes, clients, etc.

Le métier est exigeant, il faut savoir se mettre au niveau rapidement, réaliser un travail de veille important et constant car les technologies et les vulnérabilités changent aussi vite que les missions du responsable de projet sécurité.



« LE CHEF OU LA CHEFFE DE PROJET SÉCURITÉ DES SYSTÈMES D'INFORMATION DÉFINIT, MET EN ŒUVRE ET CONDUIT DES PROJETS DE DÉPLOIEMENT DE SOLUTIONS ET D'OUTILS DE SÉCURITÉ, EN LIEN AVEC LES OBJECTIFS DE SÉCURITÉ FIXÉS PAR L'ORGANISATION. »

06

CONSULTANT·E EN CYBERSÉCURITÉ

Niveau d'études : Bac+5

Spé Conseillée : Maths ou NSI

Employabilité : Très Bonne

Salaire débutant : 3 500 €

Code ROME : M1802 - Code FAP : M2Z

LE CONSULTANT EST UN PROFESSIONNEL EXTERNE À L'ENTREPRISE RECONNU POUR SON EXPERTISE DANS UN DOMAINE PARTICULIER. LE CONSULTANT EN CYBERSÉCURITÉ PRÉSENTE SON PLAN D'ACTIONS AU MANAGER DE LA CYBERSÉCURITÉ.

Salaire

Le salaire d'un consultant expert en cybersécurité est variable selon les années d'expérience et le profil de l'entreprise pour laquelle il réalise sa carrière professionnelle.

Un consultant junior en début de carrière peut prétendre gagner entre 3 000 et 3 500 euros brut mensuels.

Au bout de quelques années, sa rémunération peut atteindre facilement les 4 500 à 5 800 euros brut mensuels, selon s'il exerce en cabinet de conseil ou chez un client final.

Où travailler ?

Il est possible d'exercer le métier de consultant expert en cybersécurité dans des environnements professionnels très divers.

Ainsi, les consultants peuvent travailler dans les secteurs industriels, pour des sociétés de services ou encore dans le secteur public. Les entreprises du monde bancaire, des assurances, des télécommunications, mais aussi des PME et TPE qui n'ont pas les ressources en interne peuvent faire appel à un consultant.

Freelance

Pour rester autonome dans le choix de ses missions et de ses clients, il est possible d'exercer le métier de consultant en cybersécurité en tant qu'indépendant. Il est également possible de rejoindre un cabinet. Ainsi, le consultant en cybersécurité n'aura pas à gérer la partie commerciale de son activité, qui sera traitée par le cabinet de conseil. De plus, le consultant en cybersécurité qui intervient pour un cabinet d'experts aura l'avantage de travailler avec d'autres experts de la cybersécurité et ainsi de développer son réseau et ses compétences.

Compétences

Pour envisager le métier de consultant expert en cybersécurité, il est indispensable de posséder un socle de compétences informatiques solides orientées cybersécurité.

Il est également nécessaire de maîtriser les principes de chiffrement.

L'anglais oral et écrit doit être d'un bon niveau, les documents techniques étant bien souvent rédigés en anglais. Enfin, il est important de rester en veille permanente sur les avancées technologiques.

Concrètement, il doit pouvoir :

· Analyser les besoins du client et projet
· Concevoir les solutions techniques
· Maîtriser les méthodes d'analyse (systémique, fonctionnelle, de risques…)
· Connaître les normes et standards
· Maîtriser les principes d'intégration de matériels et de logiciels
· Concevoir l'architecture d'un système d'information
· Évaluer le résultat de ses actions
· Connaître les règles de sécurité informatique et télécoms et les évaluer
· Procéder aux phases de tests des applications développées
· Mettre en place les procédures techniques d'exploitation, d'utilisation et de sécurité des systèmes
· Maîtriser la modélisation informatique
· Définir et contrôler l'application des procédures qualité et sécurité des systèmes d'information et de télécoms
· Connaître le droit du numérique
· Pouvoir effectuer une assistance technique
· Savoir traiter l'information
· Mettre à jour une documentation

En résumé, le consultant en cybersécurité est un expert de la sécurité informatique polyvalent, qui doit pouvoir analyser rapidement une situation de vulnérabilité informatique et déployer en réponse, la solution la plus adaptée pour l'entreprise.

C'est aussi un facilitateur, qui accompagne et sensibilise les équipes aux enjeux de sécurité informatique.

Comment le devenir ?

Pour devenir consultant en cybersécurité, il est nécessaire de préparer un diplôme d'ingénieur ou un Master en cybersécurité.

Le consultant en cybersécurité est un expert de la sécurité informatique mais aussi un facilitateur doté d'un bon relationnel pour accompagner et sensibiliser les entreprises aux enjeux de sécurité informatique.

À l'heure où les données numériques nécessitent d'être de plus en plus sécurisées, le consultant en cybersécurité est un expert très recherché sur le marché de l'emploi.

Le consultant en cybersécurité peut exercer dans les domaines publics ou privés, dans les secteurs de la défense, des télécommunications, de la santé, de la banque… Il peut intervenir en tant que freelance ou être rattaché à un cabinet de conseil.

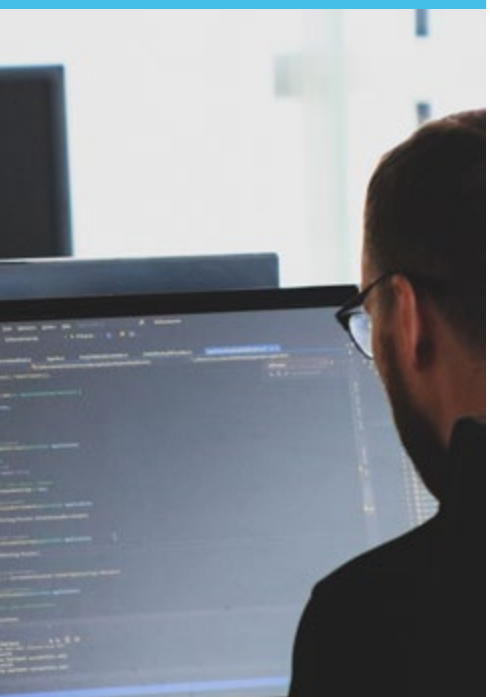
L'AVIS DU PROFESSIONNEL

« Pendant que je réalisais mon travail de recherche, j'ai commencé à travailler chez SPIE (entreprise spécialisée dans la smart city et le smart building) sur le sujet de la sécurité des données personnelles à travers les objets connectés. Je suis resté trois ans dans cette entreprise. Aujourd'hui, j'ai intégré un cabinet de conseil et je suis consultant expert en cybersécurité avec une spécialité en Internet des objets. Les consultants avec lesquels je travaille ont chacun leur propre spécialité. Ainsi, nous pouvons répondre de manière complémentaire et globale aux besoins des entreprises. »

Guillaume Celosia
Head of OT/IoT Security
CMA CGM

QUALITÉS

- À l'écoute
- Bon relationnel
- Curieux
- Se tenir informé



Missions

Le consultant accompagne les entreprises qui souhaitent sécuriser leurs systèmes.

Il intervient en matière de prévention, de détection et de lutte contre la cybercriminalité. Ainsi, le consultant peut être appelé aux différents stades de "maturité digitale" de l'entreprise. En effet, il n'agit pas seulement à posteriori en réaction à un problème de sécurité informatique, son rôle est aussi et surtout, de donner à l'entreprise toutes les clés de compréhension et d'anticipation face à une potentielle attaque informatique.

À l'image du médecin de famille qui prend en considération les antécédents, l'environnement et le mode de vie de son patient de façon à poser le bon diagnostic, le consultant expert en cybersécurité compose avec l'existant de l'entreprise en matière de sécurité informatique, fait le point sur les outils et compétences techniques en interne puis, en fonction du diagnostic qu'il aura établi, fait des recommandations et déploie les solutions adaptées.

En pratique, le consultant en cybersécurité travaille donc de concert avec l'entreprise afin de mieux connaître ses besoins, ses problématiques et ses enjeux, ce qui lui permet d'établir une stratégie sur-mesure adaptée à chaque client.

Le consultant pourra par exemple définir des scénarios d'attaques du système d'information d'une entreprise, lancer des tests d'intrusion dans un environnement informatique ultra sécurisé à la recherche d'une faille éventuelle, traquer les virus et les malwares sur les machines d'un client...

Le rôle du consultant en cybersécurité ne se limite pas qu'à un rôle de prestation technique. En effet, c'est lui qui bien souvent devra accompagner le personnel de la société sur la nécessité de sécuriser le système informatique et les former aux usages et réglementations en vigueur en matière de sécurité informatique. Il apporte donc son expertise aussi bien sur des sujets méthodologiques que techniques.

L'AVIS DU PROFESSIONNEL

« Lorsque nous intervenons pour le compte d'un client, nous sommes vus comme des guides par l'entreprise. Pourtant, arriver en tant que conseil extérieur au sein d'une entreprise n'est jamais chose aisée. Comprendre le fonctionnement d'une équipe, ses process, ses enjeux... c'est comme une grande énigme à résoudre ! Le consultant doit faire son propre cheminement au sein de l'entreprise. Dans notre métier, dès lors que nous avons bien saisi les enjeux et problématiques du client, une relation de confiance s'installe sur le long terme et nous avons un réel impact sur la vie de l'entreprise. L'avantage, par-delà l'aspect humain, c'est aussi de pouvoir apprécier dans le temps l'évolution des actions mises en place. »

Guillaume Celosia
Head of OT/IoT Security
CMA CGM

Évolution de carrière

La cybersécurité est devenue un élément stratégique pour toutes les organisations publiques et privées. Les débouchés sont donc nombreux.

Néanmoins, le marché du conseil est très compétitif et il faut savoir se démarquer de la concurrence avec des compétences ciblées et éventuellement une spécialisation.

Un consultant en cybersécurité pourra, s'il le souhaite, évoluer vers un poste de responsable sécurité des systèmes d'information (RSSI) ou prendre en charge des missions de plus en plus complexes.

Études

Pour devenir consultant en cybersécurité, vous devrez justifier d'un diplôme Bac +5. C'est bien souvent ce qui est demandé par des entreprises lors d'un recrutement. Un niveau d'étude qui fait déjà de vous un expert en cybersécurité.

Il est possible de préparer par exemple un diplôme d'ingénieur ou un Master 2 avec une spécialité en cybersécurité.

L'AVIS DU PROFESSIONNEL

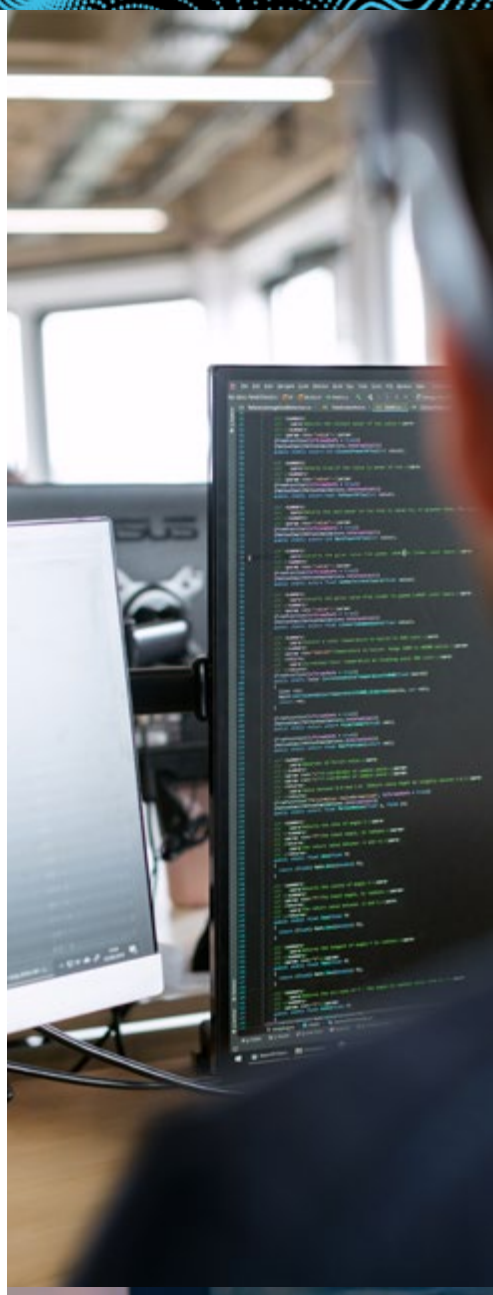
« On manque de compétences sur les objets industriels. Il y a un vrai créneau à prendre pour les consultants qui voudraient s'intéresser à ce sujet. »

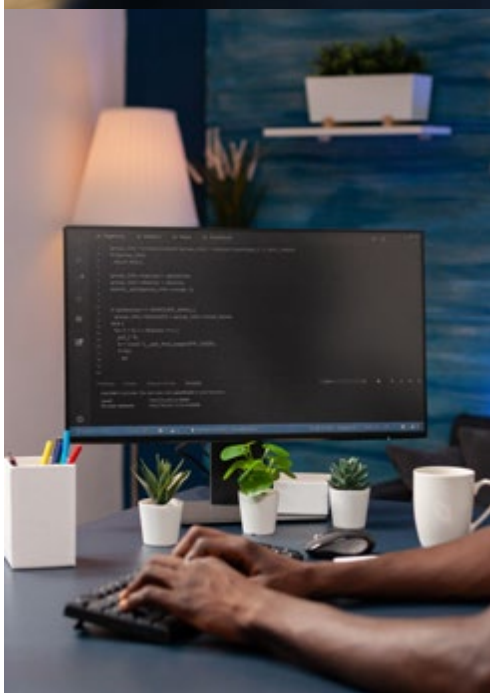
Guillaume Celosia
Head of OT/IoT Security
CMA CGM

L'AVIS DU PROFESSIONNEL

« Les compétences métiers dépendent des sujets d'intérêt de la personne car chaque consultant peut avoir des expertises différentes. Il faut bien sûr avoir des connaissances dans le domaine de la sécurité informatique, car même les projets de sécurité orientés plus sur la gouvernance ou les risques demandent d'avoir des connaissances en informatique. »

Amandine Durand
Lean Compliance Designer
COMPLEYE.IO





Avantages et inconvénients

« On ne s'ennuie jamais dans ce métier ! » Parmi les avantages du métier de consultant en cybersécurité, Guillaume Celosia apprécie la diversité des rencontres, des missions et environnements de travail.

Amandine Durand ajoute : *"Les avantages du métier de consultant sont le fait de travailler sur des projets très divers, ce qui permet d'acquérir de l'expérience sur une large palette de sujets. Cela permet aussi de découvrir quels sont les sujets qui nous intéressent le plus dans le domaine très large de la cyber. Il n'y a pas de routine dans la mesure où le passage d'un projet à un autre permet de changer régulièrement de sujets."*

Du côté des inconvénients, la nécessité de mettre à jour ses compétences régulièrement est à prendre en considération, afin de ne pas se retrouver rapidement dépassé. En effet, le sujet de la cybersécurité évoluant très rapidement, nombreux sont les consultants experts en cybersécurité qui, comme Guillaume Celosia, continuent de se former, via des Mooc, des webinars, des certifications, afin d'actualiser leurs compétences

Freelance

Pour rester autonome dans le choix de ses missions et de ses clients, il est possible d'exercer le métier de consultant en cybersécurité en tant qu'indépendant. Il est également possible, comme Guillaume Celosia de rejoindre un cabinet de consultants experts en cybersécurité. Ainsi, le consultant en cybersécurité n'aura pas à gérer la partie commerciale de son activité, qui sera traitée par le cabinet de conseil. De plus, le consultant en cybersécurité qui intervient pour un cabinet d'experts aura l'avantage de travailler avec d'autres experts de la cybersécurité et ainsi développer son réseau et ses compétences.

L'AVIS DU PROFESSIONNEL

« Après le Bac, je savais que je voulais faire de l'informatique mais je ne savais pas quoi exactement. J'ai choisi de m'inscrire dans un cursus d'ingénieur en 2012. L'école proposait un tronc commun d'enseignements autour de la sécurité des technologies informatiques. Je me suis ensuite orienté vers une option sécurité des systèmes ubiquitaires. Puis, j'ai effectué un stage de 7 mois chez Thalès en tant qu'ingénieur cybersécurité. Enfin, en 2017, j'ai réalisé une thèse sur le thème des défis de vies privées dans les communications sans fil de l'Internet des objets (IOT). Ma thèse m'a beaucoup apporté dans le quotidien de mes missions en qualité de consultant expert en cybersécurité. J'ai en effet acquis une méthodologie de recherche et d'analyse que je réinvestis chaque jour dans mes missions auprès du client. »

Guillaume Celosia
Head of OT/IoT Security
CMA CGM

07

CRYPTOLOGUE

Niveau d'études : Bac+5

Spé Conseillée : Maths ou NSI

Employabilité : Très Bonne

Salaire débutant : 2 800 €

Code ROME : M1802 - Code FAP : M2Z

LE CRYPTOLOGUE OU CRYPTANALYSTE EST CHARGÉ DE SÉCURISER LES DONNÉES D'UNE ENTREPRISE EN CRÉANT DES ALGORITHMES COMPLEXES QUI EMPÊCHERONT L'EXPLOITATION DE DONNÉES DITES SENSIBLES À DES FINS ILLÉGALES.

Missions

La cryptographie désigne l'ensemble des mécanismes destinés à garantir la sécurité et la protection de messages que l'on souhaite protéger.

Le cryptologue ou cryptanalyste ou encore ingénieur cryptologue est chargé de sécuriser les données d'une entreprise en créant des algorithmes complexes qui empêcheront l'exploitation de données dites sensibles à des fins illégales.

Le cryptologue élabore des méthodes de codage en créant un procédé de chiffrage de données inviolable. Fraude bancaire, usurpation d'identité, intrusion dans un système informatique… Le cryptologue est chargé d'empêcher la compromission d'informations sensibles en développant des méthodes de chiffrement qui consistent à transformer un message clair en message incompréhensible et qui est seulement accessible pour qui détient la clé de chiffrement.

Pour devancer les pirates informatiques, cet expert en sécurité des systèmes de communication teste sans cesse la résistance et la fiabilité de ses encodages et met à l'épreuve les programmes conçus par ses collègues pour s'assurer de leur efficacité. Il cherche notamment à éliminer tout risque d'interception des mots de passe ou de redirection des utilisateurs vers un serveur pirate.

Compétences

A la fois informaticien et mathématicien, le métier de cryptologue nécessite de développer des compétences multiples telles que :

· Disposer de connaissances solides en informatique, sécurité réseaux et développement
· Maîtriser les techniques de cryptographie
· Des connaissances approfondies en cryptanalyse
· Maîtriser l'anglais oral et écrit
· Rester en veille permanente sur les avancées technologiques
· Analyser les besoins du client et du projet
· Concevoir les solutions techniques
· Maîtriser les méthodes d'analyse
· Connaître les normes et standards d'exploitation
· Maîtriser les principes d'intégration de matériels et de logiciels
· Concevoir l'architecture d'un système d'information
· Évaluer le résultat de ses actions
· Connaître les règles de sécurité informatique et télécoms
· Procéder aux phases de tests des applications développées
· Connaître les normes rédactionnelles
· Mettre en place les procédures techniques d'exploitation, d'utilisation et de sécurité des équipements informatiques
· Maîtriser la modélisation informatique
· Définir et contrôler l'application des procédures qualité et sécurité des systèmes d'information et de télécoms
· Connaître le droit du numérique
· Pouvoir effectuer une assistance technique
· Savoir traiter l'information (collecter, classer et mettre à jour)
· Mettre à jour une documentation technique

Salaire

Les profils d'experts cryptologues sont très convoités. En effet, le marché de l'emploi étant extrêmement favorable à l'évolution des recrutements dans le secteur de la cybersécurité, le métier de cryptologue est un choix de carrière offrant de belles perspectives et opportunités.

Le salaire d'un cryptologue est variable selon les années d'expérience et le profil de l'entreprise où il réalise sa carrière professionnelle.

En France, un cryptologue en début de carrière peut prétendre entre 2 500 et 2 800 euros brut mensuels.

En milieu de carrière, le salaire peut tourner autour des 4 900 euros brut mensuels.

Quant à l'étranger, le salaire annuel moyen d'un cryptologue se situe entre 83 000 et 150 000 dollars aux Etats-Unis par exemple.

Où travailler ?

Il est possible d'exercer le métier de cryptologue dans des environnements professionnels très divers.

Ainsi, les experts cryptologues peuvent travailler dans les secteurs industriels, pour des sociétés de services ou encore dans le secteur public.

· Secteur de la défense DGSE, Direction Générale de la Sécurité Extérieure ou DGSI, Direction Générale de la Sécurité Intérieure
· Editeurs de logiciels et entreprises informatiques
· Secteur bancaire
· Secteur des télécommunications
· Sociétés de conseil en hautes technologies

QUALITÉS

· Apprécier le travail en équipe
· Faire preuve de méthode et de rigueur
· Être patient et persévérant
· Avoir une bonne résistance au stress et à la pression

Études

Devenir cryptologue revient à s'engager dans un processus de formation long, d'au minimum cinq ans afin d'avoir toutes les compétences et connaissances que requirent le métier. Il faut un très bon niveau technique notamment.

Le choix peut se tourner vers la préparation d'un diplôme d'ingénieur avec une spécialité en cryptographie, sécurité et codage de l'information.

Ou de privilégier un diplôme de niveau master dans une école spécialisée en cybersécurité avec des options en cryptographie et sécurité des systèmes d'information.

Freelance

Pour rester autonome dans le choix de ses missions et de ses clients, il est possible d'exercer le métier de cryptologue en tant qu'indépendant. Après la création des statuts de l'entreprise, il faudra trouver ses clients, aussi bien auprès de son réseau qu'en faisant de la prospection commerciale. C'est pourquoi, posséder une expérience en entreprise est un sérieux atout.

Il est également possible de rejoindre un cabinet de consultants indépendants experts en cybersécurité. Ainsi, le cryptologue n'aura pas à gérer seul la partie commerciale de son activité.

Évolution de carrière

La cybersécurité est devenue un élément stratégique pour toutes les organisations publiques et privées. Les débouchés sont donc nombreux.

Un cryptologue peut par exemple évoluer vers un poste de responsable sécurité des systèmes d'information (RSSI) ou prendre en charge des missions de plus en plus complexes.

Avantages et inconvénients

Le métier de cryptologue est un métier passion que l'on choisit rarement par hasard. Si vous adorez passer plusieurs heures à en découdre avec un message codé complexe, ce métier peut tout à fait vous correspondre !

Il faudra néanmoins faire preuve de beaucoup de patience, de rigueur et être doté d'une bonne résistance au stress, le cryptologue intervenant dans des situations professionnelles extrêmement sensibles.

Comment le devenir ?

Pour devenir cryptologue, il faut avant tout avoir de solides compétences en mathématiques complexes et en codage informatique.

Il est possible par exemple de préparer un diplôme d'ingénieur ou un Master avec une spécialité en cryptographie, sécurité et codage de l'information.

A l'heure où les données numériques nécessitent d'être de plus en plus sécurisées, le cryptologue est un expert de la cybersécurité très recherché sur le marché de l'emploi. En début de carrière, il pourra prétendre à un salaire mensuel avoisinant les 2 900 euros et pourra voir sa rémunération doubler en milieu de carrière. L'ingénieur cryptologue peut exercer dans les domaines publics ou privés, dans les secteurs de la défense, des télécommunications, de la santé, de la banque...

En fonction de son expertise technique et de la manière dont il exploitera ses compétences et savoir-être en entreprise, le cryptologue confirmé pourra être amené à développer des projets de plus en plus complexes, et éventuellement encadrer une équipe en qualité de responsable sécurité des systèmes d'information.

Cryptosystèmes connus

Aujourd'hui, un cryptologue fera appel à deux systèmes de codage bien distincts afin de sécuriser les communications et les données d'une entreprise.

On distingue en effet deux grandes familles de cryptosystèmes : les cryptosystèmes symétriques (ou à clé secrète) et les cryptosystèmes asymétriques (ou à clé publique).

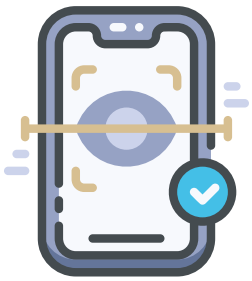
Les algorithmes de chiffrement symétrique se fondent sur une même clé pour chiffrer et déchiffrer un message. L'un des problèmes de cette technique est que la clé, qui doit rester totalement confidentielle, doit être transmise au correspondant de façon sûre. La mise en œuvre peut s'avérer difficile, surtout avec un grand nombre de correspondants (il faut autant de clés que de correspondants).

Quelques algorithmes de chiffrement symétrique très utilisés :

· Chiffre de Vernam (le seul offrant une sécurité théorique absolue, à condition que la clé ait au moins la même longueur que le message à chiffrer, qu'elle ne soit utilisée qu'une seule fois et qu'elle soit totalement aléatoire)
· DES
· 3DES
· AES
· RC4
· RC5
· MISTY1

Quelques algorithmes de cryptographie asymétrique très utilisés :

· RSA (chiffrement et signature)
· DSA (signature)
· Protocole d'échange de clés Diffie-Hellman (échange de clés)



08

DÉVELOPPEUR·EUSE DE SOLUTIONS

Niveau d'études : Bac+5

Spé Conseillée : Maths ou NSI

Employabilité : Très Bonne

Salaire débutant : 3 800 €

Code ROME : M1802 - Code FAP : M2Z

LE DÉVELOPPEUR DE SOLUTIONS DE SÉCURITÉ CONÇOIT DES PROGRAMMES, LOGICIELS ET APPLICATIONS, QUI RÉSISTENT AUX ATTAQUES À TOUS LES NIVEAUX (INTERFACE, DESIGN, CODE SOURCE).

Missions

Le développeur de solutions de sécurité assure la conception et la certification de solutions et de produits adaptés face aux menaces et vulnérabilités de cybersécurité.

Ce professionnel combine une expertise technique dans l'écriture de logiciels et des compétences dans l'analyse des menaces de sécurité et le développement de produits. Il travaille en équipe et collabore avec les concepteurs et les ingénieurs pour s'assurer que les menaces potentielles sont prévues et traitées de manière adéquate.

Son rôle est d'envisager dans les solutions créées toutes les options possibles et de les intégrer pleinement à l'architecture de référence des systèmes d'information.

Les missions du développeur de solutions de sécurité sont découpées en quatre étapes :

L'analyse :

· Analyser et prendre en compte les besoins de sécurité et le contexte des menaces
· Contribuer à la définition des spécifications générales de la solution de sécurité
· Réaliser l'analyse technique et l'étude détaillée de la solution de sécurité

Le développement :

· Planifier et conduire les différents projets de développement de solutions de sécurité
· Assurer le développement de solutions de sécurité

La qualification :

· Réaliser des tests afin de s'assurer que les solutions de sécurité répondent bien aux exigences de protection ou de détection
· Contribuer à l'implémentation de la solution ou du produit dans une architecture logicielle et le tester

La maintenance :

· Assurer la maintenance corrective et la maintenance évolutive des solutions de sécurité

Où travailler ?

Le développeur en solutions de sécurité étant LE professionnel de la cybersécurité le plus recherché à l'heure actuelle, les opportunités d'emploi sont donc nombreuses et notamment dans les domaines suivants :

· Editeurs de logiciels et entreprises informatiques
· La banque
· Les télécommunications

Freelance

Pour rester autonome dans le choix de ses missions et de ses clients, il est possible d'exercer le métier de développeur en solutions de sécurité en tant qu'indépendant. Sous le statut d'auto-entrepreneur ou d'une société individuelle, travailler à la mission pour le compte de clients est une option qui séduit de nombreux professionnels. Ce qui est d'ailleurs le cas plus généralement pour les développeurs informatiques. Si cette idée fait son chemin, sachez qu'il faudra une vraie maîtrise technique, une rigueur à toute épreuve, un sens de la négociation et du relationnel.

Compétences

Pour devenir développeur de solutions de sécurité, il est indispensable de posséder un socle de compétences informatiques solides orientées programmation, développement et cybersécurité. Plus précisément, il faut maîtriser :

· Le développement logiciel et ingénierie logicielle (sous l'angle de la sécurité) : conception, développement des applications et des vulnérabilités logicielles
· Le système d'information, de l'urbanisation et de l'architecture du SI
· Conseil, services et recherche
· La production de procédures
· Cyberdéfense : connaissance des techniques d'attaques et d'intrusions et des vulnérabilités des environnements
· Connaissance des couches applicatives
· Connaissance en développement (codes embarqués, langages de conception)
· Contribution des architectures à la sécurité : intégration des systèmes

Salaire

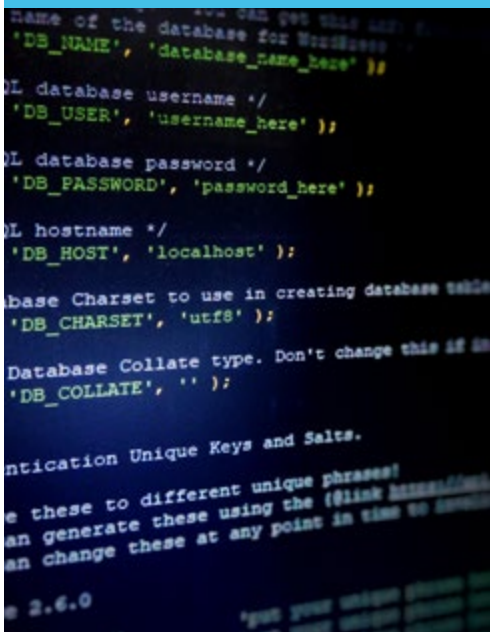
A l'heure où le sujet de la cybersécurité touche toutes les sphères professionnelles, les profils de développeurs de solutions de sécurité sont très recherchés.

Parmi les professions qui sont en tension, on retrouve celles liées au développement dans la filière cybersécurité, avec des candidats en position de force pour négocier leur package de rémunération. Le dernier baromètre des salaires du numérique 2021 présenté par la plateforme de recrutement CodinGame indique en effet que les développeurs qui travaillent dans ce domaine sont ceux qui bénéficient des plus hauts niveaux de rémunération.

Avec un salaire annuel moyen de 46 000 euros, la sécurité reste en effet le secteur d'activité qui paye le mieux les développeurs en 2021.

QUALITÉS

· La rigueur
· Le bon relationnel
· La créativité
· L'ambition
· Une bonne résistance au stress



Avantages et inconvénients

Si vous détestez l'ennui et la routine, vous serez à l'aise dans le métier de développeur de solutions de sécurité. Les missions du poste nécessitent une grande créativité et une agilité qui raviront les geeks aux idées complexes et foisonnantes.

Le métier de développeur de solutions de sécurité est un travail très bien rémunéré car ce profil d'expert est très recherché par les entreprises.

Du côté des inconvénients, il est possible de citer la pression liée à la charge de travail. Il est important de savoir garder son sang-froid car le développeur de solutions de sécurité intervient sur des programmes et des solutions d'envergure.

Évolution de carrière

La cybersécurité est devenue un élément stratégique pour toutes les organisations publiques et privées. Les débouchés sont donc nombreux pour les développeurs.

Les menaces de sécurité pesant sur les appareils connectés et sur le secteur de l'Internet des objets (IOT) font partie des défis actuels et à venir de la cybersécurité. De nombreuses opportunités se dessinent pour les développeurs afin de créer des programmes qui limitent les risques et vulnérabilités des appareils autonomes.

Études

Bac + 3 à Bac+ 5. Pour vouloir travailler comme développeur, il faut pouvoir maîtriser un certain nombre d'outils et de techniques et avoir des compétences en matière de cybersécurité, si bien qu'un diplôme trois ans après le Bac est le minimum requis.

Le choix se tournera vers un diplôme d'ingénieur par exemple dans une école spécialisée ou un Master 2 informatique avec une spécialité en sécurité des systèmes d'information par exemple.

09

DIRECTEUR·RICE CYBERSÉCURITÉ

Niveau d'études : Bac+5

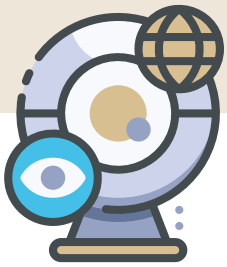
Spé Conseillée : Maths ou NSI

Employabilité : Très Bonne

Salaire débutant : 8 000 €

Code ROME : M1802 - Code FAP : M2Z

LE DIRECTEUR DE LA CYBERSÉCURITÉ DOIT APPORTER SA VISION ET SON EXPERTISE POUR ÉLABORER UNE STRATÉGIE CYBERSÉCURITÉ QU'IL DÉCLINE DANS DES PROGRAMMES PLURIANNUELS, EN COHÉRENCE AVEC LES ENJEUX MÉTIERS DE L'ENTREPRISE.



Missions

Dans ses missions au quotidien, le directeur cybersécurité assure la surveillance des vulnérabilités internes relatives à la gestion de l'information de l'entreprise. Il gère la mise en place de l'organisation (ressources humaines) qu'il maintient en condition opérationnelle de sécurité les infrastructures et services de l'entreprise à l'aide de procédures de sécurité. Il produit le tableau de bord de suivi des actions de réduction des vulnérabilités et de l'exposition aux cyber-attaques et assure la veille technique et fonctionnelle pour être en mesure d'anticiper une éventuelle attaque ou défaillance des services de l'entreprise. Enfin, il pilote la communication, la formation et la sensibilisation de tous les employés à la protection du capital informationnel de l'entreprise.

Ainsi, les missions du directeur de la cyber-sécurité sont de l'ordre de la planification, de l'animation, de la vérification/veille et de l'évaluation :

Planifier :

· Définir les axes et les objectifs stratégiques en matière de cybersécurité et les faire valider par la Direction générale
· Identifier les enjeux de sécurité, les risques majeurs de sécurité pesant sur l'organisation et les exigences de conformité légale et réglementaire
· Définir et maintenir la politique de sécurité des SI en collaboration avec les parties prenantes

· Définir la stratégie de mise en conformité au cadre législatif et réglementaire ; assurer les relations avec les acteurs de son secteur d'activité autour de la cybersécurité
· Définir un plan d'actions annuel ou pluriannuel
· Définir une politique d'investissement au regard des objectifs de sécurité
· Définir l'organisation de la cybersécurité au sein de l'organisation et l'animer
· Définir les mesures organisationnelles et techniques à mettre en œuvre pour atteindre les objectifs de sécurité
· Piloter la réalisation de la charte de sécurité informatique de l'organisation et la promouvoir auprès de tous les utilisateurs
· Contribuer à répondre aux sollicitations des clients et partenaires de l'organisation sur les aspects sécurité

Animer :

· Animer le réseau des RSSI à travers une gouvernance sécurité
· Apporter un support à la mise en œuvre en fournissant une assistance technique et méthodologique ainsi que des outils et des solutions de sécurité, éventuellement à travers un catalogue de services

Vérifier :

· Évaluer le niveau de sécurité au sein de l'organisation, notamment à travers la réalisation d'audits périodiques et de contrôles permanents
· Contrôler que les politiques et règles de sécurité des SI sont appliquées dans l'organisation et vis-à-vis des tiers et sous-traitants (third parties)

Rendre compte :

· Rapporter régulièrement auprès de la Direction générale sur le niveau de couverture courant des risques de sécurité SI
· Assurer un rôle de conseil auprès de la Direction générale et des métiers de l'organisation
· Représenter l'organisation dans les relations avec les autorités de régulation

Compétences

Pour devenir directeur de la cybersécurité, il est indispensable de posséder une connaissance pointue des enjeux de sécurité de l'entreprise et de maîtriser l'ensemble des expertises internes en cybersécurité. Voici la liste des compétences à savoir :

· Les enjeux et des métiers de l'organisation
· Construire la stratégie cybersécurité de l'organisation
· Compréhension des menaces cybersécurité
· Système d'information et principes d'architecture
· Fondamentaux dans les principaux domaines de la SSI
· Technologies de sécurité et des outils associés
· Gestion des risques, politique de cybersécurité et SMSI
· Connaissance juridique en matière de droit informatique lié à la sécurité des SI et à la protection des données
· Connaissance de la gouvernance, des normes et des standards dans le domaine de la sécurité : normes ISO (2700X), normes sectorielles (PCI-DSS…)

Salaire

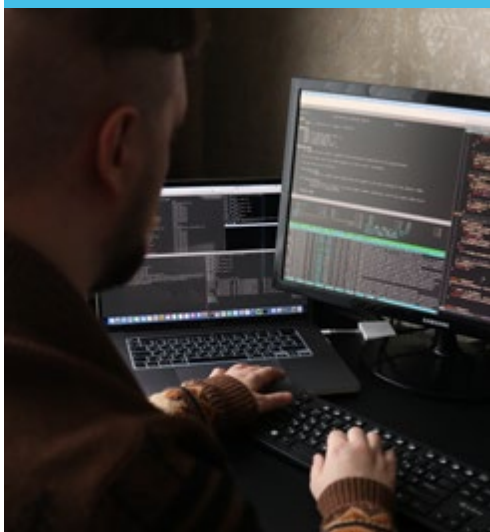
A l'heure où le sujet de la cybersécurité nécessite d'être organisé au sein d'une direction structurée, les profils de directeurs de la cybersécurité sont très recherchés.

Le salaire des directeurs cybersécurité expérimentés est en moyenne compris entre 100 000 et 200 000 euros annuels et varie en fonction de la taille de l'entreprise et le domaine d'activité.

A l'international, aux Etats-Unis par exemple, un directeur de la cybersécurité peut gagner entre 100 000 et 200 000 dollars annuels.

QUALITÉS

· Leadership
· Capacité d'influence
· Sens de l'intérêt général
· Management d'équipe
· Capacité à travailler en transverse au sein de l'organisation
· Capacité d'appropriation des enjeux métiers
· Rigueur
· Bon relationnel
· Ambition
· Excellente résistance au stress



Où travailler ?

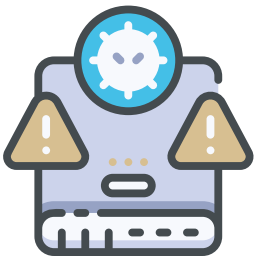
Pour les entreprises ayant acquis une sensibilité aux cyber-risques, on constate de plus en plus souvent l'existence d'un « département de gestion des risques » composé de plusieurs représentants : de la cybersécurité, de l'audit, du contrôle interne (s'il existe), de la direction juridique, de la gestion de la finance/assurance, de la gestion de la sécurité physique, et parfois de représentants métiers comme aussi de la Direction Informatique. Dans d'autres cas, on constate que le directeur cybersécurité est rattaché à la direction informatique, mais comme la protection de l'information est l'affaire de tous, il est nécessaire qu'il ait à minima un rôle transversal dans l'entreprise.

Voici un exemple d'entreprises et institutions qui font appel à des directeurs cybersécurité :

· Editeurs de logiciels et entreprises informatiques
· Secteur bancaire
· Secteur des télécommunications
· Sociétés de conseil en Hautes Technologies

Études

Avant de prétendre à un poste de direction, il faudra justifier d'une expérience professionnelle supérieure à 10 ans dans le domaine de la cybersécurité. Au tout début de la chaîne, il faut d'abord envisager des études supérieurs pour atteindre un Bac +5. Le mieux étant de se lancer dans la filière informatique avec une spécialisation en cybersécurité. Diplôme d'ingénieur ou master 2 sont les deux voies à privilégier à l'université ou en école formant aux métiers de la cybersécurité.



Évolution de carrière

La cybersécurité est devenue un élément stratégique pour toutes les organisations publiques et privées. La crise pandémique s'est accompagnée d'une recrudescence des cyberattaques, de nouvelles techniques de contournement des protections en place et d'une augmentation de la surface d'attaques des entreprises liée au télétravail. Dans bien des entreprises, la situation a remis au premier plan la nécessité de recruter un directeur de la cybersécurité. Les débouchés sont donc nombreux, et les ambitions de ce métier devraient continuer de se développer.

Comment le devenir ?

Pour devenir directeur cybersécurité, il est nécessaire de préparer un Bac +5 en informatique avec une spécialité en sécurité des systèmes d'information.

Il faudra avoir fait ses preuves pendant au moins 10 ans sur des projets de cybersécurité avant de pouvoir prétendre à un poste de direction.

Le directeur de la cybersécurité est un expert qui doit savoir faire preuve d'une grande rigueur et d'une excellente résistance au stress car il a en gestion et en suivi les enjeux de cyberdéfense d'organisations importantes et complexes.

Il doit être charismatique et posséder un excellent relationnel afin de pouvoir porter les ambitions digitales de sa direction auprès des équipes.

Avantages et inconvénients

Le poste de directeur de la cybersécurité est passionnant pour les profils de leader qui recherchent la variété des missions, le challenge intellectuel et un fort sentiment d'utilité professionnelle.

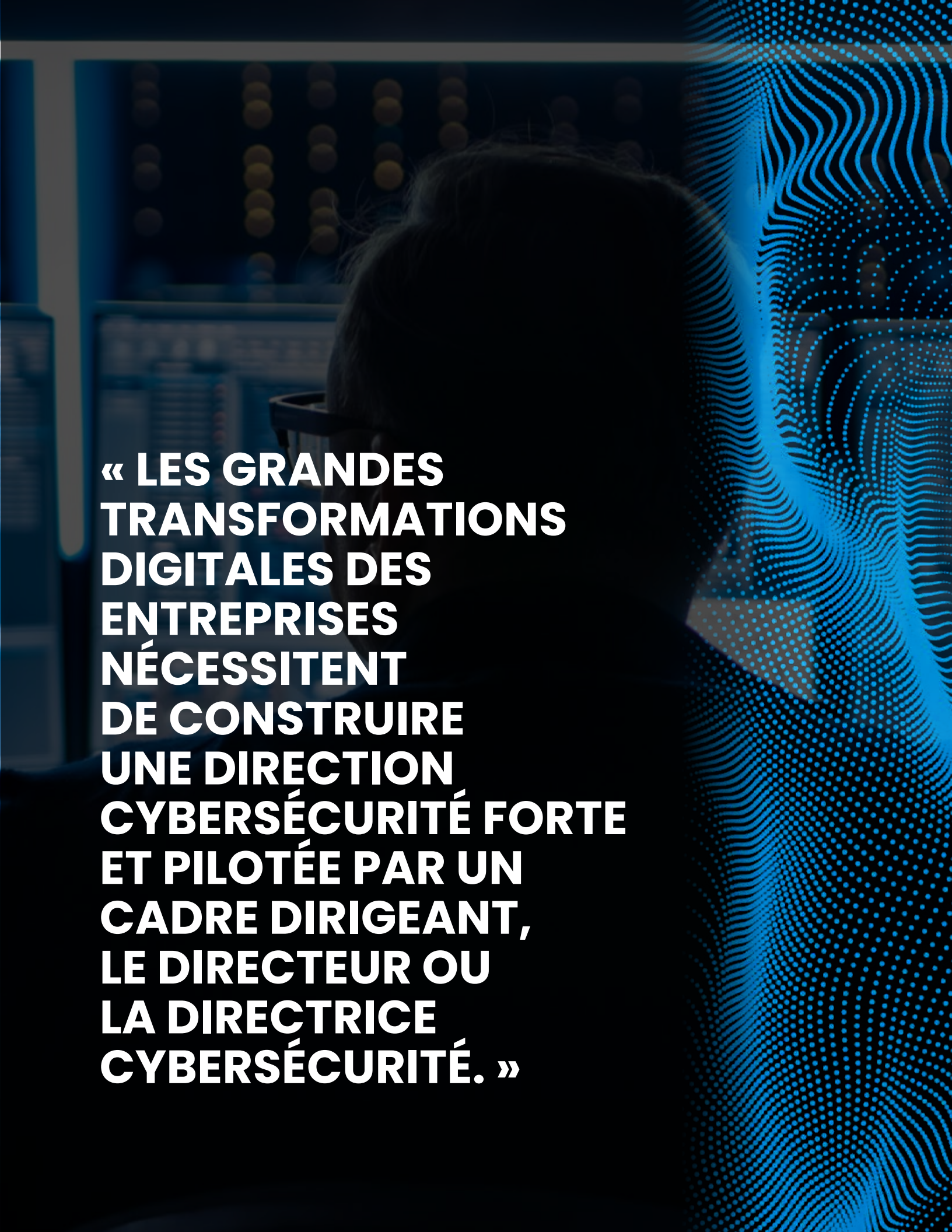
Le métier de directeur de la cybersécurité est un profil très bien rémunéré, mais cela va de pair avec les grandes responsabilités qui incombent à ce profil extrêmement précieux pour l'entreprise.

Du côté des inconvénients, il est possible de citer la pression liée à la charge de travail.

Freelance

Exercer le métier de directeur de la cybersécurité en tant qu'indépendant en proposant son conseil aux entreprises, telle est la mission de certains directeur cybersécurité qui ont fait le choix de travailler à la mission (plus ou moins longue). Ceci étant ce n'est pas le statut le plus courant pour ce métier, contrairement à des métiers comme développeur ou consultant. En effet, les entreprises recherchent davantage des profils internalisés puisqu'il s'agit de travailler sur des données sensibles.

Toutefois, un directeur cybersécurité freelance peut facturer entre 1 000 et 2 000 euros la journée de prestation.



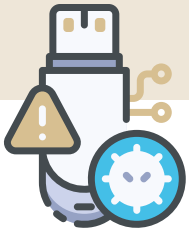
« LES GRANDES TRANSFORMATIONS DIGITALES DES ENTREPRISES NÉCESSITENT DE CONSTRUIRE UNE DIRECTION CYBERSÉCURITÉ FORTE ET PILOTÉE PAR UN CADRE DIRIGEANT, LE DIRECTEUR OU LA DIRECTRICE CYBERSÉCURITÉ. »

FORMATEUR·RICE EN CYBERSÉCURITÉ

Niveau d'études : Bac+5
Spé Conseillée : Maths ou NSI
Employabilité : Bonne
Salaire débutant : 2 900 €

Code ROME : M1802 - Code FAP : M2Z

LE FORMATEUR EXPERT EN CYBERSÉCURITÉ DÉFINIT DES PROGRAMMES DE SENSIBILISATION SUR LE SUJET DE LA CYBERSÉCURITÉ ET CONÇOIT DES OUTILS ET SUPPORTS DE FORMATION ADAPTÉS À DIFFÉRENTS PUBLICS.



Comment le devenir ?

Pour devenir formateur en cybersécurité, il est nécessaire de préparer un diplôme de niveau Bac + 5 en informatique avec une spécialité en sécurité des systèmes d'information. Le formateur en cybersécurité devra également être rompu aux techniques d'animation et d'ingénierie pédagogique.

À l'heure où les données numériques nécessitent d'être de plus en plus maîtrisées par les équipes qui utilisent quotidiennement les SI de l'entreprise, le formateur en cybersécurité est un expert facilitateur très recherché sur le marché de l'emploi. En début de carrière, il pourra prétendre à un salaire avoisinant les 2 000 euros brut mensuels et pourra voir sa rémunération quasiment doubler en milieu de carrière.

Il peut exercer dans les domaines publics ou privés, intervenir en tant que freelance, être salarié d'un cabinet de conseil et de formation à la cybersécurité, ou être directement rattaché à un organisme de formation.

Évolution de carrière

La cybersécurité est devenue un élément stratégique pour toutes les organisations publiques et privées. Les débouchés sont donc nombreux.

Néanmoins, le marché de la formation est très compétitif et il faut savoir se démarquer de la concurrence, surtout si l'on décide de se lancer en freelance.

Un formateur en cybersécurité pourra, s'il le souhaite, évoluer vers un poste de consultant expert en SSI ou prendre en charge des missions de formations de plus en plus complexes.

Missions

Le formateur en cybersécurité intervient auprès de publics qui souhaitent être accompagnés sur le sujet de la cybersécurité : entreprises, partenaires, sous-traitants ou encore étudiants en informatique avec des programmes sur-mesure. Il partage ses compétences et son savoir-faire et s'assure que les volets réglementaires, techniques ou opérationnels de la cybersécurité soient bien assimilés par les publics en formation. Il apporte donc son expertise aussi bien sur des sujets méthodologiques que techniques.

Le formateur en cybersécurité partage ses connaissances en matière de prévention, de détection et de lutte contre la cybercriminalité.

Ainsi, cet expert en cybersécurité peut être amené à former une entreprise sur le fonctionnement de l'architecture de solutions de sécurité, expliquer comment effectuer les meilleurs choix technologiques au sein des systèmes d'information, ou encore montrer comment optimiser tous les paramètres dans des environnements de production avec certaines exigences de sécurité.

Quels que soient les interlocuteurs auxquels s'adresse le formateur en cybersécurité, l'objectif de sa méthodologie de formation est de rendre autonomes les utilisateurs et les publics exposés aux risques des systèmes d'information et de favoriser leur montée en compétences.

Voici le détail des missions réalisées par le formateur en cybersécurité :

· Définir des plans de formation et de sensibilisation adaptés aux différents publics
· Concevoir et réaliser des parcours et des supports de formation à destination des utilisateurs et des publics exposés aux risques de sécurité des SI
· Concevoir, organiser et animer des formations internes et externes dans le domaine de la sécurité des SI en s'appuyant sur des experts le cas échéant
· Se tenir informé de l'état de l'art dans son domaine et assurer une veille active permettant d'actualiser les formations en fonction de l'évolution du contexte (technique, organisationnel, menaces, régulation)
· Construire et piloter les actions de sensibilisation à la sécurité des SI et de conduite du changement auprès des utilisateurs
· Évaluer le niveau des publics cibles en entrée et en sortie des actions de formation ou de sensibilisation

Avantages et inconvénients

Parmi les avantages du métier de formateur en cybersécurité, la transmission de savoirs est l'aspect le plus gratifiant et appréciable dans le fait de former des apprenants.

Du côté des inconvénients, la nécessité de mettre à jour ses compétences régulièrement est à prendre en considération, afin de ne pas se retrouver rapidement dépassé. En effet, le sujet de la cybersécurité évoluant très rapidement, nombreux sont les formateurs experts en cybersécurité qui continuent de se former, via des Mooc, des webinars, des certifications, afin d'actualiser leurs compétences.

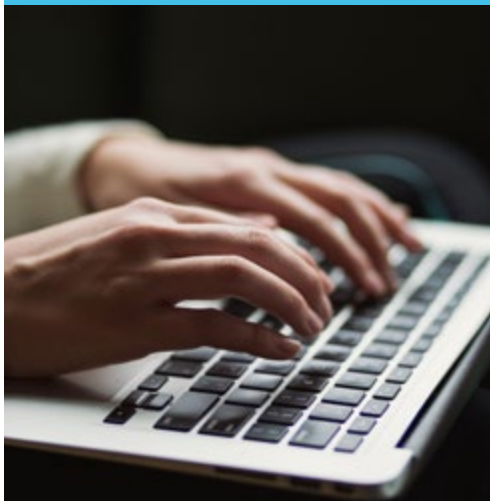
Freelance

Pour rester autonome dans le choix de ses missions et de ses clients, il est possible d'exercer le métier de formateur en cybersécurité en tant qu'indépendant. La première option consiste à créer un statut d'auto-entrepreneur ou une société individuelle.

Il sera ainsi possible de facturer ses prestations de formations à tout type de clients, entreprises, services publics ou encore organismes de formations. Il est également possible de rejoindre un cabinet de formateurs experts en cybersécurité.

QUALITÉS

· Pédagogue
· Curieux
· À l'écoute
· Réactif
· Créatif
· Adaptable
· Disponible
· Avoir le goût du défi
· Savoir faire de la veille technoloqique



Où travailler ?

Il est possible d'exercer le métier de formateur expert en cybersécurité dans des environnements professionnels très divers.

Ainsi, ils peuvent travailler dans les secteurs industriels, pour des sociétés de services ou encore dans le secteur public. Le formateur en cybersécurité peut aussi travailler pour le compte d'une école ou d'un organisme de formation.

Voici un exemple d'entreprises et institutions qui font appel à des formateurs en cybersécurité :

· Editeurs de logiciels et entreprises informatiques
· Secteur bancaire
· Secteur des télécommunications
· Sociétés de conseil en hautes technologies
· Organismes de formation initiales et continue

Salaire

A l'heure où le sujet de la cybersécurité touche toutes les sphères professionnelles, les profils de formateurs experts en cybersécurité sont très recherchés.

Le salaire d'un formateur expert en cybersécurité est néanmoins variable selon son expérience, les compétences techniques maîtrisées et le type de formation proposée (expertise, durée de la mission, etc.)

Un formateur junior en début de carrière peut prétendre entre 2 000 et 2 900 euros brut mensuels.

Au bout de quelques années d'expérience, sa rémunération peut atteindre facilement les 4 000 euros brut mensuels, selon qu'il exerce à son propre compte, en cabinet de conseil ou au sein d'un organisme de formation.

A l'international, aux Etats-Unis par exemple, un formateur en cybersécurité peut gagner entre 68 000 et 100 000 dollars annuels.

Compétences

Pour devenir formateur expert en cybersécurité, il est indispensable de posséder un socle de compétences informatiques solides orientées cybersécurité, telles que des compétences avancées sur les architectures, les déploiements, les protocoles, les applications, les systèmes, les bases de données.

Enfin, il est important de rester en veille permanente sur les avancées technologiques du secteur de la cybersécurité. Concrètement, cela se traduit par :

· La maîtrise des outils et plateformes spécifiques à la formation en SSII
· La connaissance du système d'information et des principes d'architecture
· La connaissance des technologies de sécurité et des outils associés
· La gestion des risques, politique de cybersécurité et SMSI
· La maîtrise des fondamentaux dans les principaux domaines de la SSI
· Une veille technologique cybersécurité et étude des tendances

Études

Pour devenir formateur en cybersécurité, un diplôme de niveau Bac +5 minimum sera généralement la première condition pour exercer à ce poste. Une exigence demandée par les entreprises qui doivent assurer un haut niveau de compétences vis-à-vis de leur client. Pour cela, il est possible de préparer un Master 2 informatique avec une spécialité en cybersécurité.

Afin de pouvoir sensibiliser les publics au sujet de la cybersécurité, vous devrez, parallèlement à vos études d'informatique, vous former aux techniques d'ingénierie pédagogique, d'accompagnement au changement et d'animation collective. L'idéal est en plus de cela d'avoir une expérience dans le milieu avant de vous lancer en tant que formateur.

GESTIONNAIRE CRISE CYBERSÉCURITÉ

Niveau d'études : Bac+5

Spé Conseillée : Maths ou NSI

Employabilité : Bonne

Salaire débutant : 3 800 €

Code ROME : M1802 - Code FAP : M2Z

LE GESTIONNAIRE CRISE DE CYBERSÉCURITÉ INTERVIENT SOUVENT AU SEIN D'UN CSIRT (COMPUTER SECURITY INCIDENT RESPONSE TEAM) OU D'UN CERT (COMPUTER EMERGENCY RESPONSE TEAM) INTERNE À DES GRANDS GROUPES.

Missions

Voici le détail des activités et tâches au quotidien du gestionnaire crise de cybersécurité :

Anticipation :

· Conseiller l'organisation
· Définir les moyens nécessaires à la gestion de crise
· Vérifier tous les éléments de préparation des crises
· Assurer la formation
· Tester et valider la capacité de l'organisation à réagir à une attaque

Réaction :

· Organiser la gestion de crise pour agir et traiter la crise
· Animer la cellule de crise décisionnelle
· Coordonner l'action des différentes parties en présence et la diffusion des informations
· Assurer les relations avec les autorités et les assurances
· S'assurer de la cohérence de la stratégie de communication
· Organiser les revues post-mortem

Les étapes de la gestion de crise :

Lors d'une crise cyber, il faut en principe entre une semaine et un mois afin de retrouver une situation normale. Elle se déroule en plusieurs étapes :

· Phase d'endiguement : contrer l'attaque et colmater les failles
· Phase d'assainissement : réinitialiser le périmètre corrompu
· Phase de durcissement : audit complet pour prévenir les prochaines attaques

C'est quoi un CSIRT ou CERT ?

Les experts CSIRT sont composés de chercheurs, d'ingénieurs informatiques, d'analystes sécurité et de spécialistes en business intelligence qui réunissent leurs expertises afin de détecter et de prévenir les failles de vulnérabilités au sein de serveurs, programmes et logiciels. A eux également de réagir en cas d'incidents de sécurité informatique.

Ils contribuent à faire évoluer les technologies au sens large et les systèmes de protection et de sécurité informatiques.

Les tâches prioritaires d'un CSIRT sont les suivantes :

· Centralisation des demandes d'assistance suite aux incidents de sécurité (attaques) sur les réseaux et les systèmes d'information : réception des demandes, analyse des symptômes et éventuelle corrélation des incidents ;

· Traitement des alertes et réaction aux attaques informatiques : analyse technique, échange d'informations avec d'autres CERT, contribution à des études techniques spécifiques ;

· Établissement et maintenance d'une base de données des vulnérabilités ;

· Prévention par diffusion d'informations sur les précautions à prendre pour minimiser les risques d'incident ou au pire leurs conséquences ;

· Coordination éventuelle avec les autres entités : centres de compétence réseaux, opérateurs et fournisseurs d'accès à Internet, CERT nationaux et internationaux.

Face à une menace informatique toujours croissante et en mutation, l'amélioration de la résilience numérique par l'entraînement à la gestion de crise cyber n'est plus seulement une opportunité, mais bien une nécessité pour toutes les organisations.

Demain, l'organisation responsable et génératrice de confiance sera celle qui s'attache à maîtriser le risque numérique et fait preuve de sa capacité à se relever d'une crise d'origine cyber. Or, les crises cyber ont leurs spécificités : technicité du sujet, impacts fulgurants, évolutivité, sortie de crise longue, etc.

Le gestionnaire crise de cybersécurité analyse l'ampleur de la crise, met en place les actions nécessaires à sa résolution et coordonne les équipes pour qu'elles appliquent ses recommandations.

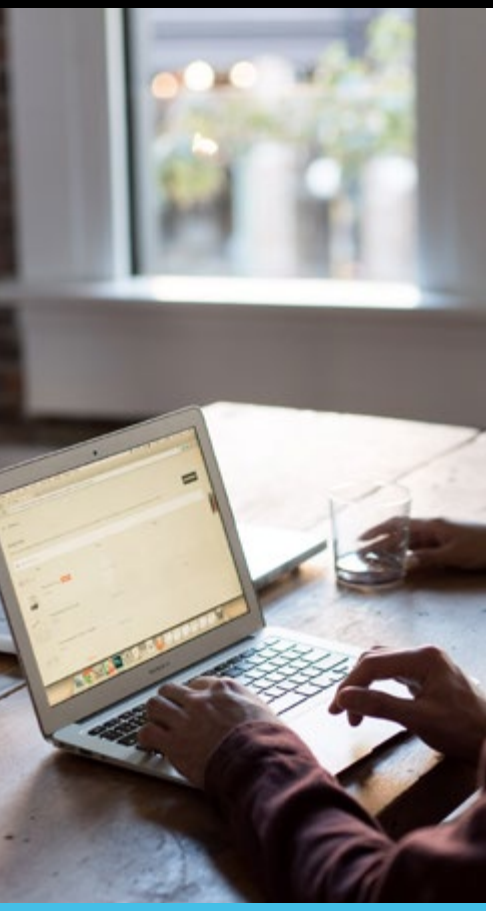
Il conseille les directions métiers afin de résoudre les crises de cybersécurité.

Il organise la capacité de l'organisation à affronter de nouvelles menaces en matière de cybersécurité.

L'AVIS DU PROFESSIONNEL

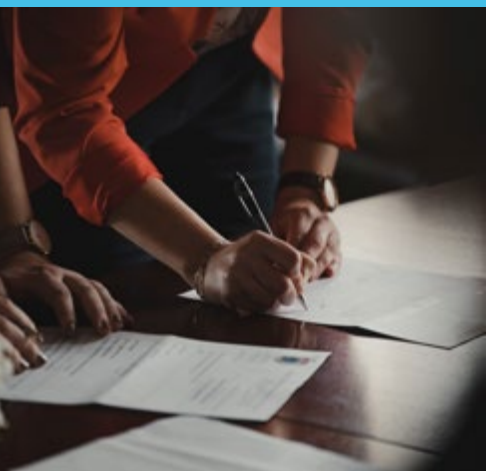
« Le gestionnaire crise de cybersécurité est avant tout un gestionnaire de crise. De manière générale, il a pour tâches d'appréhender une situation difficile, d'en estimer les conséquences et impacts, d'envisager des réponses dont certaines seront déployées jusqu'à retour à une situation calme. La cybersécurité est un champ d'application comme la finance ou l'industrie chimique. L'erreur consisterait à concevoir la gestion d'une cybercrise comme une situation technique qui doit être résolue par des cybertechniciens. Car ses impacts touchent notamment les métiers de l'entreprise, sa stabilité économique, de nombreuses parties prenantes dont les clients, la réputation de l'entreprise et peut se conclure par des inculpations judiciaires, 5 aspects dont les cybertechniciens ignorent tout. Ils font partie des équipes mobilisées pour résoudre la crise, mais ne sont pas pilotes de sa gestion. »

Olivier Velin
Gestionnaire crise de cybersécurité
DEVOTEAM



QUALITÉS

· Avoir le sens de l'interêt général
· S'approprier les enjeux métiers
· Restituer et vulgariser à des publics non techniques
· Coordonner de nombreuses équipes
· Résister à la pression
· Communiquer en interne et en externe



Où travailler ?

Le gestionnaire crise de cybersécurité intervient souvent au sein d'un CSIRT. Les CSIRT sont un réseau international, composé d'entreprises et d'institutions de tailles et profils très variés.

Liste des CSIRT ou CERT en France :

· CERT gouvernemental : CERT-FR (anciennement CERTA appartenant à l'ANSSI / SGDSN) est le CERT affecté au secteur de l'administration française
· Ai CERT : CERT privé interne du Groupe Airbus
· AlliaCERT : CERT de la société Alliacom ouvert à l'ensemble des entreprises et des institutions
· Axa CERT : CERT privé interne du Groupe Axa
· CERT-Akaoma : CSIRT de la société Akaomaproposant des services de cyber-surveillance et de réponse aux incidents de sécurité à l'ensemble des entreprises et institutions
· CERT-AlgoSecure : CSIRT privé de la société AlgoSecure ouvert à l'ensemble des entreprises et des institutions
· CERT-AG : CERT du Groupe Crédit Agricole et des filiales
· CERT-Amossys: CERT de la société Amossys
· CERT-Areva : CERT privé interne du groupe Areva
· CERT-BDF : CERT de la Banque de France

Avantages et inconvénients

Le métier de gestionnaire crise de cybersécurité est un poste à hautes responsabilités dans lequel la routine n'existe pas avec des salaires élevés.

Ce métier est à réserver aux profils qui savent faire preuve de sang-froid et qui ne craignent pas la pression, car la gestion de crise cyber est un processus complexe et sensible au sein des organisations.

Compétences

Exercer comme gestionnaire crise de cybersécurité demande de solides compétences informatiques et des connaissances pointues en cybersécurité telles que :

· Les enjeux et les métiers de l'organisation
· Les technologies de sécurité et des outils associés
· La maîtrise des fondamentaux dans les principaux domaines de la SSI
· Cyberdéfense : connaissance en gestion de crise, des types d'attaques et d'intrusions, des vulnérabilités des environnements
· Le droit informatique lié à la sécurité et à la protection des données

Évolution de carrière

Au sein des organisations qui ne disposent pas d'une structure de réponse à incidents spécifique, le métier de gestionnaire de crise de cybersécurité n'est pas toujours dédié, alors les missions peuvent être assurées par le RSSI ou par d'autres acteurs de l'organisation de gestion de crise.

Il est possible en outre de prétendre, après plusieurs années d'exercice, à un poste de responsable du CSIRT.

Études

Pour devenir gestionnaire crise de cybersécurité, vous devrez justifier d'un diplôme en informatique de niveau Bac + 5 avec une spécialisation en cybersécurité.

Une expérience professionnelle de 5 ans minimum au sein d'un CSIRT sera exigée avant de pouvoir devenir gestionnaire de cellule de crise cyber.

Freelance

Le gestionnaire crise de cybersécurité peut exercer en tant que freelance indépendant. La première option consiste à créer un statut d'auto-entrepreneur ou une société individuelle auprès de la Chambre de Commerce. Il sera ainsi possible de facturer ses prestations à tout type de clients.

Un gestionnaire crise de cybersécurité freelance peut facturer entre 400 et 1200 euros la journée.

Néanmoins, ce choix est encore plutôt rare, dans la mesure où, d'ordinaire, ce métier est exercé au sein d'un CSIRT.

Salaire

La rémunération d'un gestionnaire crise de cybersécurité varie selon le type d'organisation au sein de laquelle il intervient.

Le salaire médian d'un gestionnaire crise de cybersécurité en France est de 45 000 euros annuels.

Un profil senior ou expert pourra prétendre à un salaire allant jusqu'à 56 000 euros annuels.

Aux Etats-Unis, dans le comté de New-York par exemple, un gestionnaire crise de cybersécurité est rémunéré entre 130 000 et 175 000 dollars annuels.

« ANTICIPER SUR LA POTENTIELLE SURVENANCE D'UNE CRISE, IDENTIFIER LES VULNÉRABILITÉS QUI EN SERAIENT À L'ORIGINE »

L'AVIS DU PROFESSIONNEL

« D'un point de vue stratégique, l'existence d'un dispositif de gestion de crise montre la capacité d'anticipation de la direction, son leadership et son souci d'amélioration permanente de ses processus. D'un point de vue organisationnel, les membres d'une cellule de crise structurée, donc non improvisée, développent un savoir-faire collectif et des savoir-être individuels qui renforcent leurs capacités de gestion des situations habituelles. D'un point de vue RH, la gestion de crise accroît la cohésion au sein des équipes et, en cas de crise déclarée, contribue à préserver les emplois. D'un point de vue IT ou cyber. D'un point de vue financier, limitation des pertes. D'un point de vue communication, défense de l'image de l'entreprise et de ses dirigeants afin d'éviter une détérioration de leurs réputations. »

Olivier Velin
Gestionnaire crise de cybersécurité
DEVOTEAM

12 HACKER·EUSE ÉTHIQUE

Niveau d'études : Bac+5

Spé Conseillée : Maths ou NSI

Employabilité : Très Bonne

Salaire débutant : 4 000 €

Code ROME : M1802 - Code FAP : M2Z

PROFESSIONNEL DE LA CYBERSÉCURITÉ, LE HACKER ÉTHIQUE INTERVIENT AU SEIN DES ENTREPRISES ET DES ORGANISATIONS AFIN D'ASSURER LA PROTECTION DES SYSTÈMES D'INFORMATION FACE À D'ÉVENTUELLES MENACES DE PIRATAGE.

Salaire

La rémunération d'un hacker éthique varie en fonction de la taille de l'entreprise qui l'emploie et de son expérience. En moyenne, un hacker éthique débutant qui exerce en France touchera 4 000 euros brut par mois contre 7 500 euros brut pour un profil sénior.

De plus en plus de professionnels sont également rémunérés sous forme de récompenses à la résolution d'un bug grâce aux plateformes de bug bounty.

Aux États-Unis, le salaire annuel moyen avoisine les 80 000 dollars.

Avantages et inconvénients

Choisir de faire carrière en tant que hacker éthique, c'est avant tout s'engager dans un métier passion qui est en première ligne dans la lutte en faveur de la cyberdéfense. Le salaire peut aussi être intéressant et sur les missions relevées. Un challenge qui peut motiver.

Le hacker éthique, en revanche, ne comptera pas ses heures afin de parvenir à sécuriser au mieux le SI de l'entreprise qui l'emploie. Le métier demande un engagement assez important.

Évolution de carrière

Même si le métier de hacker éthique n'est pas encore vraiment reconnu en tant que tel dans les entreprises, cela tend à changer rapidement face à la hausse et à la diversité des menaces cybercriminelles.

En France, les hackers éthiques sont souvent, à la base, des experts en systèmes d'information ou des experts sécurité et réseaux, formés par la suite en cybercriminalité. Il s'agit plus d'une évolution de poste que d'un véritable changement de fonction.

Où travailler ?

Le hacker éthique peut exercer dans divers types d'organisations qui recherchent des profils compétents. Elles sont bien souvent importantes et gèrent des données sensibles. On les retrouve dans des secteurs de l'industrie de pointe, de la défense ou encore chez des éditeurs de services informatiques. Cela peut être aussi le cas dans les secteurs bancaire, assurance, numérique ou service public

Freelance

Le hacker éthique peut exercer en tant que freelance pour cela, il lui faut un statut d'entreprise. L'idéal étant pour démarrer celui d'autoentrepreneur. Il peut ainsi choisir ses clients, ses missions, son tarif et s'organiser comme il le veut. En contrepartie, les clients rechercheront des compétences, de la qualité et une rigueur.

Toujours en étant indépendant, il peut aussi faire le choix de travailler pour un cabinet d'experts en cybersécurité qui le positionnera sur plusieurs missions.

Le tarif journalier moyen d'un hacker éthique freelance peut varier entre 800 et 2 200 euros.

Compétences

Exercer comme hacker éthique demande de solides compétences informatiques et des connaissances pointues en cybersécurité :

· Capacité de compréhension des menaces cybersécurité
· Capacité à exploiter des sources ouvertes de manière sécurisée
· Mise en place de plans de veille sur un ou plusieurs secteurs déterminés
· Détection, qualification et analyse d'informations pertinentes
· Le droit et les réglementations en vigueur en matière de cybersécurité

Études

Pour devenir hacker éthique, il faut posséder un bon niveau en informatique et plus précisément une spécialisation en cybersécurité.

Une formation de niveau Bac +3 minimum est requise ou poursuivre jusqu'à Bac +5.

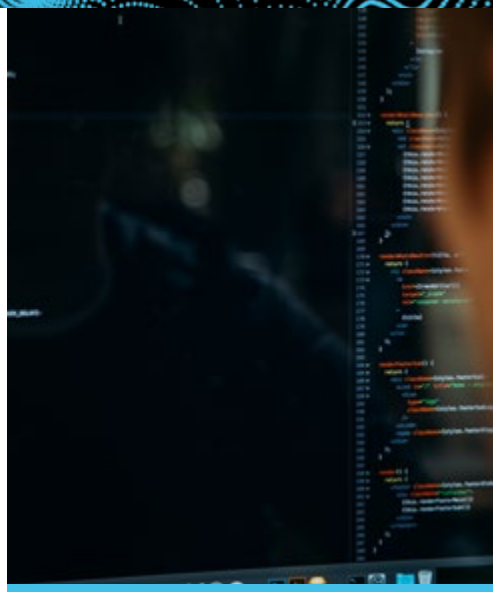
Plusieurs possibilités pour suivre une formation : à l'université, en école d'ingénieurs ou faire le choix d'une école spécialisée dans les métiers de la cybersécurité.

Missions

Le hacking est un ensemble de techniques permettant d'exploiter les possibilités, failles et vulnérabilités d'un élément informatique.

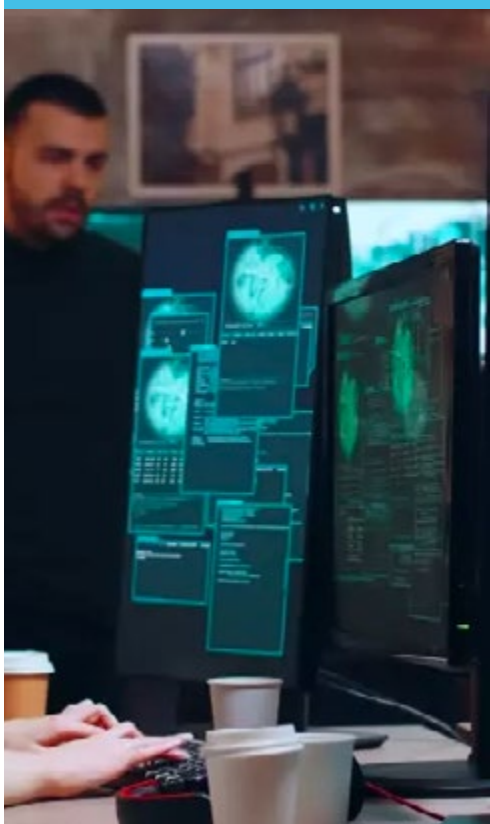
Le hacking ou piratage éthique décrit l'activité de hacking lorsqu'elle n'est pas malveillante. Ainsi, le piratage éthique désigne le processus par lequel un hacker bienveillant également baptisé "white hat" accède à un réseau ou un système informatique avec les mêmes outils et ressources que son confrère malveillant, "black hat", à la différence qu'il y est autorisé.

Cette pratique séduit de plus en plus d'entreprises craignant la fuite ou la compromission de leurs données confidentielles. Concrètement, le hacker éthique va contourner les règles de sécurité de la société et organiser une attaque informatique afin de détecter les failles du système d'information et les différents points de vulnérabilité. En effet, pour contrer un pirate informatique mal intentionné, il faut penser et agir comme lui.



QUALITÉS

· Rester éthique et légal
· La curiosité
· Le dynamisme
· La réactivité
· La créativité
· La disponibilité
· Le sens de la confidentialité
· Aimer le travail en équipe
· Le goût du défi



Pour aider les entreprises à se protéger des attaques informatiques, les hackers éthiques assurent, entre autres, les missions suivantes :

Mission n°1 : Identifier les mauvaises configurations de sécurité

Les entreprises sont tenues de suivre les standards de sécurité sectoriels et de se conformer à des protocoles permettant de réduire les risques d'attaques sur leur réseau. Néanmoins, si ces procédures ne sont pas correctement respectées, les hackers malveillants n'auront aucun mal à repérer les failles de sécurité. Les conséquences peuvent alors être terribles pour l'entreprise, avec des pertes de données sensibles et/ou stratégiques.

L'absence de chiffrement des fichiers, les applications web mal configurées, les appareils non sécurisés, la conservation des identifiants par défaut ou encore l'utilisation de mots de passe faibles constituent quelques-unes des erreurs de configuration les plus fréquentes. Les mauvaises configurations de sécurité sont en effet considérées comme l'une des vulnérabilités les plus courantes et les plus dangereuses.

Mission n°2 : Effectuer des scans de vulnérabilités

Avant d'installer un programme de gestion des vulnérabilités, le hacker éthique va tout d'abord cartographier tous les réseaux de l'entreprise et les classer par importance.

Les scans de vulnérabilités permettent aux entreprises de vérifier la conformité de leurs réseaux et systèmes de sécurité. Les outils d'analyse des vulnérabilités localisent avec précision les brèches ou les failles de sécurité qui peuvent être dangereuses pour les systèmes en cas d'attaque indirecte.

Les scans de vulnérabilité peuvent être effectués sur le périmètre et hors du périmètre réseau évalué.

Un scan interne identifie toute faille système qu'un cybercriminel pourrait exploiter sur différents systèmes s'il parvenait, d'une manière ou d'une autre, à accéder à un réseau local.

Un scan externe analyse l'exposition d'un réseau aux serveurs et applications de tiers directement accessibles à partir d'Internet.

Parmi les exemples de vulnérabilités logicielles courantes, citons l'injection SQL, les injections de données manquantes, une faiblesse dans la protection du pare-feu et les scripts inter sites (XSS).

Mission n°3 : Empêcher l'exposition de données sensibles

L'exposition des données dites sensibles de l'entreprise (coordonnées bancaires, mots de passe, coordonnées clients, etc.) peut engendrer des pertes importantes, en matière de données, auxquelles s'ajoutent d'autres conséquences pour l'entreprise, telles que des sanctions financières pour non-respect de la vie privée ou encore des pertes de revenus.

Les hackers éthiques réalisent des tests d'intrusion pour identifier ces types de failles et déterminer les vulnérabilités afin de documenter le mode opératoire de potentielles attaques.

Pour éviter que leurs données ne soient exposées, les entreprises peuvent se protéger avec des certificats SSL/TLS. Elles peuvent également mettre à jour leurs algorithmes de chiffrement, désactiver les caches sur les formulaires et chiffrer les données pendant et après un transfert de fichiers.

Mission n°4: Vérifier les failles d'authentification

Si l'authentification du site web de l'entreprise est compromise, des attaquants peuvent facilement récupérer des mots de passe, des cookies de session et d'autres informations liées aux comptes utilisateurs. Ces informations peuvent leur servir ultérieurement à prendre une fausse identité.

D'après une étude, près d'un tiers des vulnérabilités liées à des failles d'authentification résultent d'une mauvaise conception et d'une incapacité à limiter correctement le nombre de tentatives d'authentification.

Les hackers éthiques peuvent alors vérifier la gestion des systèmes d'authentification et suggérer les mesures de sécurité à prendre afin de protéger l'entreprise. Ils peuvent par exemple recommander de :

Contrôler la durée de session du site web de l'entreprise et déconnecter les utilisateurs après une période définie afin de prévenir le risque de détournement de session

Mettre en place un certificat d'appareils IOT pour sécuriser l'authentification, le chiffrement et l'intégrité des données et pour protéger les équipements tout au long de leur cycle de vie

Eviter d'utiliser des identifiants de session dans une URL pour ne pas se faire pirater les cookies de session

L'utilisation d'un bon VPN sécurisé est également préconisée pour que les utilisateurs puissent transférer des données d'un serveur à un autre sur un réseau privé. En chiffrant les données partagées, le VPN empêche les attaques sur la gestion des sessions.

13 INGÉNIEUR·E EN CYBERSÉCURITÉ

Niveau d'études : Bac+5

Spé Conseillée : Maths ou NSI

Employabilité : Très Bonne

Salaire débutant : 3 000 €

Code ROME : M1802 - Code FAP : M2Z

L'INGÉNIEUR CYBERSÉCURITÉ EST CHARGÉ D'ANALYSER ET DE TRAITER LES MENACES D'INTRUSION QUI VISENT LE SI DE L'ENTREPRISE. CE PRO DE LA SÉCURITÉ DÉFINIT LES PLANS D'ACTIONS NÉCESSAIRES À LA CORRECTION OU LA PRÉVENTION DES MENACES.

Salaire

La rémunération d'un ingénieur cybersécurité varie en fonction de la taille de l'entreprise qui l'emploie, de son expérience et du lieu de travail. Il y aura une certaine différence entre Paris, Lyon, Londres ou New York.En moyenne, un ingénieur cybersécurité débutant qui exerce en France touchera 3 000 euros par mois contre 5 000 euros pour un profil sénior. En Suisse, les postes de niveau débutant commencent avec un salaire environnant 44 000 CHF par an, tandis que les travailleurs les plus expérimentés peuvent percevoir jusqu'à 162 000 CHF.

Évolution de carrière

Au vu de la hausse et de la diversité des menaces cybercriminelles, l'ingénieur cybersécurité devient un professionnel de plus en plus recherché en entreprise.

L'ingénieur cybersécurité est généralement rattaché au directeur technique (CTO) voire au responsable de la sécurité des systèmes d'information (RSSI).

Il pourra donc évoluer vers un poste de management et d'encadrement d'équipe, au sein d'un SOC par exemple.

Où travailler ?

L'ingénieur cybersécurité peut exercer dans des secteurs d'activité variés. Cela va de la défense au numérique, des télécommunications au service public en passant par la banque ou le secteur des mutuelles. La croissance continue de la cybersécurité fait que les opportunités d'emploi sont nombreuses et ce, un peu n'importe où finalement.

Avantages et inconvénients

Supervision et administration des systèmes informatiques, analyse des menaces, veille, sensibilisation des équipes... Le métier d'ingénieur cybersécurité est une profession complète qui donne l'occasion, pour qui apprécie les challenges, de tenir de sérieuses responsabilités.

Le métier est exigeant, il faut savoir se mettre au niveau rapidement, réaliser un travail de veille important et constant car les technologies et les vulnérabilités changent aussi vite que les missions de l'ingénieur cybersécurité.

Compétences

Exercer comme ingénieur cybersécurité demande des compétences multiples et étendues.

Il est indispensable de posséder de bonnes connaissances générales dans le domaine de la sécurité des systèmes d'information, afin de pouvoir les appréhender dans toute leur complexité.

Au niveau technique, des bases en développement logiciel sont utiles, ainsi qu'une très bonne maîtrise des langages de scripts (Python, Perl, C ...).

Les entreprises demandent très souvent d'avoir travaillé avec des OS Windows et Linux, ainsi que des outils d'analyse de protocoles réseaux, par exemple Wireshark.

Enfin, il est fortement conseillé aux ingénieurs en cybersécurité de disposer d'une certaine adaptabilité compte-tenu des évolutions technologiques rapides.

Enfin, l'ingénieur cybersécurité doit savoir communiquer et gérer le travail en équipe.

Freelance

Faire le choix d'évoluer en tant qu'ingénieur cybersécurité freelance est une option. Il faudra avoir un statut afin de pouvoir facturer ses prestations, mais cela n'est qu'une formalité. Le plus dur peut-être est de devoir trouver des clients, notamment les premiers, ceux qui vous mettent le pied à l'étrier. Pour cela, rien de tel que de solliciter son réseau. Une bonne première étape. L'idéal pour évoluer en indépendant, c'est d'avoir eu une expérience avant en entreprise. Ce sera toujours un bon point à mettre en avant. De plus, cela crédibilisera votre profil aux yeux de clients futurs.

Le tarif journalier moyen d'un ingénieur cybersécurité freelance peut varier entre 300 et 1 200 euros, en fonction de ses expériences et références en entreprise.

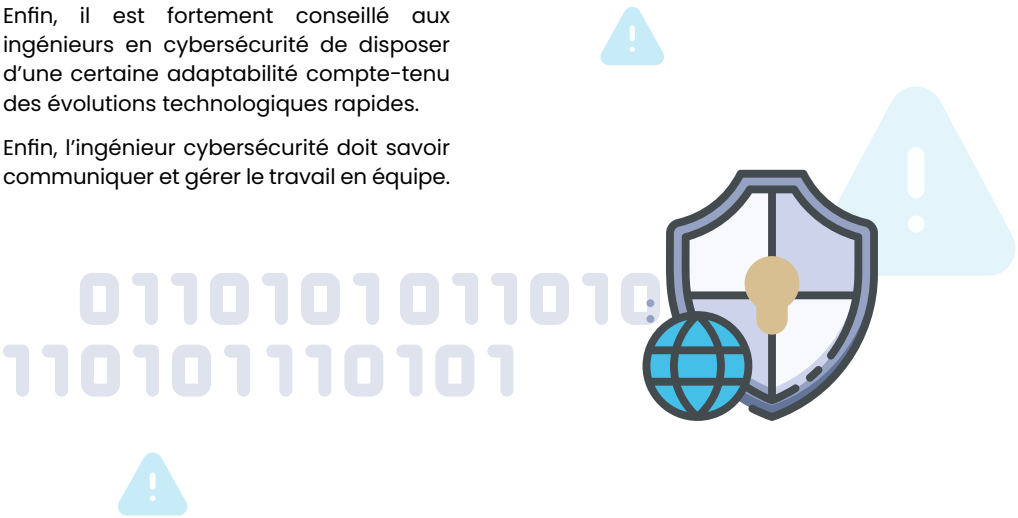
Études

Si l'objectif est de devenir ingénieur cybersécurité, il faut pouvoir alors se lancer dans plusieurs années d'étude afin d'atteindre un niveau Bac +5. Cela fera de vous un spécialiste en informatique, mais surtout un expert des enjeux cyber. Se former passe par une école spécialisée dans les métiers de la cybersécurité ou une école d'ingénieur.

A cela s'ajoute que certaines entreprises exigent des certifications en sécurité/ produit.

QUALITÉS

- Perfectionniste et organisé
- Rigoureux et méthodique
- Curieux
- Bon communiquant et capable de travailler en équipe



Missions

Le métier d'ingénieur sécurité informatique, également nommé expert sécurité des systèmes informatiques, ingénieur sécurité web ou encore ingénieur en cybersécurité, consiste globalement à assurer la sécurité des systèmes informatiques de sa propre entreprise – ou celle au sein de laquelle il intervient – et à traquer les éventuelles failles sur les réseaux internes et externes.

L'ingénieur cybersécurité doit empêcher les intrusions afin d'éviter que des pirates informatiques exploitent une faille présente sur l'architecture réseau de l'entreprise.

Sa mission première est de faire un audit permanent du niveau de sécurité des systèmes informatiques, des applications web ou de tout autre point d'entrée pouvant provoquer une attaque.

Il doit élaborer des plans d'actions très précis en cas d'attaque.

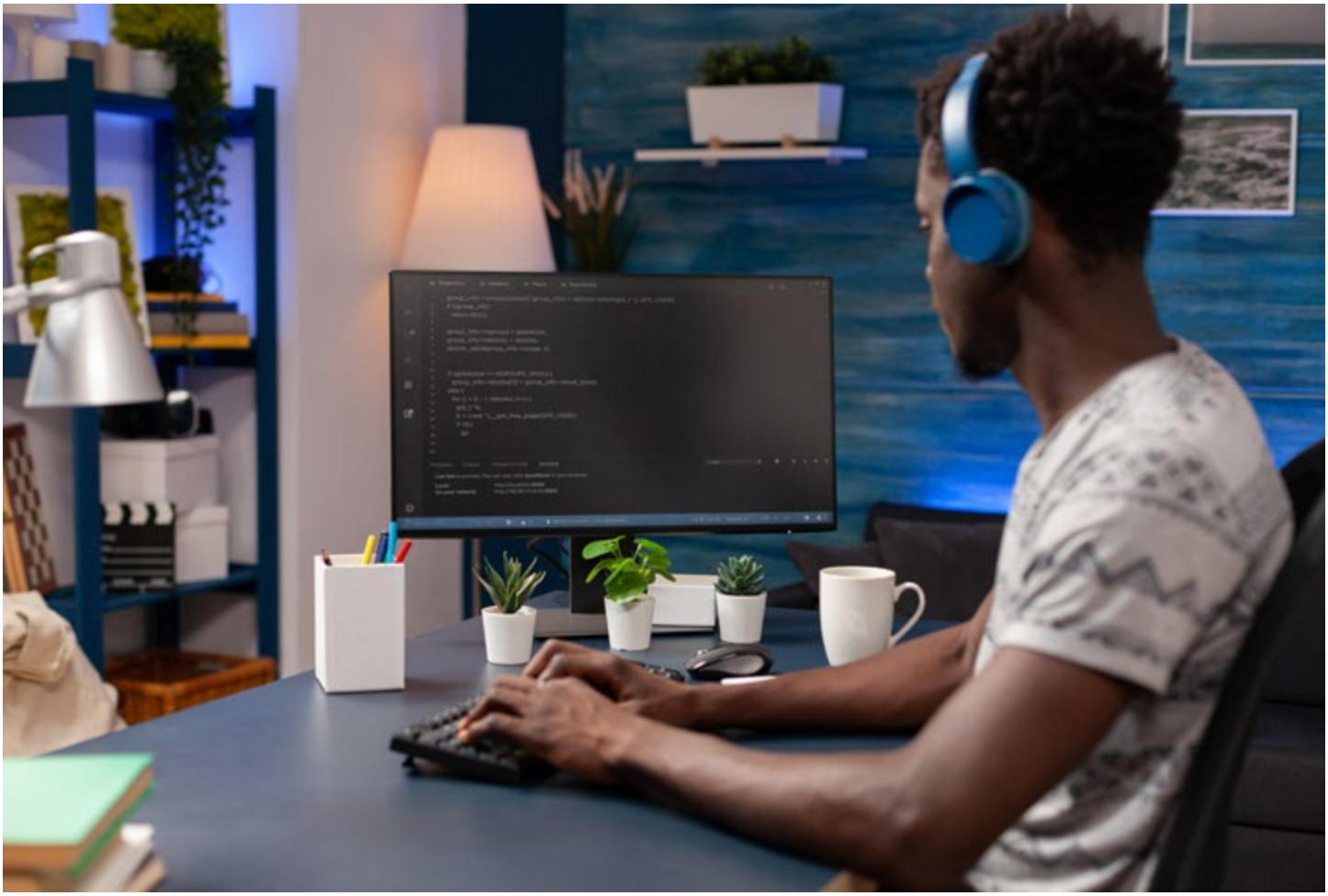
Il doit prévenir de potentielles attaques informatiques en assurant une protection maximale sur différents supports informatiques et applications. Il doit identifier les sources de potentielles attaques, leurs mécanismes et bloquer leur accès aux solutions existantes.

L'ingénieur cybersécurité participe à la définition des règles de sécurité applicatives en réponse aux exigences fixées par des référentiels de bonnes pratiques ou par des réglementations propres à l'activité de l'entreprise.

Il rédige des procédures de sécurité adaptées. En effet, l'ingénieur cybersécurité est un acteur majeur dans la sensibilisation aux enjeux de la sécurité. Pour cela, il doit réaliser et diffuser des supports de formation à l'attention de différentes équipes métiers.

Il aide et oriente les équipes techniques pour sécuriser le réseau et les systèmes informatiques.

Il doit assurer une veille sur les menaces actuelles. Ainsi, il documente les bases de connaissances et les procédures techniques réglementaires. Il doit être en mesure de suivre la vulnérabilité software et hardware. Plus précisément, il prévoit et contre la violation de données sensibles.



14

INTÉGRATEUR·RICE DE SOLUTIONS

Niveau d'études : Bac+3

Spé Conseillée : Maths ou NSI

Employabilité : Très Bonne

Salaire débutant : 2 000 €

Code ROME : M1802 - Code FAP : M2Z

L'INTÉGRATEUR DE SOLUTIONS DE SÉCURITÉ INTÈGRE DANS L'ENVIRONNEMENT DE PRODUCTION INFORMATIQUE LA SOLUTION DE SÉCURITÉ LA PLUS ADAPTÉE POUR L'ENTREPRISE.

Missions

L'intégrateur de solutions de sécurité participe à la conception et à l'intégration de la solution la plus adaptée à l'architecture système de l'entreprise.

Maintenance et Gestion :

· Assure la supervision des services, assurer la métrologie, gère les alertes et les incidents de production
· Préconise les montées de versions de la solution
· Pratique une veille sur les vulnérabilités

Conseil :

· Conseille sur le paramétrage de la solution de sécurité
· Délivre des formations sur la nouvelle solution de sécurité
· Assure une veille technologique dans le domaine de la sécurité informatique

Conception :

· Définit sous la responsabilité du responsable de projet, l'architecture fonctionnelle et technique du SI
· Assemble et intègre les différents composants
· Définit les interfaces et détermine les composants à faire évoluer pour permettre leur intégration
· Intègre la solution de sécurité dans l'environnement de production
· Contribue à la définition de l'architecture technique cible
· Met en œuvre les phases de test
· Met en production
· Réalise le paramétrage de la solution de sécurité

Compétences

Exercer comme intégrateur de solutions de sécurité informatique demande une triple compétence, à la croisée de la gestion de projet, de la sécurité informatique et de la cybersécurité :

· Maîtrise du système d'information, de l'urbanisation et de l'architecture du SI
· Gestion de projets et de portefeuille de projets
· Connaissances des solutions de sécurité du marché
· Configuration des outils liés à la sécurité
· Contribution des architectures à la sécurité : conception et modèles
· Contribution des architectures à la sécurité : intégration des systèmes

Salaire

La rémunération d'un intégrateur de solutions de sécurité varie en fonction de la taille et du profil de l'entreprise qui l'emploie.

En moyenne, un intégrateur de solutions de sécurité débutant qui exerce en France touchera 35 000 euros annuels contre 47 000 euros pour un profil sénior.

Où travailler ?

L'intégrateur de solutions de sécurité peut exercer dans divers types d'organisations et ce quelque soit le secteur d'activité comme par exemple :

· Les éditeurs de logiciels et entreprises informatiques
· La banque et les assurances
· Les télécommunications
· La santé

Freelance

L'intégrateur de solutions de sécurité peut exercer en tant que freelance. Le tarif journalier moyen qu'il peut proposer varie entre 600 et 1 200 euros, en fonction de ses expériences et références en entreprise.

Avant d'en arriver là, il est nécessaire de créer son entreprise, de se faire connaître ou tout simplement de solliciter son réseau. Devenir indépendant, c'est choisir la liberté, mais c'est aussi répondre à une exigence importante afin d'atteindre l'objectif final défini par le client. Rigueur, compétence et organisation sont fondamentaux.

Évolution de carrière

Aux vues de la hausse et de la diversité des menaces cybercriminelles, l'intégrateur de solutions de sécurité est un professionnel indispensable à l'entreprise.

Il pourra exercer en tant que responsable des systèmes d'information (RSSI) après avoir fait ses preuves plusieurs années en tant qu'intégrateur de solutions de sécurité.

Avantages et inconvénients

Si vous aimez le développement informatique mais souhaitez aussi vous impliquer sur la stratégie relative au choix des solutions de sécurité informatique de l'entreprise, le poste d'intégrateur de solutions de sécurité devrait vous combler.

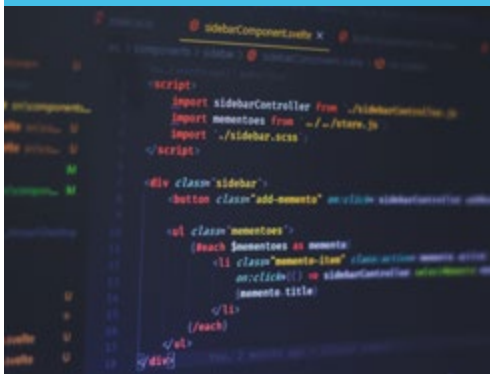
Le métier est exigeant, il faut savoir se mettre au niveau rapidement, réaliser un travail de veille important et constant car les technologies et les vulnérabilités changent aussi vite que les missions de l'intégrateur de solutions de sécurité.

Études

Pour devenir intégrateur de solutions de sécurité, il faudra partir sur une formation de niveau Bac+ 3 à Bac+ 5 avec une spécialisation en cybersécurité. Il s'agit de la voie la plus adaptée qui offrira la meilleure combinaison pour travailler à ce poste. Une école des métiers de la cybersécurité ou une faculté peuvent vous permettre d'y accéder. Il vous sera demandé 2 à 5 ans d'expérience dans le domaine de la sécurité des systèmes d'information.

QUALITÉS

· Rigueur
· Autonomie
· Bonne communication
· Bon relationnel
· Efficacité et pragmatisme
· Anticipation
· Réactivité et disponibilité en cas de problème
· Capacité à travailler en transverse au sein de l'organisation et en équipe
· Rigueur
· Capacité à définir des procédures



Niveau d'études : Bac+5

Spé Conseillée : Maths ou NSI

Employabilité : Très Bonne

Salaire débutant : 3 000 €

Code ROME : M1802 - Code FAP : M2Z

PROFESSIONNEL DE LA CYBERSÉCURITÉ, LE PENTESTER CONTRÔLE LA SÉCURITÉ DES RÉSEAUX INFORMATIQUES EN OPÉRANT DES TESTS D'INTRUSION OU "PENETRATION TEST" EN ANGLAIS, D'OÙ L'INTITULÉ DE SON MÉTIER.

Missions

Les entreprises de plus en plus sujettes aux cybermenaces doivent se doter d'experts en cybersécurité capables de raisonner de la même manière que leurs potentiels attaquants, ceci afin de limiter et anticiper au maximum les failles et intrusions malveillantes dans leur système informatique.

Le pentester est ce professionnel de la sécurité informatique dont la mission consiste à infiltrer «volontairement» un réseau ou une application informatique afin d'en évaluer le niveau de sécurité.

Son approche s'apparente à celle du pirate informatique, utilisant les mêmes techniques et approches que le hacker malveillant, mais en les détournant au bénéfice de l'entreprise. Le pentester réalise des tests d'intrusion pour vérifier la sécurité informatique de l'entreprise.

Le pentester va ainsi effectuer des tests d'intrusion pour vérifier la sécurité informatique de l'entreprise et fournir des solutions pour réduire la vulnérabilité des systèmes.

Enfin, les missions du pentester peuvent aller au-delà d'un test d'intrusion de système informatique. Elles peuvent concerner la totalité des équipements dont dispose son terrain d'intervention au sein de l'entreprise. Ainsi, le pentester pourra également réaliser des audits complets pour l'entreprise.

Tests d'intrusion

Un test d'intrusion, ou test de pénétration, ou encore pentest, est une méthode qui consiste à analyser une cible en se mettant dans la peau d'un attaquant.

Cette cible peut être une IP, une application, un serveur web, ou un réseau complet.

Le scan de vulnérabilité, différent du test d'intrusion, est en fait une composante du test d'intrusion, c'est-à-dire une sous-partie. C'est plus précisément un scan de la cible qui permet d'énumérer les vulnérabilités, sans tenter de les qualifier ou de vérifier si elles sont exploitables.

Les tests d'intrusion ont des objectifs clairs :

· Identifier les vulnérabilités du SI ou de son application
· Évaluer le degré de risque de chaque faille identifiée
· Proposer des correctifs de manière priorisée

Grâce au test d'intrusion, le pentester peut qualifier la sévérité de la vulnérabilité, la complexité de la correction, et l'ordre de priorité qu'il faut donner aux corrections.

Afin de sécuriser l'infrastructure ou l'application, les tests d'intrusion peuvent être réalisés à différents moments de la vie d'une entreprise. Ainsi, ces derniers peuvent être initiés lors de la conception du projet, afin d'anticiper les éventuelles attaques, pendant la phase d'utilisation, à intervalle régulier et enfin, suite à une cyberattaque afin que celle-ci ne se reproduise plus .

Le test d'intrusion peut se faire de l'extérieur (test d'intrusion externe). Ce test d'intrusion pourra être réalisé de n'importe quelle connexion Internet.

Le test d'intrusion peut également se faire de l'intérieur de l'infrastructure (test d'intrusion interne). Dans ce cas, le test sera opéré sur le LAN (réseau interne de l'entreprise).

Grâce à ces dispositions, le pentester évalue les failles et essaye d'attaquer le système. Les systèmes de défense à savoir l'antivirus et les firewalls sont contournés par les outils mis en avant pour l'intrusion.

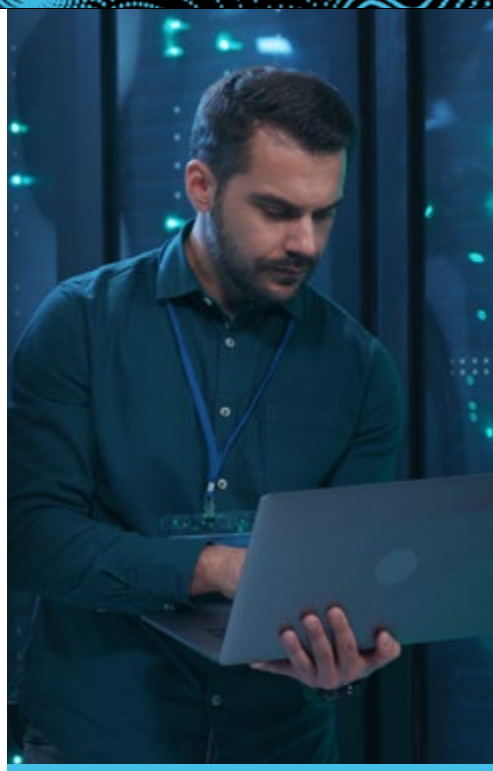
Enfin, les missions du pentester peuvent aller au-delà d'un test d'intrusion de système informatique. Elles peuvent concerner la totalité des équipements dont dispose son terrain d'intervention au sein de l'entreprise. Ainsi, le pentester pourra également réaliser des audits complets pour l'entreprise. Il en existe plusieurs types :

· Audits de code : le code source d'une application est analysé afin de relever toute faille de sécurité.
· Audits de configuration : la configuration d'un système ou d'un équipement réseau est fournie au pentester qui compare ensuite ces données à des référentiels officiels (CIS, guides de l'ANSSI…) pour relever tout écart de conformité.
· Audits d'architecture : le pentester vérifie la robustesse de l'architecture d'un système d'information face à différentes menaces. Cela est réalisé à partir des documents d'architecture client et d'entretiens.
· Audit organisationnel : le pentester vérifie l'organisation mise en place par le client d'un point de vue sécurité, de la création d'une équipe dédiée à la gestion des incidents, à partir des documents disponibles et des entretiens avec le client.

Études

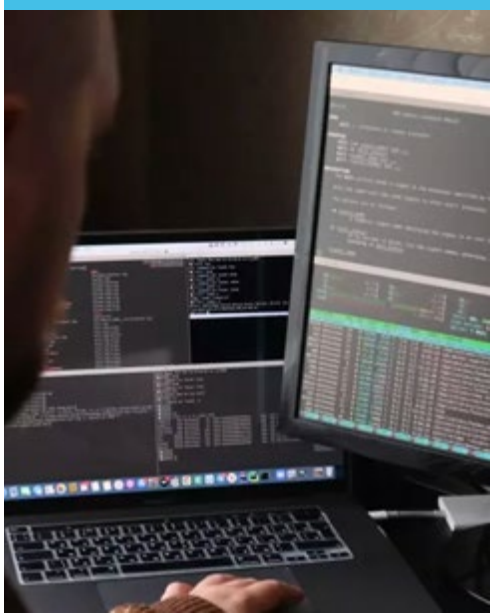
Pour devenir pentester, vous devrez justifier d'un diplôme en informatique de niveau Bac +3 à 5 avec une spécialisation en cybersécurité. Une école dans les métiers de la cybersécurité le permet. Des certifications en sécurité/produit seront demandées parfois.

A savoir que certains pentesters se sont formés en autodidactes puisqu'il s'agit d'un nouveau métier qui passionne les génies de l'informatique. D'ailleurs, des hackers pirates (dans l'illégalité) ont choisi de retrouver « le droit chemin » en devenant pentester au sein de grands groupes et sociétés.



QUALITÉS

· Ethique et légal
· Curieux
· Dynamique
· Réactif
· Créatif
· Disponibile
· Faire preuve de confidentialité
· Aimer le travail en équipe
· Avoir le goût du défi



Compétences

Exercer comme pentester demande des compétences nombreuses et étendues :

· Capacité de compréhension des menaces cybersécurité
· Capacité à exploiter des sources ouvertes de manière sécurisée
· Mise en place de plans de veille sur un ou plusieurs secteurs déterminés
· Détection, qualification et analyse d'informations pertinentes
· Connaître le droit et les réglementations en vigueur en matière de cybersécurité

A cette base théorique, il faut ajouter de très nombreuses connaissances pratiques qui ne peuvent s'acquérir que par l'expérience. Un bon moyen de commencer consiste à participer à des événements tels que « Capture the flag », où l'objectif est de trouver et d'exploiter les vulnérabilités d'un système afin de s'y introduire.

Salaire

La rémunération d'un pentester varie en fonction de la taille de l'entreprise qui l'emploie, de son expérience et du lieu de travail.

En moyenne, un étant débutant en France, il touchera 3 000 euros par mois et peut voir son salaire à plus de 5 000 euros en tant que sénior.

Aux États-Unis, le salaire annuel moyen d'un pentester avoisine les 110 000 dollars.

Où travailler ?

Le pentester peut exercer dans divers secteurs industriels, de services ou encore dans le secteur public. Il peut aussi évoluer dans les secteur suivants :

· Logiciel, informatique et numérique
· Bancaire
· Télécommunications
· Santé

Évolution de carrière

Aux vues de la hausse et de la diversité des menaces cybercriminelles, le pentester devient un expert de plus en plus recherché en entreprise.

En France, les pentesters sont souvent, à la base, des experts en systèmes d'information ou des experts sécurité et réseaux formés par la suite en cybercriminalité. Néanmoins, des formations dédiées au métier de pentester se développent de plus en plus et laissent entendre que le métier a de beaux jours devant lui.

Le pentester et le hacker éthique semblent être étroitement liés de part leurs missions et les deux termes sont souvent utilisés de façon interchangeable . Pourtant, les deux métiers présentent quelques différences.

Ainsi, le pentester met beaucoup plus l'accent sur les étapes ou les processus permettant de trouver des failles de sécurité sur un système d'information alors que le hacker éthique va plus loin et essaie d'améliorer la sécurité du système cible.

Freelance

Le pentester peut exercer en tant que freelance. Le tarif journalier moyen peut alors varier de 400 à 1 500 euros, en fonction de ses expériences et références en entreprise. Choisir ce statut, c'est être conscient des enjeux qui reposent sur vos épaules puisque vous devrez maîtriser le sujet, faire preuve de rigueur, d'organisation et d'un sens de la communication. Tout le monde ne peut ainsi pas devenir indépendant.

Avantages et inconvénients

Si vous aimez les puzzles, les casse-têtes et autres challenges, faire du pentest votre métier sera pour vous tout sauf ennuyant !

Néanmoins, sachez que le pentester, contrairement à l'imaginaire collectif qui gravite autour de son métier, n'est pas un geek solitaire et insociable.

C'est avant tout un consultant qui doit s'adapter à son auditoire en vulgarisant parfois, et qui doit savoir s'exprimer aussi bien à l'oral qu'à l'écrit . Il ne faut donc pas avoir peur de s'exprimer auprès de cibles variées, direction, équipes, clients, etc.

Le métier est exigeant, il faut savoir se mettre au niveau rapidement, réaliser un travail de veille important et constant car les technologies et les vulnérabilités évoluent aussi vite que les missions du pentester.

RESPONSABLE CSIRT/CERT

Niveau d'études : Bac+5

Spé Conseillée : Maths ou NSI

Employabilité : Bonne

Salaire débutant : 4 000 €

Code ROME : M1802 - Code FAP : M2Z

VOUS AVEZ L'AMBITION DE DIRIGER DES ÉQUIPES ET DE PILOTER DES PROJETS D'ENVERGURE ? ÊTES EN MESURE DE GÉRER DES SITUATIONS DE CRISE ET ÊTES CAPABLE DE RÉSISTER À LA PRESSION ? VOUS SOUHAITEZ INTÉGRER UN RÉSEAU D'EXPERTS RÉUNIS AUTOUR D'UN BUT COMMUN : LA LUTTE POUR LA CYBERDÉFENSE ? DEVENEZ RESPONSABLE DU CSIRT.

Avantages et inconvénients

Le responsable du CSIRT est un expert de la cybersécurité qui doit convoquer quotidiennement l'ensemble des ces compétences en cybersécurité (technique, veille, prospective) dans ses responsabilités. C'est donc un métier complet.

En retour, c'est une profession réservée aux profils qui savent manager et faire face à la pression.

Freelance

Il est plutôt rare de voir un responsable du CSIRT exercer en freelance dans la mesure où il doit être rattaché à un CSIRT. Si ce statut pourrait se généraliser dans les années à venir, il faudrait pour cela créer un statut d'entreprise afin d'établir devis et factures à des clients. Détermination, organisation, rigueur et professionnalisme seront aussi quatre inconditionnels pour travailler de cette manière. Posséder un réseau est également un plus.

Études

Pour devenir responsable du CSIRT, vous devrez justifier d'un diplôme en informatique de type Bac + 5. L'idéal étant de faire le choix d'une spécialisation en cybersécurité incluant une forte composante en systèmes et réseaux.

Les entreprises recherchent bien souvent un profil avec de l'expérience. Concrètement, cinq ans au sein d'un CSIRT seront utiles pour postuler à la fonction de responsable du CSIRT. Autrement dit, on ne le devient pas du jour au lendemain.

Où travailler ?

Les CSIRT sont un réseau international, composé d'entreprises et d'institutions de tailles et profils très variés.

Liste des CSIRT ou CERT en France :

· CERT gouvernemental : CERT-FR (anciennement CERTA appartenant à l'ANSSI / SGDSN) est le CERT affecté au secteur de l'administration française
· Ai CERT : privé interne au Groupe Airbus
· AlliaCERT : CERT de la société Alliacom ouvert à l'ensemble des entreprises et des institutions
· AXA CERT : privé interne au Groupe AXA
· CERT-AKAOMA : CSIRT de la société AKAOMA proposant des services de cyber-surveillance et de réponse aux incidents de sécurité à l'ensemble des entreprises et institutions
· CERT-AlgoSecure : CSIRT privé de la société AlgoSecure ouvert à l'ensemble des entreprises et des institutions
· CERT-AG : CERT du Groupe Crédit Agricole et des filiales
· CERT-AMOSSYS : société AMOSSYS
· CERT-AREVA : groupe AREVA
· CERT-BDF : CERT de la Banque de France

Comment le devenir ?

Le responsable du CSIRT coordonne une équipe de réponse aux incidents de sécurité ciblant les systèmes d'information de l'organisation. Il s'assure de la bonne exécution des investigations et de la coordination des parties prenantes lors d'un incident de sécurité. Le métier est accessible avec l'obtention d'un diplôme en informatique de niveau Bac +5 comprenant une spécialisation en cybersécurité et une forte composante en systèmes et réseaux. Une expérience professionnelle de 5 ans minimum au sein d'un CSIRT sera exigée avant de pouvoir en prendre la responsabilité. Le salaire médian d'un responsable CSIRT en France est de minimum 50 000 euros par an.

Les tendances et facteurs d'évolution du métier indiquent qu'il peut prendre d'autres responsabilités en devant par exemple RSSI.

Compétences

Exercer comme responsable du CSIRT demande de solides compétences informatiques et des connaissances pointues en cybersécurité et cyberdéfense telles que :

· Maîtrise du système d'information, de l'urbanisation et de l'architecture du SI
· Analyse post-mortem (forensic) : connaissance des outils d'analyse et des procédures légales
· Cyberdéfense : pratique de l'analyse de journaux (systèmes ou applicatifs), de flux réseaux, connaissance des techniques d'attaques et d'intrusions et des vulnérabilités des environnements
· Scripting

Salaire

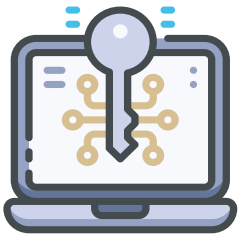
La rémunération d'un responsable du CSIRT varie selon le CSIRT au sein duquel il intervient.

Le salaire médian pour les responsables de CSIRT en France est de minimum 50 000 euros par an lors d'une prise de poste.

Un profil senior ou expert pourra prétendre à un salaire allant jusqu'à 80 000 euros annuels.

Évolution de carrière

Les tendances et facteurs d'évolution du métier indiquent que le responsable du CSIRT peut être amené à contribuer à la gestion d'incidents liés à d'autres raisons que la sécurité des SI, comme par exemple la fraude via des moyens informatiques. Il peut également devenir directeur cybersécurité ou encore RSSI.



QUALITÉS

· Restitution/vulgarisation pour des publics non techniques
· Savoir rédiger des rapports adaptés à différents niveaux d'interlocuteurs
· Savoir travailler en équipe
· Avoir la capacité à résister à la pression
· Avoir le sens de l'éthique

Missions

Dans un monde où les réseaux globaux prennent toujours plus d'expansion et une importance stratégique qui ne se dément pas, les systèmes d'information d'une organisation doivent pouvoir résister aux différentes menaces qui pèsent sur eux.

Pour sécuriser leurs systèmes et leurs réseaux, les organisations doivent pouvoir compter sur des gestionnaires capables de reconnaître les menaces et les vulnérabilités des systèmes existants et d'assurer la conception et le développement de systèmes sécuritaires.

C'est le propre de la mission du responsable du CSIRT.

Voici le détail des ses activités et tâches au quotidien.

Pilotage des opérations :

· Planifier et organiser les opérations quotidiennes du CSIRT
· Assurer un appui opérationnel à la gestion de crise de sécurité en cas d'incidents de sécurité majeurs
· Organiser les modes de fonctionnement avec le SOC (Security Operation Center) interne ou externe pour assurer la gestion des incidents de sécurité

Anticipation :

· S'appuyer sur les services de veille sur les menaces (threat intelligence) pour tenir compte des groupes d'attaquants existants, de leurs méthodes d'attaques et de leurs motivations
· Informer les équipes en charge de la sécurité des nouvelles menaces importantes et recommander des mesures tactiques pour les contrer
· Construire et maintenir des relations de confiance et d'échange avec les réseaux de CSIRT français et étrangers ainsi qu'avec les organismes gouvernementaux
· Participer aux exercices de préparation à la gestion de crise de cybersécurité

Réponse à incident :

· Élaborer et tenir à jour le processus d'intervention en cas d'incident majeur de sécurité ainsi que toutes les ressources nécessaires (outillage, procédure, etc.) ; vérifier que les prérequis techniques et documentaires sont en place et tenus à jour
· S'assurer que les parties prenantes connaissent leur rôle dans la gestion des incidents de sécurité
· S'assurer de la bonne exécution du processus de réponse à incident depuis la détection jusqu'à la résolution de l'incident ; suivre et coordonner les actions de remédiation
· Organiser les retours d'expérience concernant les incidents pour capitaliser et définir des actions d'amélioration

17 RESPONSABLE DU SOC

Niveau d'études : Bac+5

Spé Conseillée : Maths ou NSI

Employabilité : Très Bonne

Salaire débutant : 3 500 €

Code ROME : M1802 - Code FAP : M2Z

LE RESPONSABLE DU SOC (SECURITY OPERATION CENTER) PLANIFIE ET ORGANISE LES OPÉRATIONS QUOTIDIENNES AFIN D'ÉVALUER LES RISQUES DE VULNÉRABILITÉ DU SYSTÈME INFORMATIQUE ET DE DÉTECTER LES POTENTIELLES ATTAQUES.

Salaire

À l'heure où le sujet de la cybersécurité touche toutes les sphères professionnelles, les entreprises sont de plus en plus nombreuses à se doter d'un SOC afin de pouvoir suivre et analyser en continu les risques et menaces potentiels de sécurité.

En France, le responsable du SOC en début de carrière touche en moyenne entre 3 000 et 3 500 euros brut mensuels. Expérimenté, il peut être rémunéré jusqu'à 60 000 euros brut annuels. À l'international, au R.-U. par exemple, un RSOC peut gagner jusqu'à 70 000 £.

Où travailler ?

Le responsable du SOC peut travailler dans le secteur industriel, pour des sociétés de services ou encore dans le secteur public.

Voici des exemples :

· Editeurs de logiciels et entreprises informatiques
· Secteur bancaire
· Secteur des télécommunications
· Sociétés de conseil en hautes technologies

Freelance

Le responsable du SOC peut exercer en tant que freelance. Pour cela, il faut d'abord passer par la création d'une structure juridique (l'auto-entreprise est un bon début) puis ensuite il faudra commencer par démarcher ses futurs clients. Avoir de l'expérience dans le milieu est un vrai plus, gage de crédibilité et de maîtrise de compétences. Sans oublier qu'un haut niveau de rigueur, d'organisation et de gestion d'équipe sera exigé. Le tarif journalier moyen d'un responsable du SOC freelance peut varier entre 400 et 700 euros.

Missions

Le responsable du SOC assure la planification, la gestion et le suivi quotidiens des opérations.

C'est lui qui met en place le service de détection des incidents de sécurité et qui supervise toute la cellule. Il assure la bonne exécution des processus de supervision et de gestion des évènements de sécurité. Il établit le reporting complet et précis des indicateurs clés, et définit les axes d'améliorations des services.

Ce professionnel expert de la cybersécurité pilote et coordonne l'ensemble des experts du SOC composé d'analystes, d'ingénieurs en sécurité, ainsi que de managers supervisant les opérations de sécurité. Les équipes SOC travaillent étroitement avec les équipes d'intervention afin de s'assurer que le problème de sécurité soit bien réglé une fois qu'il a été découvert.

Dans le détail, les missions du responsable du SOC sont donc les suivantes :

· Planifier et organiser les opérations quotidiennes du SOC
· Assurer un appui opérationnel à la gestion de crise de sécurité en cas d'incidents de sécurité majeurs
· Assurer les relations avec les équipes de réponse à incidents CERT (Computer Emergency Response Team) ou CSIRT (Computer Security Incident Response Team), notamment en situation de crise pour coordonner les différentes équipes de sécurité opérationnelle
· Définir la stratégie du SOC, assurer la cohérence technique, prendre en compte les exigences réglementaires
· Définir et mettre en œuvre les outils du SOC pour la collecte des évènements, l'accès aux plateformes de sécurité, la recherche d'événements suspects, la gestion des alertes, les workflows de suivi d'incidents de sécurité
· Alimenter la stratégie de détection à partir d'une vision globale de la nature et du niveau de vulnérabilité du SI
· Définir les cas d'usages de détection et les intégrer dans les outils de détection
· Définir et mettre en place les processus de notification et d'escalade
· Évaluer et valider l'efficacité des outils déployés dans le SOC et conduire les plans d'action correctifs nécessaires le cas échéant
· Créer des synergies avec les autres équipes de sécurité en partageant les informations sur les menaces identifiées (en interne comme en externe)

Avantages et inconvénients

Faire sa carrière en tant que responsable du SOC, c'est choisir d'exercer un métier qui a du sens, puisque gérer le SOC signifie être est au cœur de la stratégie de cyberdéfense de l'entreprise. De plus, comme la majorité des métiers de la cybersécurité, il est facile de trouver un emploi à ce poste. Et le sera encore plus dans les années à venir.

Du côté des inconvénients, il est possible de citer la pression liée aux responsabilités du métier. En effet, il est important de savoir garder son sang-froid car le responsable du SOC est le capitaine du navire, celui qui tient la barre, pilote et déploie la stratégie du SOC auprès de ses équipes

Études

Pour devenir responsable du SOC, vous devrez avoir un diplôme de niveau Bac + 5.

Il est souhaité de préparer un Diplôme d'Ingénieur ou un Master 2 informatique avec une spécialité en sécurité des systèmes d'information Ou de'opter pour un MSc en école spécialisée dans les métiers de la cyber. Une expérience professionnelle de 5 ans au sein d'un SOC est souvent requise avant de pouvoir prétendre au poste de responsable du SOC.

QUALITÉS

· Capacité à travailler en équipe
· Capacité à définir des procédures
· Autonomie et organisation
· Capacité d'analyse et de synthèse
· Rigueur, sens de la méthode
· Qualité rédactionnelle
· Communication et expression orale

Compétences

Pour devenir responsable du SOC, il est indispensable de posséder un socle de compétences informatiques solides orientées cybersécurité. Il est également nécessaire de connaître le cadre réglementaire relatif à la sécurité informatique. Cela se traduit par :

· La sécurité des systèmes d'exploitation
· La sécurité des réseaux et protocoles
· La gestion de crise
· L'analyse de journaux (systèmes ou applicatifs)
· L'analyse de flux réseaux
· Les outils et de méthodes de corrélation de journaux d'événements (SIEM)
· Les solutions de supervision sécurité
· Les techniques d'attaques et d'intrusions
· Les vulnérabilités des environnements
· Le scripting

Comment le devenir ?

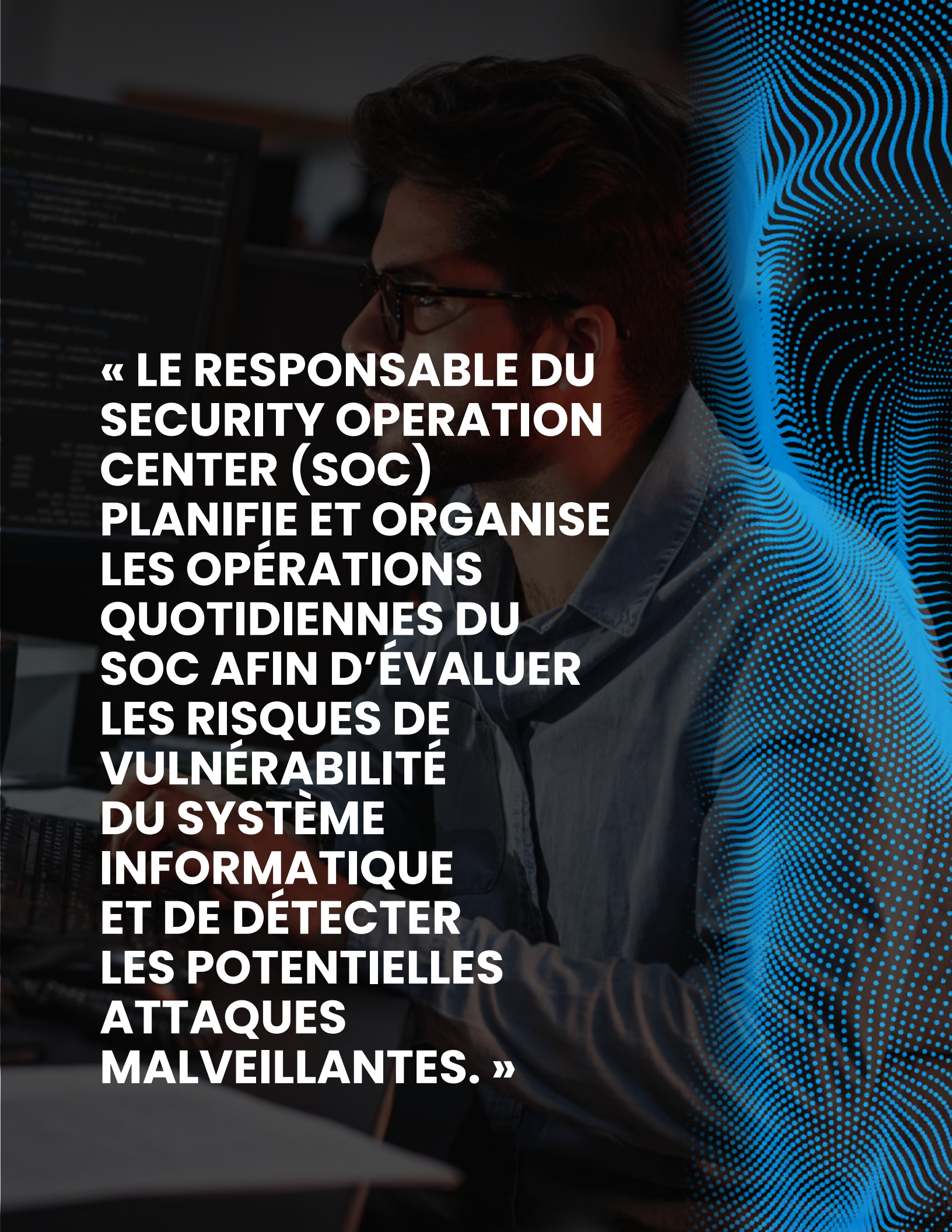
Pour devenir responsable du SOC, il est nécessaire de préparer un diplôme de niveau Bac +5 en informatique avec une spécialité en sécurité des systèmes d'information. Il faudra également justifier d'au moins 5 années d'expérience au sein d'un SOC avant d'en prendre la responsabilité. Le responsable du SOC devra faire preuve d'une grande rigueur et d'une bonne résistance au stress, car il a la responsabilité de la gestion et du suivi de tout un centre d'opération et de ses équipes.

A l'heure où le sujet de la cybersécurité touche toutes les sphères professionnelles, les entreprises sont de plus en plus nombreuses à se doter d'un SOC afin de pouvoir suivre et analyser en continu les risques et menaces potentiels de sécurité.

Évolution de carrière

La cybersécurité est devenue un élément stratégique pour toutes les organisations publiques et privées. Les entreprises sont de plus en plus nombreuses à se doter d'un dispositif de contrôle de la sécurité des données ou SOC.

Le responsable du SOC sera amené à gérer toujours plus d'incidents de sécurité et devra par conséquent développer une bonne compréhension des nouvelles menaces qui pèsent sur son périmètre. Pour suivre l'évolution des tendances, il pourra être amené à développer des compétences en machine learning et en threat intelligence afin de renforcer ses capacités de détection.



« LE RESPONSABLE DU SECURITY OPERATION CENTER (SOC) PLANIFIE ET ORGANISE LES OPÉRATIONS QUOTIDIENNES DU SOC AFIN D'ÉVALUER LES RISQUES DE VULNÉRABILITÉ DU SYSTÈME INFORMATIQUE ET DE DÉTECTER LES POTENTIELLES ATTAQUES MALVEILLANTES. »

18 RESPONSABLE DE LA SÉCURITÉ DES S.I. (RSSI)

Niveau d'études : Bac+5

Spé Conseillée : Maths ou NSI

Employabilité : Très Bonne

Salaire débutant : 5 800 €

Code ROME : M1802 - Code FAP : M2Z

LE OU LA RESPONSABLE SÉCURITÉ DES SYSTÈMES D'INFORMATION (RSSI) DÉFINIT ET DÉVELOPPE LA POLITIQUE DE SÉCURITÉ DE L'INFORMATION DE SON ENTREPRISE. IL EST GARANT DE SA MISE EN ŒUVRE ET EN ASSURE LE SUIVI.

Études

Pour devenir Responsable de la sécurité et des systèmes d'information, il est nécessaire de valider un Bac +5, via une école d'ingénieurs ou à l'université, avec une spécialisation en cybersécurité.

Il est indispensable de posséder une expérience professionnelle supérieure à 5 ans dans le domaine de la cybersécurité.

Freelance

Le RSSI peut exercer en tant que freelance. Il va falloir pour cela avoir quelques années d'expérience pour travailler à son compte et convaincre des structures de faire appel à vous. Avant toute chose, la première option consistera à créer un statut d'auto-entrepreneur ou une société individuelle. Il est également possible de rejoindre un cabinet d'experts en cybersécurité. Ensuite, votre rigueur, expertise et professionnalisme vous garantiront de pouvoir travailler sur des missions diverses. Le TJM d'un RSSI peut varier entre 700 et 1 200 euros.

Comment le devenir ?

Pour devenir RSSI, il est nécessaire de préparer un diplôme de niveau Bac +5 en informatique avec une spécialité en sécurité des systèmes d'information. Il faudra également justifier d'au moins 5 années d'expérience dans le domaine de la cybersécurité.

Le RSSI devra faire preuve d'une grande rigueur et d'une bonne résistance au stress car il a en gestion et en suivi tout ce qui se rapporte au système d'information de l'entreprise. Il devra aussi faire preuve de pédagogie et d'écoute.

Missions

Le responsable de la sécurité des systèmes d'information (RSSI) assure le pilotage de la démarche de cybersécurité sur un périmètre organisationnel et/ou géographique au sein de l'organisation. Il définit ou décline, selon la taille de l'organisation, la politique de sécurité des systèmes d'information (prévention, protection, détection, résilience, remédiation) et veille à son application.

Il assure un rôle de conseil, d'assistance, d'information, de formation et d'alerte, en particulier auprès des directeurs métiers et/ou de la direction de son périmètre.

Il s'assure de la mise en place des solutions et des processus opérationnels pour garantir la protection des données et le niveau de sécurité des systèmes d'information.

Selon la taille de l'organisation, il joue un rôle opérationnel dans la mise en œuvre de la politique de sécurité des SI ou encadre une équipe.

Les missions du Responsable de la sécurité des systèmes d'information sont nombreuses et variées :

Identifier :

· Décliner les axes et les objectifs stratégiques en matière de cybersécurité pour son périmètre et les faire valider par la direction compétente sur celui-ci
· Identifier les enjeux et les risques de sécurité majeurs sur son périmètre
· Décliner et maintenir la politique de sécurité des SI en collaboration avec les parties prenantes
· Définir un plan d'actions annuel ou pluriannuel sur son périmètre
· Définir une politique d'investissement au regard des objectifs de sécurité
· Contribuer à définir l'organisation de la cybersécurité au sein de son périmètre et l'animer
· Suivre les évolutions réglementaires et techniques de son domaine ; assurer les relations avec les acteurs de son secteur d'activité autour de la cybersécurité

Protéger :

· Organiser les structures de pilotage des plans d'actions de sécurité au sein des entités
· Définir les mesures organisationnelles et techniques à mettre en œuvre pour atteindre les objectifs de sécurité
· Assurer un support à la mise en œuvre en fournissant une assistance technique et méthodologique ainsi que des outils et services de sécurité, éventuellement à travers un catalogue de services
· Diffuser une culture SSI à destination des utilisateurs et décideurs
· Assurer la promotion des chartes de sécurité informatique sur son périmètre
· Évaluer le niveau de sécurité au sein de son périmètre, notamment à travers la réalisation d'audits périodiques et de contrôles permanents
· Contrôler que les politiques et règles de sécurité des SI sont appliquées sur son périmètre et vis-à-vis des tiers et sous-traitants (third parties)
· Contribuer à répondre aux sollicitations des prospects et des clients sur les aspects sécurité (notamment dans le cadre d'appels d'offres)
· Détecter :
· Prendre les mesures techniques et/ou organisationnelles permettant la surveillance des événements de sécurité, l'appréciation des incidents de sécurité et la réaction face aux attaques, assurer la mise en place d'un SOC (Security Operation Center)

Répondre :

· Veiller à ce que le dispositif de gestion de crise de sécurité soit opérationnel
· Contribuer au pilotage de la gestion des incidents et des crises de sécurité, le cas échéant en lien avec le CSIRT (Computer Security Incident Response Team)

Assurer la continuité et reconstruire :

· Préparer et mettre en œuvre un plan de continuité informatique, dans le cadre du plan de continuité des activités (PCA)
· Préparer et mettre en œuvre un plan de reprise informatique, dans le cadre du plan de reprise des activités (PRA)
· Proposer la stratégie de cyber-résilience

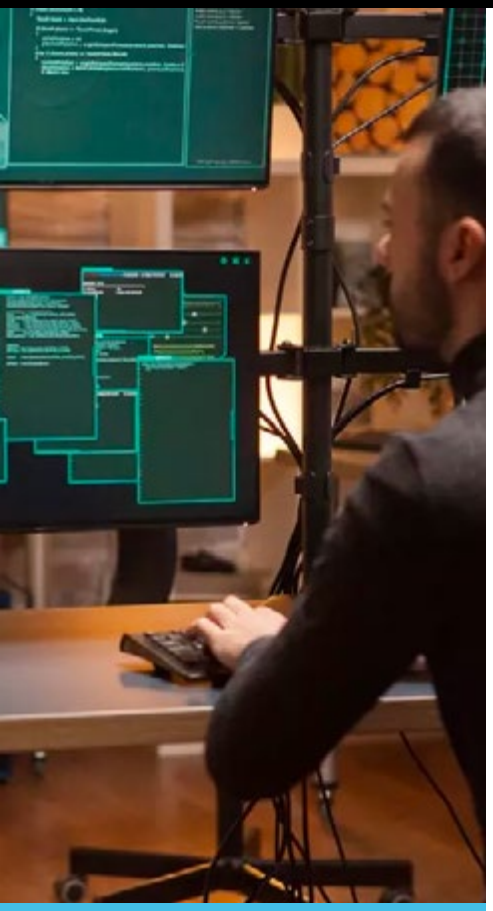
Rendre compte :

· Rapporter régulièrement auprès de sa hiérarchie sur le niveau de couverture courant des risques de sécurité SI
· Assurer un rôle de conseil auprès de sa hiérarchie et des métiers de son périmètre
· Représenter l'organisation dans les relations avec les autorités de régulation

L'AVIS DU PROFESSIONNEL

« Ce métier nécessite une remise en question permanente car il est nécessaire de s'adapter aux évolutions constantes de la menace mais aussi à l'évolution du périmètre de la structure à protéger. »

Cyril Bras
RSSI
GRENOBLE-ALPES MÉTROPOLE



QUALITÉS

· L'influence
· Avoir le sens de l'intérêt général
· Pouvoir manager des équipes
· Savoir restituer au management
· Savoir travailler en transverse au sein de l'organisation
· Résister à la pression
· S'appropriation des enjeux métiers

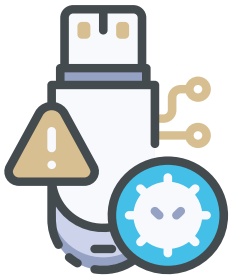
Compétences

Afin de définir et de mettre en œuvre la politique de sécurité, le Responsable de la sécurité informatique connaît la charte d'utilisation des systèmes informatiques et des systèmes de sécurité de son entreprise, ainsi que les différents processus en cas de problème.

Également, le RSSI possède des connaissances juridiques et réglementaires sur la sécurité informatique ainsi que sur d'autres domaines liés aux systèmes d'information. Il a notamment connaissance de nombreux points juridiques sur la confidentialité et la sécurité des utilisateurs, en particulier concernant la RGPD.

Ce travail nécessite l'élaboration de procédures et d'outils de sécurité informatique ainsi que la mise en place d'une démarche qualité. Pour sensibiliser les salariés, le Responsable de la sécurité des systèmes d'information peut avoir une expérience dans des domaines comme la communication. En voici le détail :

· Bonne connaissance des enjeux et des métiers de l'organisation
· Capacité à construire la stratégie cybersécurité de l'organisation
· Capacité de compréhension des menaces cybersécurité
· Connaissance du système d'information et des principes d'architecture
· Maîtrise des fondamentaux dans les principaux domaines de la SSI
· Connaissance des technologies de sécurité et des outils associés
· Gestion des risques, politique de cybersécurité et SMSI
· Connaissance juridique en matière de droit informatique lié à la sécurité des SI et à la protection des données
· Cyberdéfense : connaissances en gestion de crise
· Connaissance de la gouvernance, des normes et des standards dans le domaine de la sécurité : normes ISO (2700X), normes sectorielles (PCI-DSS…)



L'AVIS DU PROFESSIONNEL

« Le métier de RSSI, c'est 70 % d'organisationnel. On fait finalement assez peu de technique à moins d'avoir une double casquette infrastructure + RSSI. Pour la partie organisationnelle, les formations à l'analyse de risque sont importantes. Les savoir-faire qui en découlent sont de l'ordre de la communication : présenter ses résultats d'analyse, faire accepter les plans de remédiation et les évolutions organisationnelles ou techniques qui viseront à élever le niveau de sécurité, etc. »

RSSI D'UNE UNIVERSITÉ
SOUHAITANT RESTER ANONYME

L'AVIS DU PROFESSIONNEL

« Le numérique est de plus en plus présent, si la sécurité n'est pas intégrée dans les projets de la structure c'est à plus ou moins à long terme un risque qui, lorsqu'il se concrétise, à des impacts multiples sur l'image, la gouvernance, les finances. Dès lors, en tant que RSSI, vous devez encadrer les usages du numérique afin de garantir la conformité aux exigences réglementaires comme par exemple le RGPD, mais aussi protéger le patrimoine informationnel d'actions malveillantes. Vous devez par ailleurs sensibiliser le personnel aux enjeux de la cybersécurité en faisant du maillon humain un maillon robuste de la chaîne de défense. »

« C'est un métier exigeant qui nécessite d'une part de maintenir ses compétences à jour en assurant une veille permanente et d'autre part d'être en capacité de rendre accessible et compréhensible le sujet de la sécurité du numérique aux décideurs. »

Cyril Bras
RSSI
GRENOBLE-ALPES MÉTROPOLE

Évolution de carrière

Le périmètre d'un RSSI peut s'exercer sur différents domaines en fonction de la nature de l'organisation. Dans les organisations comportant des SI industriels, il existe généralement un RSSI pour le périmètre industriel. Dans les organisations qui développent des produits comportant des SI, un RSSI peut être nommé (dans ce cas, on peut parler de Product Security Officer ou PSO).

Dans les grandes entreprises ou administrations, les activités et tâches peuvent être réparties entre un RSSI qui porte la responsabilité globale et des experts en cybersécurité qui déclinent les actions sur leurs périmètres respectifs.

Salaire

Le salaire moyen d'un RSSI se situe aux alentours de 100 000 euros avec une rémunération pouvant démarrer dès 40 000 euros et atteindre les 150 000 euros annuels. A quelques rares exceptions, le salaire peut s'afficher à plus de 200 000 euros.

Ces écarts très importants sont liés à la taille de l'entreprise et au niveau d'expertise du RSSI.

A l'international, aux Etats-Unis par exemple, un RSSI peut gagner entre 80 000 et 200 000 dollars par an.

Où travailler ?

Le Responsable de la sécurité des systèmes d'information peut travailler dans les secteurs industriels, pour des sociétés de services ou encore dans le secteur public.

Par exemple :

· Editeurs de logiciels et entreprises informatiques
· Secteur bancaire
· Secteur des télécommunications
· Sociétés de conseil en hautes technologies

19

ÉVALUATEUR·RICE DE LA SÉCURITÉ DES TECHNOLOGIES DE L'INFORMATION

Niveau d'études : Bac+3 à Doctorat

Spé Conseillée : Scientifique

Employabilité : Bonne

Salaire débutant : 3 000 €

Code ROME : M1802 - Code FAP : M2Z

EN MATIÈRE DE SÉCURITÉ DE L'INFORMATION, ON N'EST JAMAIS TROP PRUDENT. VOUS SOUHAITEZ CONSEILLER ET ACCOMPAGNER LES ENTREPRISES DANS LE DÉVELOPPEMENT D'UNE ARCHITECTURE SYSTÈME SÉCURISÉE ET ROBUSTE ? L'ÉVALUATEUR DE LA SÉCURITÉ DES TECHNOLOGIES DE L'INFORMATION EST CE NOUVEL EXPERT DE LA CYBERSÉCURITÉ QUI CONNAÎT SUR LE BOUT DES DOIGTS LES NORMES ET PROCESSUS RELATIFS AUX SYSTÈMES DE MANAGEMENT DE LA SÉCURITÉ DE L'INFORMATION.

Missions

Dans un monde où les réseaux globaux prennent toujours plus d'expansion et une importance stratégique qui ne se dément pas, les systèmes d'information d'une organisation doivent pouvoir résister aux différentes menaces qui pèsent sur eux. Pour sécuriser leurs systèmes et leurs réseaux, les organisations doivent pouvoir compter sur des gestionnaires capables de reconnaître les menaces et les vulnérabilités des systèmes existants et d'assurer la conception et le développement de systèmes sécuritaires. C'est le propre de la mission de l'évaluateur de la sécurité des technologies de l'information.

L'évaluateur ou l'évaluatrice de la sécurité des technologies de l'information intervient au sein de laboratoires qui réalisent des évaluations de sécurité des technologies de l'information pour des commanditaires. Il/elle vérifie la conformité d'un produit, voire d'un système, par rapport à sa spécification de sécurité, selon une méthode et des critères normalisés, réglementaires (Critères Communs-CC, Certification de Sécurité de Premier Niveau-CSPN…) ou privés (définis par le commanditaire). Il/elle agit en tant que tierce partie indépendante des développeurs de produits et des commanditaires de l'évaluation de sécurité.

Il peut être spécialisé dans l'évaluation de produits matériels (hardwares) ou logiciels (softwares) ou encore proposer son assistance à un commanditaire pour la préparation d'une évaluation réalisée par une autre évaluatrice.

La réalisation de l'évaluation pour un évaluateur qui intervient seul revient à :
· Respecter une procédure et une méthodologie d'évaluation selon des critères préalablement définis
· Vérifier que la documentation fournie par le développeur est conforme
· Réaliser des tests techniques afin de vérifier que les fonctions de sécurité atteignent le niveau requis de robustesse en adéquation avec la cible de sécurité et le niveau de certification visé
· Évaluer la robustesse des mécanismes cryptologiques du produit
· Rédiger le rapport d'évaluation à destination de l'autorité de certification
· Participer à l'amélioration continue des moyens et des méthodes d'évaluation

Les missions d'assistance à un commanditaire pour la préparation d'une évaluation réalisée par un autre évaluateur consistent à :
· Assister à la rédaction de la cible de sécurité et des fournitures nécessaires à l'évaluation
· Conduire des tests de sécurité en amont

Compétences

Exercer comme évaluatrice de la sécurité des technologies de l'information demande de solides compétences informatiques et des connaissances pointues en cybersécurité, telles que :

· Certifications et évaluations de produits : connaissance des processus d'évaluation sécuritaires (Critères Communs, CPSN, etc.)
· Sécurité de l'électronique et des architectures matérielles
· Tests d'intrusion : maîtrise des techniques d'audits techniques de sécurité
· Cyberdéfense : connaissance des techniques d'attaques et d'intrusions
· Cyberdéfense : connaissance des vulnérabilités des environnements
· Connaissance en rétro-ingénierie de systèmes (ou reverse engineering)
· Connaissance en développement (codes embarqués, langages de conception, scripting)

Études

Pour devenir évaluateur de la sécurité des technologies de l'information, vous devrez justifier d'un diplôme informatique de niveau Bac+3 à Doctorat et d'une spécialisation en cybersécurité. Ce métier est accessible à partir d'une expérience professionnelle en audit de sécurité. Pour certains types d'évaluations, des profils doctorants spécialisés peuvent être nécessaires (cryptologie notamment).

Salaire

La rémunération d'un évaluateur de la sécurité des technologies de l'information varie selon le Centre d'Évaluation de la Sécurité des Technologies de l'Information au sein duquel il intervient.

Le salaire médian pour les emplois d'évaluateurs de la sécurité des technologies de l'information en France est de 39 000 euros par an. Les postes de niveau débutant commencent avec un salaire environnant 32 000 euros par an, tandis que les travailleurs les plus expérimentés perçoivent jusqu'à 124 800 euros par an.

QUALITÉS

· Rigueur
· Qualités rédactionnelles pour la rédaction de rapports adaptés à différents niveaux d'interlocuteurs
· Capacité à travailler en équipe

Où travailler ?

Les évaluateurs de la sécurité des technologies de l'information interviennent au sein de Centres d'Evaluation de la Sécurité des Technologies de l'Information (CESTI) agrées.

Cesti qui recrutent des évaluateurs de la sécurité des technologies de l'information

CESTI agréés pour les évaluations CC et ITSEC dans le domaine technique logiciels et équipements réseaux :

· Amossys
· Oppida

CESTI agréés pour les évaluations CC et ITSEC dans les domaines techniques composants électroniques, microélectroniques et logiciels embarqués :

· CEA – Leti
· Serma Safety & Security
· Thales (TCS-CNES)

CESTI agréés pour les évaluations CC dans le domaine des équipements matériels avec boîtiers sécurisés :

· Thales (TCS-CNES)
· AMOSSYS + SERMA
· CEA-LETI
· OPPIDA + SERMA

Évolution de carrière

Les tendances et facteurs d'évolution du métier indiquent que l'évaluateur de la sécurité des technologies de l'information devra prendre en compte dans l'exercice des ses missions, les réglementations internationales, notamment celles liées à la certification des produits connectés (IOT).

Freelance

L'évaluateur de la sécurité des technologies de l'information peut exercer en tant que freelance indépendant. La première option consiste à créer un statut d'auto-entrepreneur ou une société individuelle auprès de la Chambre de Commerce. Il sera ainsi possible de facturer ses prestations à tout type de clients.

Néanmoins, ce choix est encore plutôt rare, dans la mesure où l'évaluatrice de la sécurité des technologies de l'information doit être rattaché à un organisme agrée (CESTI) pour exercer.

Avantages et inconvénients

L'évaluateur de la sécurité des technologies de l'information est un expert de la cybersécurité qui doit convoquer quotidiennement l'ensemble des ces connaissances en cybersécurité (technique, veille, prospective) dans ses missions d'évaluation. C'est donc un métier complet .

Ce métier, qui évolue aussi vite que les technologies de l'information, est à réserver aux profils qui savent s'adapter au changement et qui ne craignent pas de devoir réactualiser fréquemment leurs connaissances par de la formation continue.

Comment le devenir ?

L'évaluateur de la sécurité des technologies de l'information vérifie la conformité d'un produit, voire d'un système, par rapport à sa spécification de sécurité, selon une méthode et des critères normalisés, réglementaires ou privés. La profession est accessible avec l'obtention d'un diplôme en informatique de niveau Bac+3 à Doctorat comprenant une spécialisation en cybersécurité. Ce métier requiert une expérience professionnelle en audit de sécurité. Le salaire médian pour les emplois d'évaluateurs de la sécurité de l'information en France est de 39 000 euros par an. Les tendances et facteurs d'évolution du métier indiquent que l'évaluatrice de la sécurité des technologies de l'information devra prendre en compte dans l'exercice des ses missions, les réglementations internationales, notamment celles liées à la certification des produits connectés (IOT).

20 COORDINATEUR·RICE CYBERSÉCURITÉ

Niveau d'études : Bac+3

Spé Conseillée : Scientifique

Employabilité : Bonne

Salaire débutant : 2 500 €

Code ROME : M1802 - Code FAP : M2Z

LE COORDINATEUR CYBERSÉCURITÉ EST LE GARANT DE LA MISE EN ŒUVRE ET DE L'OPTIMISATION DE LA SÉCURITÉ INFORMATIQUE AUPRÈS DES ÉQUIPES IT ET COLLABORATEURS DE L'ENTREPRISE. VÉRITABLE CHEF D'ORCHESTRE DE LA CYBERSÉCURITÉ AU SEIN DES ORGANISATIONS, CET EXPERT DE LA CYBERDÉFENSE POSSÈDE LA VISION D'ENSEMBLE DES SYSTÈMES D'INFORMATION DE L'ENTREPRISE. VOUS SOUHAITEZ PILOTER DES ÉQUIPES PROJETS DANS LE BUT DE LUTTER CONTRE LES CYBERMENACES ? POSSÉDEZ UN TALENT POUR L'ORGANISATION ET LA PLANIFICATION ? VOUS FEREZ À COUP SÛR UN PARFAIT COORDINATEUR CYBERSÉCURITÉ !

Missions

Le coordinateur cybersécurité assure un appui au pilotage des actions de sécurité des systèmes d'information sur un périmètre de l'organisation (sur une entité ou bien en lien avec une thématique : par exemple, coordination des actions de sécurité sur les environnements Cloud, coordination de la mise en conformité à une réglementation, etc.).

Il apporte un support aux équipes opérationnelles pour la réalisation des actions de sécurité et assure le suivi des plans d'actions..

Il est chargé de prendre en compte les différentes alertes de cybersécurité et d'y apporter la meilleure réponse opérationnelle en fonction de la criticité de l'alerte. Les alertes peuvent venir du CERT, du SOC, des campagnes d'audit et d'intrusion, des sondes de détection, ou des propres actions de vérifications effectuées par le coordinateur cybersécurité.

Il est par ailleurs responsable du traitement à court terme des alertes, ainsi que du traitement des causes racines à plus long terme. De plus, il travaille en mode projet avec les équipes d'experts et de run (incident manager, problem manager, change manager et service delivery manager) ainsi que des IT Managers.

Enfin, le coordinateur de cybersécurité veille à ce que les collaborateurs de l'entreprise puissent accomplir leur travail en toute sécurité. Il fixe en effet des normes de sécurité informatique pour leur environnement de travail sur la base d'exigences légales et forme les

collaborateurs afin que ces derniers soient aptes à comprendre ces règles.

Au quotidien, le coordinateur cybersécurité est chargé des missions suivantes :

· Apporter un appui aux équipes opérationnelles dans la prise en compte des politiques de sécurité des systèmes d'information et des exigences réglementaires
· Participer à la déclinaison des politiques en directives de cybersécurité sur un périmètre organisationnel ou technique
· Participer à la réalisation des analyses de risques de sécurité
· Assurer le suivi des plans d'actions de sécurité
· Assurer le suivi de la gestion des vulnérabilités, des recommandations issues des audits et des contrôles de sécurité, suivre les plans de remédiation
· Participer à l'animation du réseau des relais de la sécurité des systèmes d'information
· Mener des contrôles opérationnels ou permanents de sécurité des systèmes d'information
· Répondre aux sollicitations des différentes entités de l'organisation en matière de sécurité
· Assurer la production d'indicateurs et de tableaux de bord de sécurité pour son périmètre (tableaux de bord de pilotage de son activité, tant en termes de prise en compte des alertes, des plans d'action à définir, que des réponses à apporter aux émetteurs)
· Participer aux actions de sensibilisation à la sécurité des systèmes d'information

En résumé, le coordinateur cybersécurité assure un appui au pilotage des actions de sécurité des systèmes d'information sur un périmètre de l'organisation. Le coordinateur cybersécurité est chargé de prendre en compte les différentes alertes de cybersécurité et d'y apporter la meilleure réponse opérationnelle en fonction de la criticité de l'alerte. Le coordinateur de cybersécurité veille à ce que les collaborateurs de l'entreprise puissent accomplir leur travail en toute sécurité sans risque de compromission de leurs données et outils systèmes.

Savoir-être

· Capacité à définir des procédures
· Pédagogie sur les sujets de cybersécurité
· Capacité de travail en équipe
· Capacité d'influence
· Capacité de restitution au management
· Capacité à travailler en transverse au sein de l'organisation

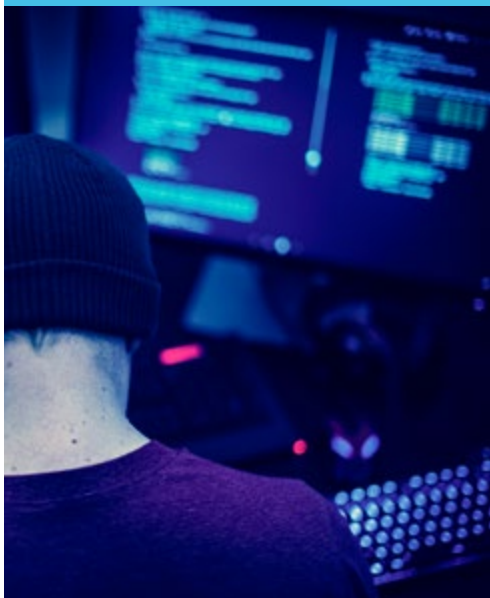
Compétences

Exercer en qualité de coordinateur cybersécurité demande de posséder de solides connaissances sur les sujets des systèmes et réseaux informatiques :

· Du système d'information et des principes d'architecture
· Des technologies de sécurité et des outils associés
· La gestion des risques, politique de cybersécurité et SMSi
· Des méthodologies d'analyse des risques de sécurité
· Maîtrise des fondamentaux dans les principaux domaines de la sécurité des systèmes d'information

QUALITÉS

· Rigueur
· Diplomatie
· Communication
· Leadership
· Sang-froid
· Bonnes capacités d'anticipation



« LA COORDINATION AU SEIN D'UNE ORGANISATION EST L'UNE DES FONCTIONS-CLÉS DU MANAGEMENT QUI CONSISTE À ASSURER POUR UN ENSEMBLE DE PERSONNES ET DE TÂCHES, D'UNE CONJONCTION DES EFFORTS EN VUE D'UN OBJECTIF COMMUN. »

Il est de plus en plus demandé aux coordinateurs cybersécurité de se former également à la gestion de projet et au management agile. Pour cela, il doit :

· Se montrer agile et proactif dans ses démarches
· S'adapter aux changements, à l'incertitude et à la complexité
· Comprendre les enjeux relationnels et de pouvoir en entreprise
· Prendre en compte plusieurs paramètres à la fois dans ses analyses et ses décisions
· Faire preuve d'ouverture d'esprit et d'impartialité en étant factuel
· Développer l'empathie et l'écoute positive
· Entretenir des relations assertives avec les différents interlocuteurs
· Etre capable de travailler seul ou en équipe interculturelle et pluridisciplinaire, et en réseau
· Identifier ses besoins d'apprentissage et apprendre régulièrement, y compris en auto-apprentissage, dans les domaines associés à sa fonction
· Intégrer l'éco-responsabilité dans toutes les dimensions de son activité
· Transmettre des savoirs et savoir-faire
· Effectuer une veille permanente sur la réglementation et les normes liées à son activité et les risques juridiques encourus
· Expliquer et convaincre avec pédagogie

Études

Pour mettre toutes les chances de votre côté afin de devenir coordinateur cybersécurité, vous devrez obtenir un diplôme informatique de niveau Bac +3 avec une spécialité en cybersécurité. Il est également recommandé de se former à la gestion de projet agile.

Salaire

La rémunération d'une coordinatrice cybersécurité diffère en fonction de la typologie de l'entreprise où elle est amenée à exercer et peut varier selon les missions qui lui sont confiées et selon son niveau d'expérience professionnelle.

Le salaire médian est de 30 000 euros annuels. Les profils débutants pourront commencer leur carrière sur la base d'un salaire annuel estimé à 25 000 euros tandis que les collaborateurs les plus expérimentés pourront gagner jusqu'à 46 800 euros par an.

A l'international, aux Etats-Unis par exemple, un coordinateur cybersécurité peut percevoir un salaire annuel moyen de 100 000 dollars. Au Canada, il pourra prétendre à environ 110 000 dollars annuels.

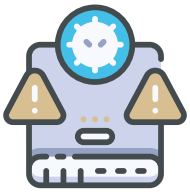
Où travailler ?

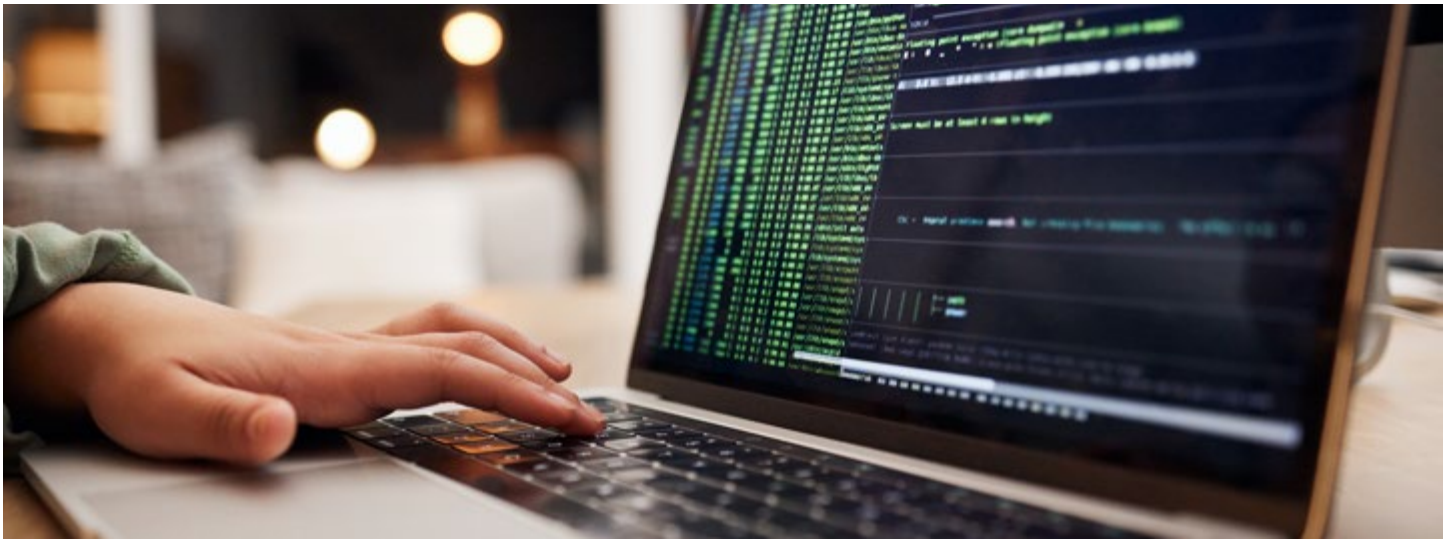
Les coordinateurs cybersécurité interviennent au sein d'organisations publiques comme privées. Ils peuvent par exemple exercer dans les secteurs industriels ou pour des sociétés de services.Voici un exemple d'entreprises et institutions qui font appel à des coordinateurs cybersécurité :

· Editeurs de logiciels et entreprises informatiques
· Secteur bancaire
· Secteur des télécommunications
· Sociétés de conseil en Hautes Technologies
· Secteur de la Défense et de la sécurité gouvernementale

Évolution de carrière

En règle générale, les coordinateurs cybersécurité évoluent vers des postes de Responsables de la sécurité informatique ou encore de Directeurs de la cybersécurité.





« FACE À L'AUGMENTATION DES ATTAQUES CYBER, IL DEVIENT INDISPENSABLE POUR LES ENTREPRISES DE VEILLER À L'UNITÉ, LA COHÉRENCE ET LA SÉCURITÉ DES SYSTÈMES D'INFORMATION.AFIN DE RÉPONDRE AUX EXIGENCES DE SÉCURITÉ INFORMATIQUE DES ORGANISATIONS, IL EST FORTEMENT RECOMMANDÉ DE METTRE EN PLACE ET DÉPLOYER UN ENSEMBLE DE PROCESSUS ET DE MESURES DE CYBERSÉCURITÉ, EN PARTIE TECHNIQUES MAIS PAS SEULEMENT, VISANT À ASSURER LE MAINTIEN DE LA SÉCURITÉ DU SYSTÈME D'INFORMATION. »

Freelance

Le coordinateur cybersécurité peut exercer en tant que freelance indépendant. Il n'aura qu'à créer un statut d'auto-entrepreneur ou une société individuelle auprès de la Chambre de Commerce. Il lui sera ainsi possible de facturer ses prestations à tous types de clients.

Le tarif journalier moyen en freelance est de 600 euros. Ce tarif peut augmenter jusqu'à 1200 euros par jour pour les profils les plus expérimentés.

Avantages et inconvénients

La coordinatrice cybersécurité exerce des missions variées et le challenge intellectuel est important. Également, ils ont le sentiment de rendre vraiment service lorsqu'ils mettent leurs compétences au service de la protection des données sensibles de l'entreprise. Ce poste reste néanmoins très prenant et potentiellement stressant et les échecs possibles sur certaines missions peuvent être compliqués à gérer émotionnellement parlant, surtout pour un profil débutant.

Comment le devenir ?

Le coordinateur cybersécurité est le garant de la mise en œuvre et de l'optimisation de la sécurité informatique auprès des équipes IT et collaborateurs de l'entreprise. Le coordinateur cybersécurité est un expert très recherché et ce métier représente une voie professionnelle d'avenir. La coordinatrice cybersécurité exerce des missions variées et le challenge intellectuel est important. Elle perçoit en moyenne 30 000 euros annuels lorsqu'il débute en entreprise. Une évolution de carrière intéressante est possible, la plupart évoluant rapidement après quelques années d'expérience vers des postes de responsables de la sécurité informatique ou encore de directeurs de la cybersécurité.

21 SPÉCIALISTE EN DÉVELOPPEMENT SÉCURISÉ

Niveau d'études : Bac+3 à Bac+5

Spé Conseillée : Scientifique

Employabilité : Bonne

Salaire débutant : 2 900 €

Code ROME : M1802 - Code FAP : M2Z

LE SPÉCIALISTE EN DÉVELOPPEMENT SÉCURISÉ EST CE NOUVEL EXPERT FORMÉ AU DÉVELOPPEMENT WEB ET À LA SÉCURITÉ INFORMATIQUE CAPABLE D'ACCOMPAGNER LES DÉVELOPPEURS DANS LA MISE EN PLACE D'UNE STRATÉGIE DE SÉCURITÉ APPLICATIVE EFFICACE AU SEIN DE L'ENTREPRISE. VOUS VOULEZ DEVENIR DÉVELOPPEUR ? DANS CE CAS, NE FAITES PAS L'IMPASSE SUR LA SÉCURITÉ DE L'INFORMATION ET DEVENEZ SPÉCIALISTE EN DÉVELOPPEMENT SÉCURISÉ !

Missions

Le spécialiste en développement sécurisé intervient en appui des équipes de développement informatique afin d'accompagner les développeurs dans la prise en compte des exigences de sécurité. Il teste la sécurité des développements et suit la correction des vulnérabilités identifiées.

Au quotidien, il exerce des missions de conception liées aux solutions de développement, coordonne des activités de soutien auprès des équipes de développement et réalise une veille technologique sur les solutions de développement sécurisé. Ses tâches sont les suivantes :

Conception

· Définir ou contribuer à la définition des guides de développement sécurisé
· Contribuer au choix des solutions de revue de code

Soutien auprès des équipes de développement

· Participer à la rédaction des exigences de sécurité applicative
· Faire respecter les bonnes pratiques de sécurité du développement sur les projets et, en phase d'intégration, contribuer aux sprints pour suivre les revues sécurité pour les développements en méthode agile
· Assurer la formation des développeurs

aux techniques de développement sécurisé et aux risques de sécurité sur la base de frameworks de développement sécurisé du marché
· Former les développeurs aux outils de revue de code
· Évaluer la bonne implémentation des exigences de sécurité à travers des audits applicatifs et des revues de code
· Prioriser les vulnérabilités rencontrées et accompagner les développeurs dans la bonne prise en compte des mesures de remédiation

Partage de connaissances et veille technologique

· Assurer une veille technologique sur les techniques de développement sécurisé
· Proposer des solutions pour améliorer la sécurité sur son périmètre d'expertise

Compétences

Exercer en qualité de spécialiste en développement sécurisé demande de solides compétences en développement informatique et des connaissances pointues en cybersécurité, telles que :

· Développement logiciel et ingénierie logicielle (sous l'angle de la sécurité) :
· conception et développement des applications
· Développement logiciel et ingénierie logicielle (sous l'angle de la sécurité) : tests de codes applicatifs
· Développement logiciel et ingénierie logicielle (sous l'angle de la sécurité) : connaissance des vulnérabilités logicielles
· Tests d'intrusion : maîtrise des techniques d'audits techniques de sécurité
· Connaissances en développement (codes embarqués, langages de conception, etc.)
· Contribution des architectures à la sécurité : intégration des systèmes
· Innovation sécurité

Savoir-être

· Capacité à prendre en compte les nouvelles méthodes de gestion de projet (méthode agile notamment).
· Capacité de restitution aux managers
· Capacité d'appropriation des enjeux métiers
· Pédagogie sur les sujets de cybersécurité
· Capacité de travail en équipe
· Capacité à définir des procédures

Études

Pour vous engager sur la voie d'un métier d'avenir et devenir spécialiste en développement sécurisé, vous devrez justifier d'un diplôme informatique de niveau Bac+3 à Bac+5 et d'une spécialisation en développement et en cybersécurité.

Ce métier est accessible à partir d'une expérience préalable en développement.

Une expérience professionnelle de 5 ans en sécurité des systèmes d'information peut également être exigée.

Salaire

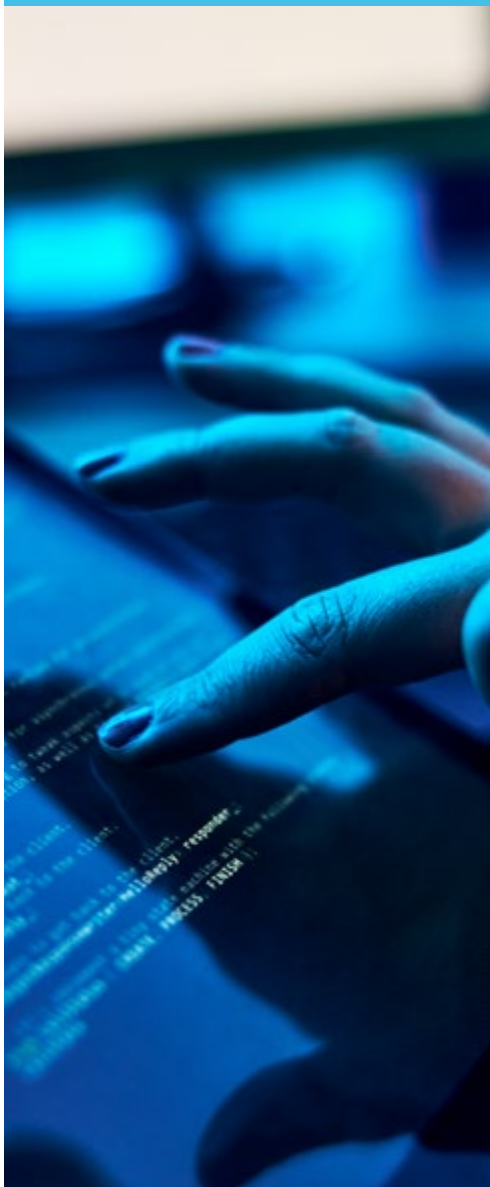
La rémunération d'un spécialiste en développement sécurisé diffère en fonction de la typologie de l'entreprise où il est amené à exercer, selon les missions qui lui sont confiées et va dépendre de son niveau d'expérience professionnelle.

Le salaire médian en France est de 40 000 euros annuels. Un spécialiste débutant sera rémunéré 35 000 euros annuels, les profils confirmés pouvant prétendre jusqu'à 65 000 euros annuels.

A l'international, aux Etats-Unis par exemple, un spécialiste en développement sécurisé peut percevoir un salaire annuel moyen de 58 000 dollars. En Suisse, il pourra prétendre à environ 82 000 francs suisses annuels.

QUALITÉS

· Pédagogie
· Communication
· Polyvalence



Où travailler ?

Les spécialistes en développement sécurisé interviennent au sein d'organisations publiques comme privées. Ils peuvent par exemple exercer dans les secteurs industriels ou pour des sociétés de services.Voici un exemple d'entreprises et institutions qui font appel à des spécialistes en développement sécurisé :

· Editeurs de logiciels et entreprises informatiques
· Secteur bancaire
· Secteur des télécommunications
· Sociétés de conseil en Hautes Technologies

Évolution de carrière

Dans le cadre d'une démarche agile, le spécialiste en développement sécurisé intervient au sein des équipes pour définir les users stories et les abusers stories et suivre la prise en compte des anomalies (démarche DevSecOps).

En plus de ses compétences en sécurité applicative, le métier nécessitera de posséder par ailleurs une compétence en gestion opérationnelle de la sécurité de systèmes et en sécurité des middlewares.

Freelance

Le spécialiste en développement sécurisé peut exercer en tant que freelance. Il conviendra de créer un statut d'auto-entrepreneur ou une société individuelle auprès de la Chambre de Commerce. Il sera ainsi possible de facturer ses prestations à tout type de clients.

Le tarif journalier moyen d'un spécialiste en développement sécurisé freelance est de 700 euros. Ce tarif peut facilement grimper jusqu'à 1200 euros par jour pour les profils les plus expérimentés.

Avantages et inconvénients

Le spécialiste en développement sécurisé est un expert de la cybersécurité qui exerce des missions tant techniques que managériales. C'est un métier qui demande une forte appétence pour la communication car le spécialiste en développement sécurisé est en interaction quotidienne avec les développeurs. Ce métier implique un travail de veille important concernant les nouvelles technologies de sécurité, aussi cet expert devra prévoir de mettre à jour et réactualiser fréquemment ses connaissances par de la formation continue.

Comment le devenir ?

Faire le choix de devenir spécialiste en développement sécurisé implique de posséder un diplôme informatique de niveau Bac + 3 à Bac + 5 avec une double spécialisation en développement et en cybersécurité. Ce métier est accessible à partir d'une expérience professionnelle préalable en développement. Le salaire médian pour les spécialistes en développement sécurisé qui exercent en France est d'environ 40 000 euros annuels. En plus de posséder de solides compétences en sécurité applicative, le métier nécessitera de développer très rapidement des compétences en gestion opérationnelle de la sécurité de systèmes et en sécurité des middlewares.

22

AUDITEUR·RICE DE SÉCURITÉ ORGANISATIONNELLE

Niveau d'études : Bac+2 à Bac+5

Spé Conseillée : Scientifique

Employabilité : Moyenne

Salaire débutant : 2 900 €

Code ROME : M1802 - Code FAP : M2Z

IL EST CHARGÉ D'EFFECTUER UNE ÉVALUATION COMPLÈTE (D'UN POINT DE VUE TECHNIQUE, JURIDIQUE ET ORGANISATIONNEL) DES PROCESSUS LIÉS À LA SÉCURITÉ PHYSIQUE ET À LA CYBERSÉCURITÉ MIS EN PLACE PAR UNE ENTREPRISE. L'OBJECTIF EST DE DÉTERMINER L'EFFICACITÉ GLOBALE DES CONTRÔLES LIÉS À CES PROBLÉMATIQUES : SONT-ILS MIS EN ŒUVRE CORRECTEMENT, FONCTIONNENT-ILS COMME PRÉVU ET PRODUISENT-ILS LE RÉSULTAT ATTENDU ? CET EXPERT FOURNIT ÉGALEMENT UNE ÉVALUATION DE LA CRITICITÉ DES FAIBLESSES DÉCOUVERTES DANS LE SI ET RECOMMANDE DES ACTIONS CORRECTIVES.

Missions

Pour analyser et évaluer les contrôles et les pratiques de sécurité (au sens global comme nous l'avons indiqué précédemment), ces professionnels doivent travailler en étroite collaboration avec l'équipe informatique, les responsables métiers et la direction.

En s'appuyant sur des entretiens poussés avec différents salariés, il peut élaborer des plans pour améliorer la conformité en matière de sécurité, réduire les risques et gérer les menaces pour le SI et la réputation de l'entreprise.

Plus précisément, ces experts créent et exécutent des audits basés sur les politiques organisationnelles et les réglementations en vigueur dans le pays ou les pays où intervient l'entreprise. Ils mettent au point des tests des systèmes informatiques pour identifier les risques et les insuffisances au niveau des logiciels de sécurité (antivirus, pare-feu, contrôle des accès et des identités…), les protocoles de chiffrement des données et des flux ainsi que les mesures de sécurité connexes.

Toutes les évaluations effectuées en interne et en externe doivent être expliquées et détaillées dans des rapports précisant le degré de risque de l'organisation. Ces rapports doivent également présenter les solutions et processus à mettre en place pour remédier aux faiblesses et renforcer la résilience de l'activité de l'entreprise.

La résilience peut en effet être améliorée par ces auditeurs de sécurité qui présentent de nouvelles pratiques et technologies. En conseillant les entreprises, d'apporter des changements en fonction

de leurs pratiques actuelles, des tendances et des problématiques émergentes dans leur domaine, les auditeurs de sécurité facilitent la proactivité. Ils assument donc une responsabilité importante et profitent des occasions de développer des solutions de sécurité créatives.

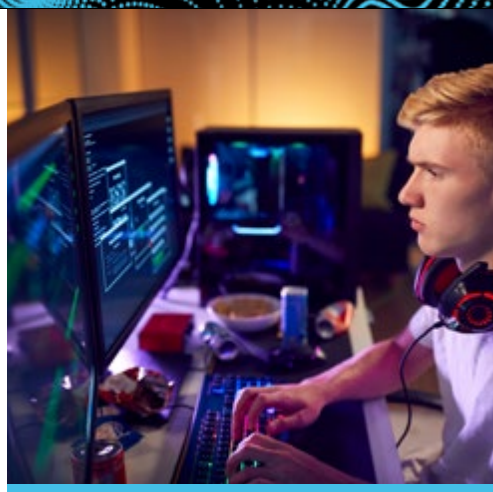
Mais les responsabilités professionnelles d'une auditrice de sécurité organisationnelle peuvent varier en fonction du poste et des besoins de l'entreprise ou de l'organisme gouvernemental.

Les responsabilités et les tâches peuvent comprendre les éléments suivants :

· Préparation et réalisation du volet organisationnel des audits : contrôle de conformité, analyse de documents, entretiens, vérification des preuves fournies, audit de sécurité physique…
· Rédaction de rapports d'audit, assortis de préconisations portant sur les faiblesses organisationnelles et techniques identifiées
· Formalisation et standardisation des procédures d'audits organisationnels
· Rédaction de recommandations génériques dans les domaines organisationnels (réglementation, gouvernance, intégration de la sécurité dans les projets, homologation, continuité des activités…
· Développement de méthodes pour surveiller et mesurer les efforts en matière de risques, de conformité et d'assurance
· Vérification des postures de sécurité des logiciels d'application/réseaux/systèmes pour s'assurer qu'elles sont mises en œuvre comme prévu
· Détection et documentation des écarts entre la réalité et ce qui est recommandé ou obligatoire et proposer les actions pour les corriger
· Veille active sur les réglementations, les normes et bonnes pratiques dans les domaines de la protection des SI et de la gouvernance SSI
· Assistance à la reprise de contrôle d'un SI suite à un incident de grande envergure
· Évaluation des dossiers de sécurité : analyse de risques, PSSI, procédures

Dans l'ensemble, le travail consiste à offrir une vision approfondie des domaines dans lesquels les systèmes de cybersécurité sont suffisants et performants, et des domaines dans lesquels des améliorations sont possibles ou nécessaires. Si des améliorations sont nécessaires, l'auditeur de sécurité peut également être chargé de fournir une analyse coûts-avantages des mesures recommandées pour renforcer la sécurité.

« LE SYSTÈME D'INFORMATION (SI) D'UNE ENTREPRISE EST CONSTAMMENT SOUMIS À DES MENACES ET À DES VULNÉRABILITÉS EXTERNES OU INTERNES. IL EST DONC INDISPENSABLE D'ÉVALUER L'EFFICACITÉ DES CONTRÔLES DE SÉCURITÉ MIS EN PLACE OU, PIRE, QUI N'AURAIENT PAS ÉTÉ INSTAURÉS… »



QUALITÉS

Être rigoureux et autonome sont deux qualités majeures d'une auditrice de sécurité organisationnelle. Savoir vulgariser des concepts complexes à des décideurs qui ne maitrisent pas les rouages de la cybersécurité et de l'IT en général est également indispensable. L'objectif des rapports est en effet de proposer des solutions pertinentes et réalisables (en fonction des contraintes métier et réglementaires) aux faiblesses constatées.

Compétences

Il est indispensable d'avoir de bonnes connaissances à propos des principaux référentiels, normes et réglementations relatifs à la sécurité des systèmes d'information (ISO 2700x, ISO 22301, RGS, IGI 1300, etc.). Des connaissances à propos de la gouvernance SSI, de la gestion des incidents, de la continuité et la reprise des activités (après une cyberattaque ou un incident) sont également nécessaires.

Des connaissances techniques (sécurisation des systèmes d'exploitation, mécanismes de contrôle d'accès, architecture réseau, etc.) sont essentielles afin d'appréhender les vulnérabilités techniques et d'en déterminer les causes organisationnelles.

Les auditeurs de sécurité doivent également connaître les langages de programmation, comme C++ et Java et être familiers avec différents systèmes d'exploitation, tels que Windows et Linux. Une expérience avec les outils COTS/GOTS/DOD CS pour l'examen de l'organisation et de l'enquête de sécurité sont appréciés. Enfin, la familiarité avec les outils d'audit et de défense réseau comme Proofpoint, Symantec ProxySG et Advanced Secure Gateway permet aux auditeurs de sécurité de mener des audits efficaces et approfondis.

Globalement, les auditeurs de sécurité organisationnelle disposent des compétences suivantes :

· Maitrise des méthodologies d'audits
· Connaissance du système d'information et des principes d'architecture
· Maitrise des fondamentaux dans les principaux domaines de la SSI
· Connaissance de la gouvernance, des normes et des standards dans le domaine de la sécurité : normes ISO et normes sectorielles (PCI-DSS…)
· Conception et maintien d'un SI sécurisé
· Compétences comportementales
· Capacité de synthèse et de vulgarisation pour des publics non techniques
· Rédaction de rapports adaptés à différents niveaux d'interlocuteurs
· Législation et jurisprudence
· Gestion des risques
· Test et évaluation de systèmes
· Évaluation des vulnérabilités

Études

Il est recommandé d'avoir Bac +5, même si ce métier est accessible à partir d'une expérience professionnelle en audit. D'autres offres d'emploi demandent d'être titulaire d'un diplôme de niveau 7, dans le domaine de l'IT et de justifier d'une expérience dans le domaine de l'audit SSI organisationnel.

Quel diplôme ? Un baccalauréat en technologie de l'information, en informatique ou dans une discipline connexe permet aux analystes de la sécurité de se familiariser avec les technologies, les théories et les pratiques de base dans ce domaine.

Différentes certifications constituent des atouts majeurs pour convaincre un employeur :

· Certified Information System Security Professional (CISSP)
· ISACA Certified Information Security Manager (CISM)
· Certified ISO 27001 Lead Implementer 1
· ISACA Certified Information Systems Auditor (CISA)
· GIAC Systems and Network Auditor (GSNA)
· Certified ISO 27001, Lead Auditor, Internal Auditor 1
· IRCA ISMS Auditor

Salaire

La rémunération varie selon votre expérience. La grille commence généralement autour de 35 000 euros brut/an. Les auditeurs seniors peuvent prétendre le double.

Où travailler ?

Ce type de profil très particulier intéresse les grands comptes ou les entreprises dont le secteur d'activité est très réglementé ou sensible. Des ESN et des cabinets de consultants en cybersécurité peuvent être également une piste d'emploi.

« L'OBJECTIF D'UN AUDIT ORGANISATIONNEL DE SÉCURITÉ PERMET D'ÉTABLIR UN ÉTAT DES LIEUX COMPLET ET OBJECTIF DU NIVEAU DE SÉCURITÉ DE L'ENSEMBLE DU SI D'UN POINT DE VUE ORGANISATIONNEL, PROCÉDURAL ET TECHNOLOGIQUE. »

Évolution de carrière

Ces profils étant très recherchés, un auditeur de sécurité organisationnelle peut travailler en freelance (à condition d'avoir un bon réseau ou d'avoir acquis une solide expérience auparavant) et évoluer en interne pour devenir Risk manager voire RSSI.

Freelance

Les entreprises travaillant dans des secteurs réglementés ou sensibles font appel à des auditeurs de sécurité à intervalles réguliers pour vérifier leur propre efficacité et s'assurer que leurs systèmes sont conformes aux normes du secteur.

Il est donc possible de travailler en indépendant à condition de disposer d'un bon réseau et de solides capacités de persuasion pour trouver des clients. Mais en tant qu'auditeur externe, vous disposez d'un atout non négligeable : vous apportez une perspective objective sur les pratiques de sécurité d'une organisation. Un regard extérieur est souvent le bienvenue. Mais attention cependant aux susceptibilités internes que vous pourriez rencontrer de la part de DSI (Directeur des systèmes d'information), de responsables informatiques, voire d'autres cadres dont les (mauvaises) habitudes présentent des risques pour l'entreprise.

Avantages et inconvénients

Du fait de la diversité des missions à gérer, ce métier ne connaît pas la routine. En fonction de votre poste, vous pouvez être amené à voyager souvent. Par contre, ces auditeurs de sécurité travaillent souvent seuls même s'ils rencontrent de nombreuses personnes afin de rédiger leurs rapports. Ils doivent donc faire preuve de motivation pour mener à bien leurs tâches.

Comment le devenir ?

Les cyberattaques devenant de plus en plus complexes et variées, les entreprises prennent conscience de leurs impacts sur leur résilience. Les auditeurs de sécurité organisationnelle sont donc des profils recherchés, car les organisations doivent mettre en place des Plans de reprise d'activité afin de limiter les impacts des actes malveillants. Pour devenir auditrice de sécurité organisationnelle, il est nécessaire d'avoir de bonnes compétences en informatique et de maitriser les différents aspects de la cybersécurité, tant d'un point de vue technique que juridique. Il est donc recommandé de commencer par obtenir un Bac scientifique puis d'intégrer une école d'ingénieur avec un cursus en cybersécurité axé sur la gouvernance des données.

Niveau d'études : Bac+2

Spé Conseillée : Scientifique

Employabilité : Très bonne

Salaire débutant : 3 300 €

Code ROME : M1802 - Code FAP : M2Z

L'ANALYSTE EN RÉPONSE AUX INCIDENTS EST UN PROFIL TRÈS RECHERCHÉ, CAR SES MISSIONS SONT DEVENUES ESSENTIELLES AUX ENTREPRISES. CE MÉTIER A DEUX FACETTES. LA PREMIÈRE EST TECHNIQUE (TROUVER DES PREUVES DES CYBERATTAQUES). LA SECONDE EST LA GESTION DE LA CRISE (ACCOMPAGNER ET COMMUNIQUER AVEC SA DIRECTION VICTIME D'UNE ATTAQUE INFORMATIQUE). CELA RESSEMBLE UN PEU AUX ENQUÊTES POLICIÈRES, MAIS POUR UN PARC INFORMATIQUE. OUTRE SON RÔLE CLÉ EN MATIÈRE DE DÉTECTION ET DE RÉPONSE À INCIDENTS, IL CONTRIBUE ÉGALEMENT À L'AMÉLIORATION DE LA RÉSILIENCE DE SON ENTREPRISE.

Missions

L'analyste en réponse à incidents de son côté va mener une «enquête technique» orientée sécurité : ordinateurs, réseau, logiciels malveillants, rétro-ingénierie de logiciels, identification de compromission matérielle, etc.

Sa principale responsabilité est de minimiser les effets globaux d'une violation sur les systèmes d'information (SI), les réseaux et les actifs numériques d'une entreprise. Ce rôle implique la maintenance de réseaux à grande échelle ainsi que des interactions potentielles avec les forces de l'ordre.

Ces spécialistes ont également pour mission de surveiller, tester, évaluer et améliorer les systèmes de cybersécurité de leur entreprise. Ils peuvent également contribuer à l'élaboration de protocoles, de politiques et de programmes de formation qui permettent aux organisations de mieux réagir aux incidents de sécurité.

De par son profil, il doit prendre en compte et diligenter des investigations techniques et inforensiques (qualification poussée des cyberattaques) pour documenter les menaces. Il doit aussi, lancer des vérifications techniques et contextuelles sur les nouvelles menaces qui sont susceptibles d'affecter l'activité et la réputation de son entreprise, mais aussi celle de ses clients et partenaires. Les analystes en réponse à incident doivent aussi collaborer et échanger avec d'autres CERT français et internationaux.

Ces experts ne restent pas pour autant dans leur tour d'ivoire. De façon plus concrète pour l'ensemble des salariés de son entreprise, ces analystes doivent contribuer à la sensibilisation aux menaces numériques via des formations en intra, des webinaires ou du e-learning.

Enfin, ils doivent participer ponctuellement aux exercices de gestion de crises organisés par son employeur ou les autorités si son entreprise est considérée comme « sensible » ou fait partie des opérateurs d'importance vitale (OIV), c'est-à-dire identifiée par l'État comme ayant des activités indispensables à la survie de la nation ou dangereuses pour la population.

Les responsabilités

Ses responsabilités sont très variées. Il doit notamment analyser les informations provenant des systèmes de surveillance (notamment les sondes réseau), des incidents opérationnels et d'autres sources pour déterminer la portée et l'impact des incidents de sécurité potentiels, et les traiter en conséquence.

Il doit également contribuer à la conception et à la mise en œuvre des solutions de détection et de prévention des menaces jugées nécessaires à la protection des actifs de l'entreprise. Il doit être une force de proposition en participant à l'amélioration des corrélations, des règles et des analyses des équipes de détection.

L'évaluation de manière critique des pratiques actuelles de son entreprise est également l'une de ses missions. L'objectif de cette veille est de fournir un retour d'information à la direction sur les possibilités d'amélioration, notamment en cas de manquements à la conformité (Règlement général sur la protection des données à caractère personnel-RGPD, directive européenne sur les services de paiement 2e version-DSP2…) et aux réglementations propres au secteur d'activité de son employeur.

Enfin, il doit assurer la maintenance des systèmes attribués afin de garantir la disponibilité, la fiabilité et l'intégrité, y compris la supervision de la capacité, des performances et des licences actuelles et prévues.

Compétences

Il est indispensable d'avoir une très bonne compréhension des implications de la sécurité et des méthodes d'investigation pour les composants IT les plus communs :

- LAN (Local Area Network), WAN (Wide Area Network)
- VPN (Virtual private network)
- IDS/IPS
- systèmes Linux et Windows
- Active Directory
- serveurs d'emails
- serveurs web
- serveurs applicatifs
- bases de données
- SIEM (Security information and event management)
- principes et outils cryptographiques, etc.

Comme nous l'avons déjà évoqué précédemment, il doit être capable de réaliser des investigations inforensiques sur des réseaux, des périphériques disposant des technologies précitées et intégrant des systèmes d'exploitation répandus. Cela implique des connaissances dans l'investigation des technologies mobiles (Android/iOS), des protocoles réseau associés et des applications populaires.

« DANS LE CONTEXTE ACTUEL, IL N'EST PAS SURPRENANT QUE LES ANALYSTES EN RÉPONSE AUX INCIDENTS FASSENT PARTIE DES PROFESSIONNELS DE LA CYBERSÉCURITÉ LES PLUS RECHERCHÉS DANS LE SECTEUR. »

QUALITÉS

Avant de pouvoir commencer à travailler en tant qu'analyste en réponse à incidents, vous devez acquérir de l'expérience dans un poste de cybersécurité de premier échelon. Les employeurs ont tendance à rechercher des candidats qui ont une expérience « vérifiable » au sein de l'équipe de sécurité d'une organisation similaire à la leur. Les postes d'administrateur de sécurité, de réseau ou de système peuvent fournir une expérience pertinente pour un analyste à réponse à incidents. En général, il faut deux à trois ans d'expérience professionnelle pour être admis dans une équipe de réponse aux incidents de sécurité informatique (Computer Security Incident Response Team-CSIRT). Un CSIRT est une équipe de sécurité opérationnelle, composée d'experts de différents domaines (malwares, test d'intrusion, veille, lutte contre la cybercriminalité, forensics…).
Une fois que vous êtes membre d'une CSIRT, vous pouvez apprendre des gestionnaires, des responsables et d'autres professionnels de la sécurité de haut niveau afin d'élargir vos connaissances et vos compétences appliquées. Toutes ces compétences techniques ne suffisent pas. Il doit être doté d'une bonne expression écrite et orale et avoir une bonne capacité à synthétiser de la documentation et des rapports destinés à sa direction. Un bon sens du relationnel et être force de persuasion (tout en étant capable d'adapter sa communication) sont deux atouts majeurs. Enfin, il fait résister au stress qui peut être engendré par une cyberattaque sophistiquée ou une forte charge de travail ponctuelle. Des compétences en matière de collaboration sont très utiles pour travailler avec différentes équipes dans une organisation internationale. Vous devez également être capable de travailler de manière autonome et d'apporter des améliorations.

« CE MÉTIER EST TRÈS RECHERCHÉ, CAR PEU D'ENTREPRISES DISPOSENT EN INTERNE DE CE TYPE DE PROFIL. UNE ÉTUDE RÉCENTE D'IBM A EN EFFET CONSTATÉ QUE 77 % DES ENTREPRISES N'ONT PAS DE PLAN DE RÉPONSE AUX INCIDENTS DE CYBERSÉCURITÉ. IL S'AGIT D'UNE STATISTIQUE ALARMANTE, SURTOUT SI L'ON CONSIDÈRE QUE LE FBI A SIGNALÉ UNE AUGMENTATION DE 300 % DES ACTES DE CYBERMALVEILLANCE ET DE PIRATAGE DEPUIS LE DÉBUT DE LA PANDÉMIE DE COVID. »

Il doit être également capable de réaliser des investigations dans les environnements bureautiques, des datacenters et dans le Cloud. De manière plus précise, il convient de disposer de ces compétences :

· Expérience des outils courants de RI tels que SIEM, gestion des journaux, IDS, systèmes de détection de brèches (APT/BDS/EDR) et capture de paquets
· Large compréhension de TCP/IP, DNS, des services réseau courants et d'autres sujets fondamentaux
· Connaissance intermédiaire des techniques de détection, d'analyse et d'évasion des logiciels malveillants
· Expérience de l'analyse des logiciels malveillants (exécutables, scripts et documents bureautiques), des rootkits, des bootkits, de l'analyse du trafic (Wireshark) et une utilisation efficace de désassembleurs (IDAPro) ou de débogueurs (OllyDBG, winDBG).
· Expérience des tests de pénétration et de l'évaluation de la vulnérabilité des systèmes et réseaux d'entreprise afin de renforcer la sécurité des réseaux.
· Expérience des tests de pénétration d'applications web avec BurpSuite ou d'autres outils similaires de sécurité des applications web. Connaissance des techniques d'attaque et d'exploitation des logiciels

Études

Il faut envisager son orientation dès le lycée en faisant le choix d'une voie scientifique ou technologique (Bac STI2D). Dans les deux cas, un goût prononcé pour les mathématiques est indispensable.

Un diplôme d'ingénieur en informatique avec un bon niveau de connaissance en IT (réseaux et systèmes) ou avec une expérience en cybersécurité sont indispensables. Les certifications GIAC CGFA, GREM, GNFA ou équivalent sont un plus.

Il est recommandé d'intégrer une école d'ingénieur en cybersécurité et ensuite de suivre des formations pour obtenir certaines certifications très demandées.

Salaire

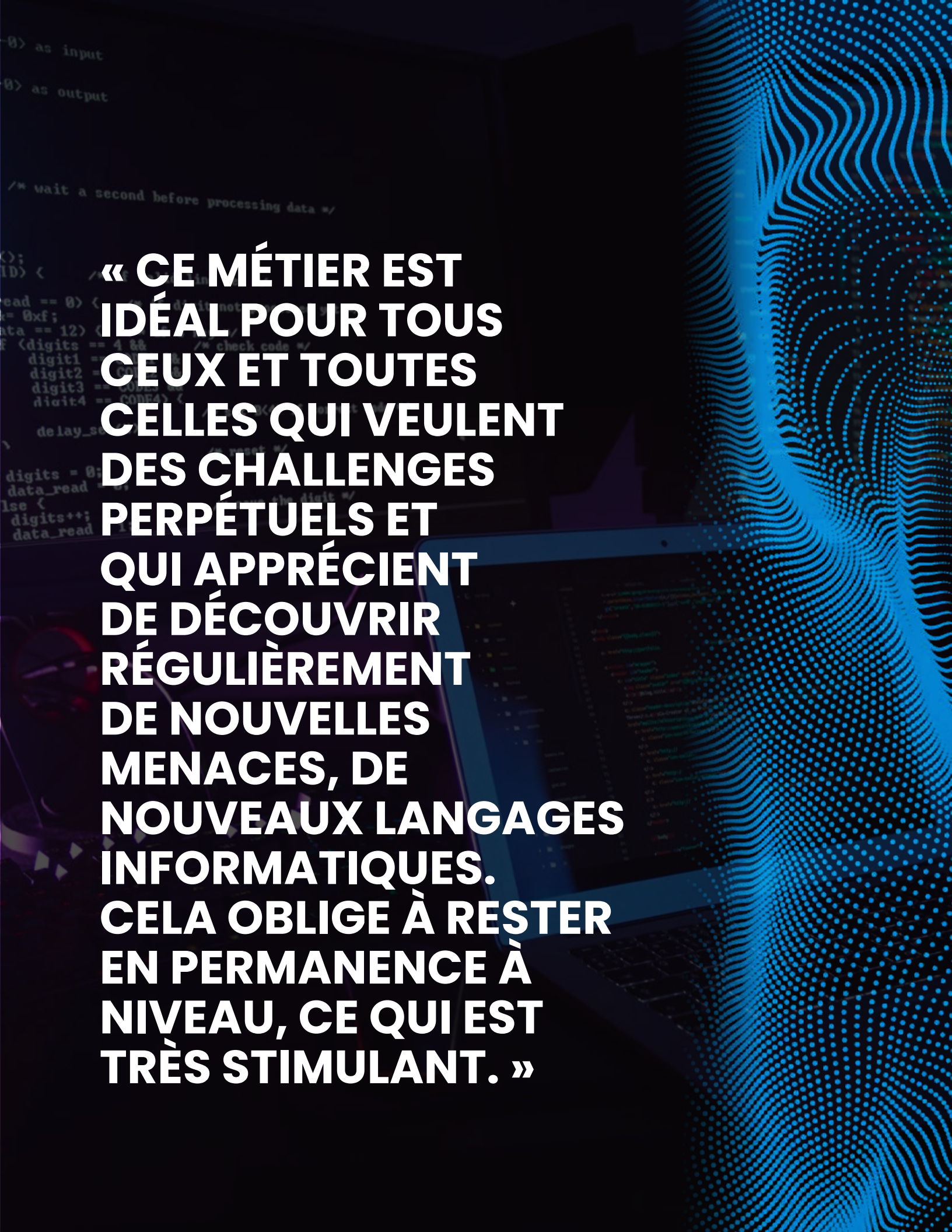
Les grands groupes, mais aussi les Entreprise de Services du Numérique (ESN), recherchent de plus en plus de tels profils. Résultat, les salaires sont attractifs. Ils commencent autour de 40 000 euros brut/an et peuvent atteindre les 70 000 euros brut/an pour les personnes très qualifiées.

Évolution de carrière

Un analyste en RI peut élargir ses compétences pour devenir à moyen et long terme RSSI ou Responsable de la gouvernance, le risque et la conformité (GRC). Il peut aussi décider de travailler en freelance.

Comment le devenir ?

Tous les jours, les entreprises sont confrontées à des incidents de cybersécurité plus ou moins critiques. La principale mission d'un analyste en RI consiste à repérer ceux qui sont les plus impactants pour l'activité de son entreprise. Il doit les analyser afin de comprendre leur fonctionnement afin d'éviter qu'ils ne se reproduisent. C'est en quelque sorte un détective de l'informatique. Pour devenir un analyste en RI, il est fortement recommandé d'avoir un Bac scientifique et d'intégrer ensuite une école d'ingénieur en cybersécurité.



« CE MÉTIER EST IDÉAL POUR TOUS CEUX ET TOUTES CELLES QUI VEULENT DES CHALLENGES PERPÉTUELS ET QUI APPRÉCIENT DE DÉCOUVRIR RÉGULIÈREMENT DE NOUVELLES MENACES, DE NOUVEAUX LANGAGES INFORMATIQUES. CELA OBLIGE À RESTER EN PERMANENCE À NIVEAU, CE QUI EST TRÈS STIMULANT. »

24 DÉLÉGUÉ·E À LA PROTECTION DES DONNÉES

Niveau d'études : Bac+3 à Bac+5

Spé Conseillée : Scientifique

Employabilité : Bonne

Salaire débutant : 2 500 €

Code ROME : K1903 - Code FAP : L5Z90

VOUS FAITES PREUVE D'UN INTÉRÊT TOUT AUSSI ÉVIDENT POUR LES QUESTIONS TECHNIQUES ET LE FAIT JURIDIQUE ? VOUS ÊTES PARTICULIÈREMENT SENSIBLE À L'ÉVOLUTION DES DROITS DANS L'UNIVERS NUMÉRIQUE ET À LA GARANTIE DE LEUR RESPECT ? DÉCOUVREZ SANS TARDER LA FONCTION DE DÉLÉGUÉ À LA PROTECTION DES DONNÉES ET LE CARACTÈRE ESSENTIEL DES MISSIONS QUI S'Y RATTACHENT.

Missions

En tant que référent de la politique de protection des données, le DPO assure une triple mission de contrôle, d'information et de conseil.

Au jour le jour, il s'assure du respect de toutes les normes en vigueur sur la question de la protection des données. C'est le volet « contrôle ». Il peut s'agir de règles propres à l'organisation ou, plus généralement, de textes législatifs au niveau national ou européen, par exemple. À ce titre, le délégué à la protection des données garantit notamment le respect du Règlement général sur la protection des données (RGPD).

En cas de non-conformité, il préconise des actions rectificatives. À ce titre, il est amené à opérer un véritable travail de veille informatique et à collaborer étroitement avec le Responsable de la sécurité des systèmes d'information (RSSI), le service juridique ou encore le service des Achats.

La mission d'information et de conseil se poursuit auprès de tous les responsables et sous-traitants touchant de près ou de loin aux données : il s'agit de s'assurer que la structure mène toutes les actions utiles pour sécuriser sa base de données et éviter une utilisation frauduleuse, par des opérateurs externes, des données de l'entreprise, de celles des employés, des clients ou des utilisateurs.

L'obligation de dpo

Le délégué à la protection des données remplace, dans les faits, le correspondant informatique et libertés (CIL), auquel les entreprises avaient l'habitude de faire appel avant le 25 mai 2018. Depuis

cette date, qui correspond à l'entrée en vigueur du RGPD, la présence d'un DPO est devenue obligatoire :

· Pour toutes les entreprises dont les activités principales supposent « un suivi régulier et systématique des personnes à grande échelle », dès lors qu'elles opèrent dans l'espace européen
· Pour toutes les structures publiques, dès lors qu'elles opèrent dans l'espace européen, à l'exception des juridictions agissant dans l'exercice de leur fonction juridictionnelle

Compétences

Plusieurs pré-requis s'imposent au délégué de protection des données. Ce dernier doit justifier de compétences à la croisée du champ technique et du champ juridique :

· Une appétence claire pour les questions de cybersécurité
· Une formation aux règles de pilotage des données personnelles à l'échelle d'une organisation
· Une capacité globale à évaluer les risques cyber et à repérer les failles de sécurité
· Une aptitude à monter et à assurer le suivi d'un programme de conformité en matière de données personnelles
· Une maîtrise des notions de base concernant la protection des données, n'impliquant pas forcément une formation juridique complète
· La capacité à gérer les contrôles d'utilisation des données opérés par la CNIL (Commission nationale de l'informatique et des libertés)

Études

En règle générale, le délégué à la protection des données est détenteur, au minimum, d'un Bac +3. Dans la grande majorité des cas, les aspirants DPO sont passés par un cursus en informatique ou en statistiques. Nombreux sont ceux ayant également suivi une spécialisation en big data.

Selon les données du ministère du Travail, on assiste depuis 2019 à une diversification croissante des profils de DPO : en 2021, 47 % d'entre eux provenaient issus d'autres domaines d'expertise que le droit et l'informatique, soit une progression de 12 % par rapport à 2019. On voit principalement augmenter la part des profils administratifs et financiers ou en lien avec la qualité ou la conformité et l'audit.

L'AVIS DU PROFESSIONNEL

« Le délégué à la protection des données est là pour rassurer et sécuriser une des ressources les plus sensibles au sein de l'entreprise, et pour baliser les chemins d'utilisation. »

Alexis O.
Délégué à la protection des données

QUALITÉS

Pour remplir sa mission dans les meilleures conditions, le Délégué à la protection des données doit présenter plusieurs qualités comportementales et soft skills :
· Un esprit pratique et une aptitude confirmée à la réflexion stratégique, permettant de mettre en place un processus de veille efficace autour de l'exploitation des données personnelles, grâce auquel les écarts et mauvaises utilisations pourront être facilement détectés
· Des compétences avérées en communication afin de recueillir rapidement les informations utiles et d'alerter sur les enjeux
· Une rigueur constante dans le traitement et le signalement des problèmes de conformité.

L'AVIS DU PROFESSIONNEL

« Le DPO est celui qui doit entraîner tout le monde dans la bonne direction, en matière de traitement des données, et assume une responsabilité cruciale là où de très nombreux acteurs sont impliqués. »

Alexis O.
Délégué à la protection des données

Salaire

En France, le salaire moyen d'un DPO varie entre 2 500 et 5 670 euros brut mensuels. La différence de salaire peut être importante :

· Selon la taille de l'entreprise et le secteur dans lequel elle exerce, si le DPO est rattaché à une structure privée
· Et selon le degré d'expérience et d'ancienneté

Où travailler ?

Comme évoqué précédemment, les personnes aptes à exercer les fonctions de délégué à la protection des données peuvent s'orienter aussi bien vers le secteur public que vers le secteur privé.

De nombreuses entreprises sont soumises à l'obligation de s'attacher les services d'un DPO, du fournisseur d'accès à Internet à la compagnie d'assurance, en passant par toutes les entités commerciales collectant les données personnelles de leurs clients.

Dans le contexte de multiplication des entreprises de nature à exploiter les données personnelles de leurs clients ou utilisateurs, et face à un recours toujours plus intense à ces données, les possibilités d'embauche sont nombreuses et sont destinées à augmenter de manière substantielle dans les années à venir.

Parmi les entreprises susceptibles de recruter, il est conseillé de surveiller :

· Les enseignes de la grande distribution, notamment Monoprix, E. Leclerc ou Auchan
· Les assureurs tous secteurs confondus, notamment la Macif, AXA, la Matmut ou la MAAF
· Les banques, comme BNP Paribas, la Caisse d'Épargne ou Natixis
· Les opérateurs de téléphonie mobile et fournisseurs d'accès à internet comme Orange, Bouygues ou SFR
· La Banque de France

Évolution de carrière

Le délégué à la protection des données souhaitant changer de poste au sein de la structure à laquelle il est rattaché peut facilement prétendre à des postes à couleur stratégique et/ou juridique. On voit notamment de nombreux DPO s'orienter vers des postes de responsable des questions européennes, de conseiller stratégique pour l'utilisation des données ou de directeur du département informatique. L'accès à ces différents postes dépend bien entendu de la formation juridique ou technique initiale du candidat.

Il est également possible de postuler à un poste de responsable de projet big data, par exemple.

Avantages et inconvénients

Il est évident que l'un des plus grands atouts du poste de délégué à la protection des données est la polyvalence qu'il implique. Sa situation, au croisement des champs technique, juridique et stratégique, est particulièrement enrichissant et formateur au quotidien.

La polyvalence du poste est aussi, dans une certaine mesure, son inconvénient majeur. Il suppose une attitude de veille et donc de vigilance constante et une possibilité de devoir gérer des crises en cas de mauvaise gestion.

Parmi les avantages, on notera également la relative nouveauté du poste, qui ouvre de nombreuses perspectives en termes d'emploi et de stimulation intellectuelle.

25 ADMINISTRATEUR·RICE CYBERSÉCURITÉ

Niveau d'études : Bac+3

Spé Conseillée : Scientifique

Employabilité : Bonne

Salaire débutant : 2 700 €

Code ROME : M1802 - Code FAP : M2Z

L'ADMINISTRATEUR CYBERSÉCURITÉ EST UN EXPERT DE LA SÉCURITÉ INFORMATIQUE QUI OCCUPE UN RÔLE STRATÉGIQUE AU SEIN DES ENTREPRISES. PARTENAIRE DE CONFIANCE, L'ADMINISTRATEUR CYBERSÉCURITÉ A EN CHARGE LA MAINTENANCE ET L'AMÉLIORATION CONTINUE DES SERVICES INFORMATIQUES DES ORGANISATIONS.
ON DIT DE TOI QUE TU ES RIGOUREUX ET PÉDAGOGUE ? TU AS DE L'ASSURANCE ET SAIS FAIRE PREUVE DE DÉTERMINATION ? NOUS TE CONSEILLONS VIVEMENT DE T'INTÉRESSER AU MÉTIER D'ADMINISTRATEUR CYBERSÉCURITÉ !

Missions

L'administrateur de solutions de sécurité ou administrateur cybersécurité installe, met en production, administre et exploite des solutions de sécurité (antivirus, sondes, firewalls, IAM, etc.). Il participe au bon fonctionnement des solutions de sécurité en garantissant leur maintien en conditions opérationnelles et de sécurité.

Au quotidien, l'administratrice cybersécurité, en plus d'assurer l'administration des solutions, gère leur maintenance et leur exploitation. Elle développe également des actions de sensibilisation auprès des usagers de ces dernières. Ses tâches sont les suivantes :

Administration

· S'assurer du fonctionnement optimal des solutions de sécurité dont il a la charge
· Contribuer au paramétrage des solutions de sécurité, gérer les changements
· Configurer les solutions en conformité avec les normes et standards définis par les experts du domaine, effectuer des revues régulières des règles et paramètres mis en place
· Mettre en place la collecte des logs et des alertes issues des solutions vers un service de détection d'incidents
· Assurer un suivi des actions et une documentation des processus

Maintenance

· Maintenir et faire évoluer les solutions de sécurité de son périmètre, dans un objectif de qualité, de productivité et de sécurité globale

· Assurer le suivi et la remédiation des vulnérabilités identifiées

Exploitation

· Valider l'installation des outils dans l'environnement de production
· Gérer les droits d'accès aux solutions en fonction des profils
· Traiter les incidents ou anomalies ainsi que les exceptions
· Veiller au bon fonctionnement de la remontée des logs et des alertes

Communication

· Contribuer à la sensibilisation et à la formation des utilisateurs aux solutions de sécurité

Compétences

Exercer en qualité d'administrateur cybersécurité demande de posséder de solides connaissances sur les sujets des systèmes et réseaux informatiques :

· Système d'information, de l'urbanisation et de l'architecture du système d'information
· Conception et maintien d'un système d'information sécurisé
· Processus de production
· Sécurité des systèmes d'exploitation
· Sécurité des réseaux et protocoles
· Configuration des outils liés à la sécurité

Savoir-faire

· Capacité à définir des procédures
· Pédagogie sur les sujets de cybersécurité
· Capacité de travail en équipe

Études

Si vous envisagez de faire carrière en tant qu'administrateur cybersécurité, vous devrez justifier d'un diplôme informatique de niveau Bac+3.

Ce métier est accessible à partir d'une expérience préalable en environnement de production, d'exploitation ou de support.

Salaire

La rémunération d'un administrateur cybersécurité diffère en fonction de la typologie de l'entreprise où il est amené à exercer et peut varier selon les missions qui lui sont confiées et son niveau d'expérience professionnelle.

Le salaire médian pour les administrateurs cybersécurité est de 38 000 euros annuels. Les profils débutants pourront commencer leur carrière sur la base d'un salaire annuel estimé à 32 000 euros, tandis que les travailleurs les plus expérimentés pourront gagner jusqu'à 42 500 euros par an.

A l'international, aux Etats-Unis par exemple, il peut percevoir un salaire annuel moyen de 90 000 dollars. Au Royaume-Uni, l'administrateur cybersécurité pourra prétendre à environ 26 000 livres annuelles.

Où travailler ?

Les administrateurs cybersécurité interviennent au sein d'organisations publiques comme privées. Ils peuvent par exemple exercer dans les secteurs industriels ou pour des sociétés de services.Voici un exemple d'entreprises et institutions qui font appel à des administrateurs cybersécurité :

· Editeurs de logiciels et entreprises informatiques
· Secteur bancaire
· Secteur des télécommunications
· Sociétés de conseil en Hautes Technologies

Évolution de carrière

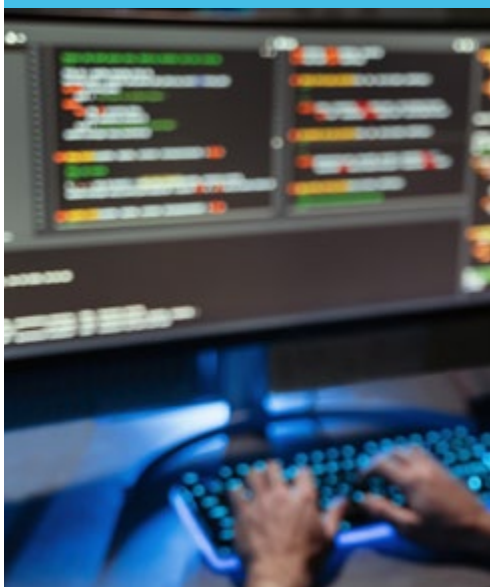
En règle générale, les administrateurs cybersécurité évoluent vers des postes à responsabilité ou de direction, tels que Directeur du Service d'Information (DSI) ou Responsable de la Sécurité et des Systèmes Informatiques (RSSI).

Il leur est également possible d'opter pour un poste de responsable systèmes et réseaux. Enfin, depuis le rapprochement technologique grandissant entre

QUALITÉS

· Rigueur
· Pédagogie
· Communication
· Assurance

L'administrateur cybersécurité installe et gère l'exploitation des systèmes de solutions de sécurité de l'entreprise. Il garantit le maintien et le bon fonctionnement de l'ensemble des outils et process de sécurité. Enfin, l'administrateur cybersécurité sensibilise les équipes internes et utilisateurs externes de ces solutions à une utilisation raisonnée et optimisée des outils et services informatiques.



l'administration systèmes et le développement informatique, de plus en plus d'administrateurs cybersécurité s'orientent vers des postes de DevOps.

Freelance

L'administrateur cybersécurité peut exercer en tant que freelance indépendant. Il pourra créer un statut d'auto-entrepreneur ou une société individuelle auprès de la Chambre de Commerce. Il lui sera ainsi possible de facturer ses prestations à tout type de clients.

Le tarif journalier moyen d'un administrateur cybersécurité freelance est de 600 euros par jour. Ce tarif peut augmenter jusqu'à 800 euros par jour pour les profils les plus expérimentés.

Avantages et inconvénients

Tout le long de son parcours, l'administrateur cybersécurité doit réaliser un important travail de veille afin de mettre à jour ses compétences s'agissant de l'apparition de nouvelles vulnérabilités informatiques.

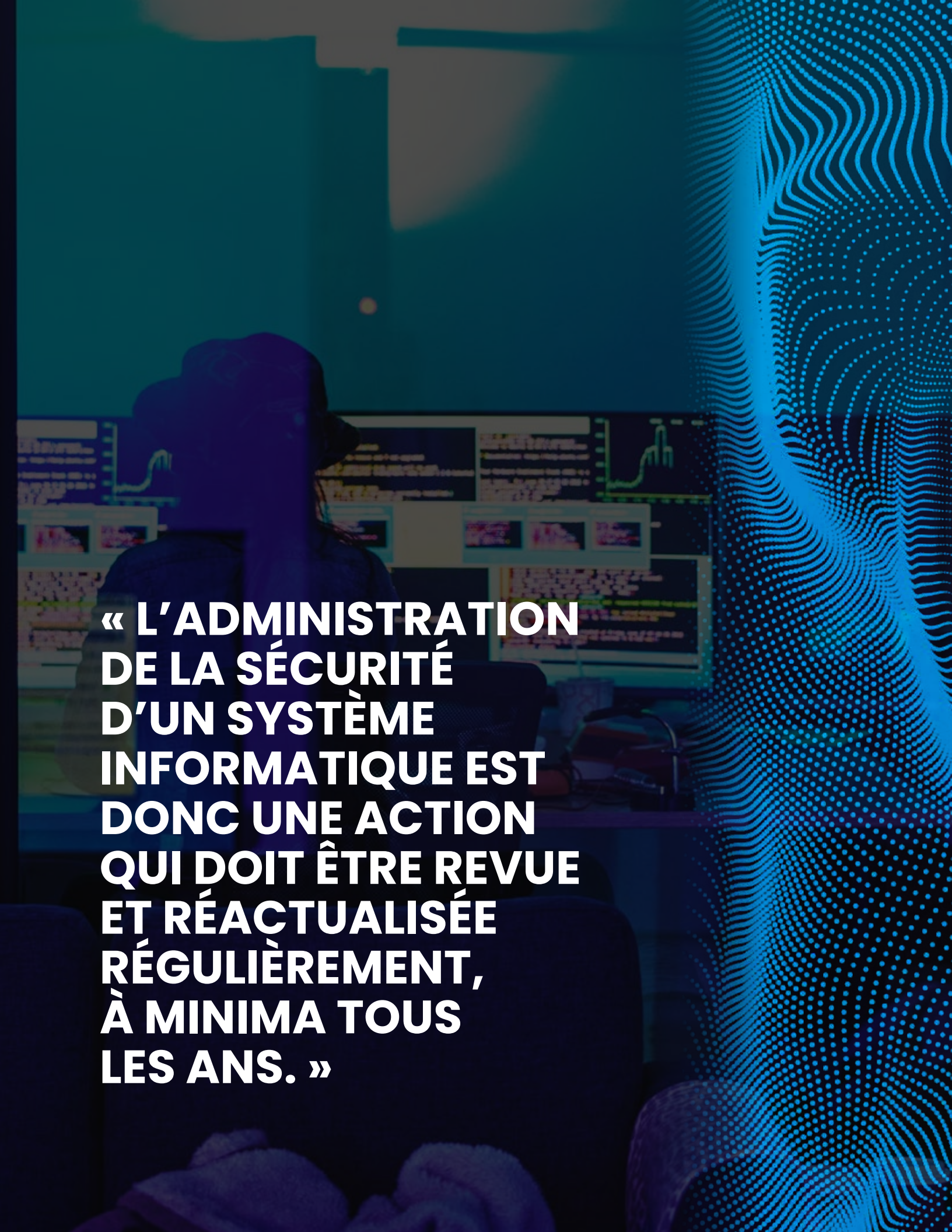
Son travail, très prenant, l'amène parfois à réaliser des journées ou nuits d'astreinte pour régler des problèmes de sécurité.

Dans un contexte de transformation numérique et de digitalisation croissante des informations dans le quotidien et dans la stratégie des entreprises, il devra en permanence opérer un ajustement entre les besoins des projets et l'agencement des informations, afin que ces dernières demeurent fiables et cohérentes en fonction de chaque client. Ce travail d'ajustement nécessite une grande adaptabilité et une forte polyvalence.

Comment le devenir ?

L'administrateur cybersécurité installe et gère l'exploitation des systèmes de solutions de sécurité de l'entreprise. En plus de compétences informatiques de base, il vous faudra maîtriser la sécurité des systèmes d'exploitation, la sécurité des réseaux et protocoles et la configuration des outils liés à la cybersécurité. Pour le devenir, vous devrez justifier d'un diplôme informatique de niveau Bac+3 avec une spécialité en cybersécurité. Ce métier est accessible à partir d'une expérience préalable en environnement de production, d'exploitation ou de support. Les qualités nécessaires à l'exercice de ce poste sont notamment la rigueur, la pédagogie, et la communication. Vous débuterez avec un salaire avoisinant les 32 000 euros annuels et pourrez gagner jusqu'à 42 500 euros annuels après quelques années d'expérience dans le métier.

« LA SÉCURITÉ INFORMATIQUE EST CRUCIALE DANS TOUTES LES ORGANISATIONS. LA SÉCURITÉ DES SYSTÈMES INFORMATIQUES INTERNES (RÉSEAUX) ET EXTERNES À L'ENTREPRISE (TERMINAUX NOMADES) PEUVENT FAIRE L'OBJET D'ATTAQUES ET D'INTRUSIONS INFORMATIQUES MALVEILLANTES QUI RENDENT CRITIQUES L'UTILISATION ET L'EXPLOITATION DES OUTILS DE L'ENTREPRISE. POUR ASSURER LA SÛRETÉ DE CETTE ADMINISTRATION, IL CONVIENT DE METTRE EN PLACE UN ENSEMBLE DE PROCESSUS ET DE MESURES, EN PARTIE TECHNIQUES MAIS PAS SEULEMENT, VISANT À ASSURER LE MAINTIEN DE LA SÉCURITÉ DU SYSTÈME D'INFORMATION. »



« L'ADMINISTRATION DE LA SÉCURITÉ D'UN SYSTÈME INFORMATIQUE EST DONC UNE ACTION QUI DOIT ÊTRE REVUE ET RÉACTUALISÉE RÉGULIÈREMENT, À MINIMA TOUS LES ANS. »

Niveau d'études :	Bac+3
Spé Conseillée :	Scientifique
Employabilité :	Bonne
Salaire débutant :	3 000 €

Code ROME : M1802 - Code FAP : M2Z

UNE ORGANISATION EST TOUJOURS CONFRONTÉE AU RISQUE DE SE TROUVER EN VIOLATION DE L'UNE OU L'AUTRE DES MULTIPLES LOIS ET RÉGLEMENTATIONS QUI LA CONCERNENT. UN RESPONSABLE DE LA GOUVERNANCE, LE RISQUE ET LA CONFORMITÉ (GRC) DOIT METTRE EN PLACE UNE APPROCHE STRUCTURÉE VISANT À ALIGNER L'INFORMATIQUE SUR LES OBJECTIFS DE L'ENTREPRISE, TOUT EN GÉRANT EFFICACEMENT LES RISQUES ET EN RESPECTANT LES EXIGENCES DE CONFORMITÉ.

Missions

Les responsables de la conformité aux risques sont considérés comme une composante essentielle de la gouvernance d'entreprise. Ils sont également chargés de déterminer comment une organisation peut être gérée et gouvernée. Ces responsabilités comprennent le maintien de bonnes relations entre les parties prenantes et l'adhésion aux objectifs fixés par l'organisation.

Ces professionnels effectuent donc des audits à intervalles réguliers et mettent en place des systèmes de contrôle de la conception, en conseillant la direction sur les risques éventuels qui pourraient survenir et sur les politiques de l'organisation.

La principale tâche d'un responsable de la conformité est de préserver l'intégrité éthique de l'organisation et de veiller à ce que les activités commerciales soient menées dans un cadre réglementaire. Ces professionnels mettent en œuvre le processus de gestion des risques en planifiant minutieusement les activités et en appliquant les politiques au sein de l'organisation.

Les rôles et les responsabilités d'un responsable de la conformité varient selon le secteur d'activité, mais les responsabilités types sont les suivantes :

· Ils sont chargés de veiller à ce que toutes les directives essentielles soient mises en place de manière appropriée, en respectant précisément les normes et réglementations du secteur d'activité de l'entreprise

· Ils effectuent des audits et des examens internes à intervalles réguliers pour s'assurer que les procédures de conformité sont régulièrement suivies
· Le rôle du gestionnaire des risques de conformité concerne également la sécurité des employés et des entreprises. Il doit s'assurer que toutes les tâches sont effectuées avec une grande précision
· Ils doivent s'assurer que tous les employés sont parfaitement informés des politiques, des réglementations et des processus de l'organisation
· Ils doivent conseiller la direction dans la mise en œuvre de programmes de conformité

Compétences

La gouvernance, le risque et la conformité (GRC), trois domaines extrêmement complexes et parfois chronophages. Résultat, ces responsables sont des «moutons à cinq pattes». Il faut en effet maitriser les différents rouages de la protection des données, la réglementation en vigueur concernant les domaines d'activité de l'employeur, et en particulier celle liée à la protection des données à caractère personnel (RGPD). On peut également citer la directive sur les services de paiement de l'Union européenne, ou DSP2. C'est l'une des réglementations les plus récentes concernant les services de paiement et les sociétés de traitement des paiements. Entrée en vigueur en septembre 2018, cette directive de l'UE a un impact majeur sur la façon dont les banques, les sociétés de traitement des paiements et les fintech conduisent leur activité à l'échelle mondiale.

Les compétences en informatique et en gouvernance des données sont également indispensables. Commencer sa carrière en tant que responsable GRC n'est donc pas une tâche facile. Ce poste exige une expertise détaillée et une attention aux moindres détails.

Études

Il est possible de suivre différentes études, car ce poste présente différentes facettes. Des études de droit sont les bienvenues comme ces études en tant qu'ingénieur en cybersécurité. Une formation de DPO (Délégué à la protection des données) complétée par différentes certifications peut également permettre de commencer une carrière de responsable GRC. Quels que soient le diplôme, ou les diplômes, il est impératif de faire preuve de beaucoup de rigueur.

Diplôme

Maîtrise, ou équivalent, en gestion des affaires, en gestion des technologies de l'information ou dans un domaine connexe.

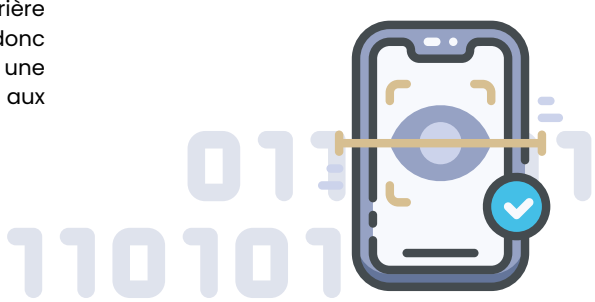
Auditeur de systèmes d'information certifié (CISA- Certified Information Systems Auditor). Créée en 1978, c'est le standard de réussite accepté à l'échelle mondiale par les professionnels de l'audit, du contrôle et de la sécurité des systèmes d'information (SI).

Bac

Baccalauréat scientifique ou littéraire avec un intérêt certain pour l'informatique et les mathématiques.

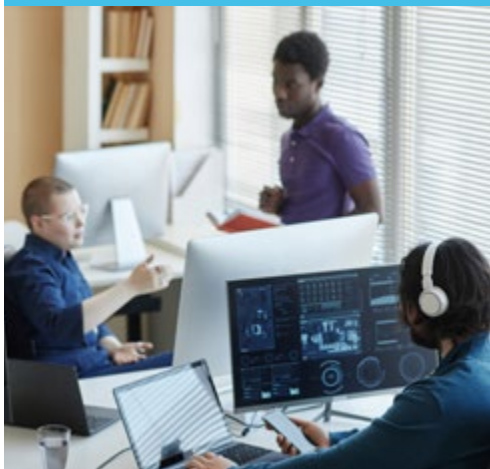
Salaire

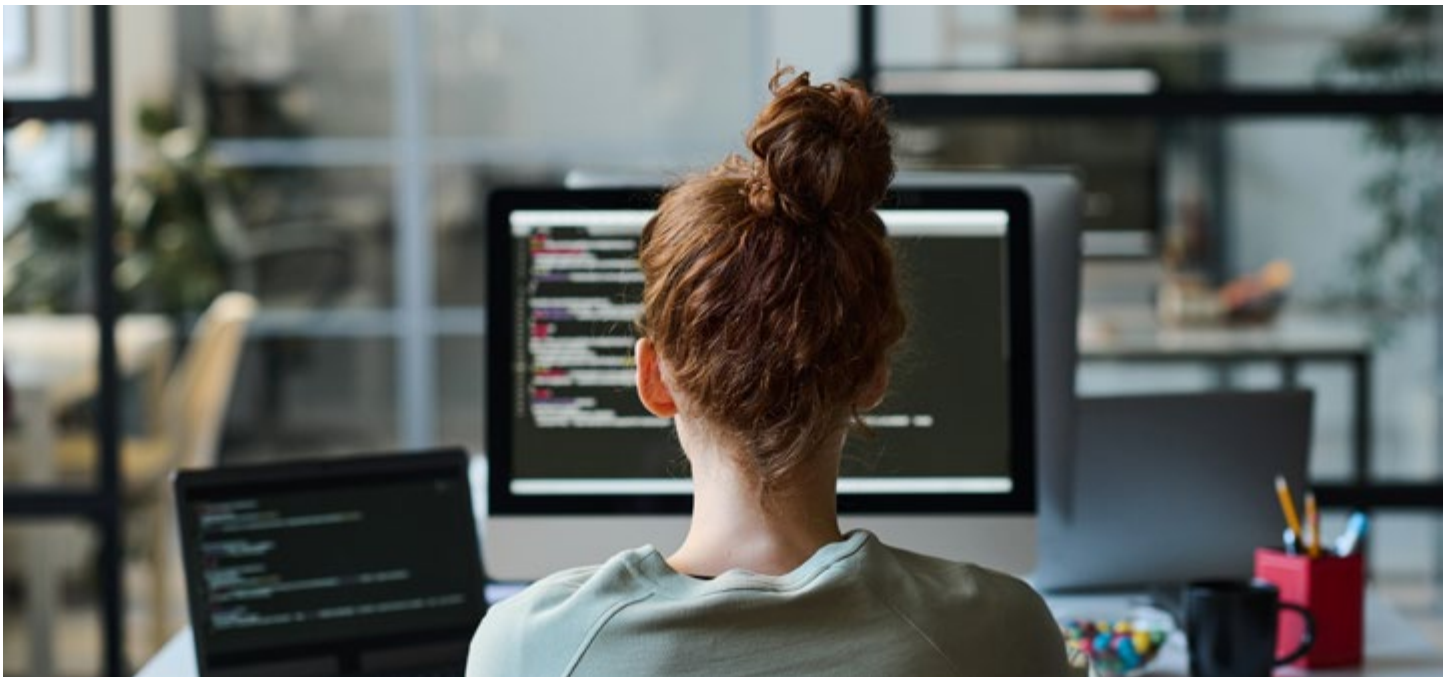
Ce type de profil peut être vu comme un mouton à cinq pattes. Il requiert en effet de solides compétences dans différents domaines complexes. C'est la raison pour laquelle, le salaire est élevé. Il se situe entre 70 000 euros brut et 150 000 euros brut pour les auditeurs les plus confirmés.



QUALITÉS

Les rôles et les responsabilités de ces professionnels sont larges et étendus. Ces responsabilités exigent d'être à la fois le moteur d'une culture d'éthique et de conformité et de surveiller en permanence les activités d'éthique et de conformité dans toute l'organisation. Ce poste convient donc aux personnes qui prêtent attention aux moindres détails au sein de l'organisation. Un responsable de la conformité doit avoir une connaissance approfondie des politiques de sécurité telles que les normes ISO, les politiques de contrôle et d'abus, les réglementations, le suivi, l'évaluation, l'examen et le rapport associés à l'audit. Une solide expérience en matière d'audits internes ou externes (financiers/opérationnels/IT) est également requise. Enfin, il est essentiel de posséder d'excellentes compétences en communication écrite et orale afin d'être capable de communiquer avec les décideurs et autres collaborateurs.





Où travailler ?

Si toutes les entreprises sont plus ou moins concernées par la gouvernance, le risque et la conformité, certaines ont plus de contraintes que d'autres. C'est le cas des OIV (Opérateurs d'importance vitale) et des OSE (Opérateur de Services Essentiels), mais également de toutes les entreprises exerçant dans un domaine très règlementé comme l'assurance et la finance.

Évolution de carrière

De par son profil technique et juridique, un responsable de la gouvernance, le risque et la conformité (GRC) peut devenir RSSI. Un responsable de la sécurité des systèmes d'information définit et développe la politique de sécurité de l'information de son entreprise. Il est garant de sa mise en œuvre et en assure le suivi. Il peut aussi devenir indépendant pour répondre aux besoins de nombreuses entreprises.

Freelance

La nécessité d'avoir une vision globale et actualisée en permanence des risques liés aux activités d'une entreprise est difficilement compatible avec un job d'indépendant.

Avantages et inconvénients

La GRC touchant de nombreux domaines, elle permet d'avoir des tâches et des objectifs très variés. Revers de la médaille, la maitrise de ces trois composants implique une veille permanente, voire des formations pour maitriser les différentes technologies et mieux appréhender les risques actuels et futurs.

Comment le devenir ?

La gouvernance des données, la gestion des risques et la conformité aux différentes réglementations et lois sont devenus des enjeux majeurs pour les entreprises. C'est la raison pour laquelle, elles recrutent de tels profils. Pour devenir responsable GRC, il est nécessaire d'avoir de bonnes compétences en informatique et de maitriser les différents aspects juridiques concernant la protection des données. Un Bac scientifique ou littéraire suivi d'études en droit (avec en option la cybersécurité ou le management des systèmes d'information) est recommandé.

AUDITEUR·RICE DE SÉCURITÉ TECHNIQUE

Niveau d'études : Bac+3 à Bac+5

Spé Conseillée : Scientifique

Employabilité : Très bonne

Salaire débutant : 3 100 €

Code ROME : M1802 - Code FAP : M2Z

VOUS SOUHAITEZ ACCOMPAGNER LES ENTREPRISES DANS LA SÉCURISATION DE LEUR SYSTÈME INFORMATIQUE ? VOUS VOUS SENTEZ CAPABLE DE TROUVER LA FAILLE, LA VULNÉRABILITÉ CACHÉE ET D'APPORTER DES SOLUTIONS DE REMÉDIATION À DES SITUATIONS DE CYBERMENACES ? VOUS SAVEZ JOUER DE VOTRE CRÉATIVITÉ DANS LA RÉSOLUTION DE PROBLÈMES COMPLEXES ? VOUS FAITES PREUVE DE PÉDAGOGIE LORS DE SITUATIONS DE CRISE ? CES COMPÉTENCES ET QUALITÉS FERONT DE VOUS UN AUDITEUR DE SÉCURITÉ TECHNIQUE D'EXCEPTION !

Missions

L'auditeur de sécurité technique conduit des évaluations techniques de la sécurité d'environnements informatiques.

Son rôle est d'identifier les vulnérabilités et de proposer des actions de remédiation.

Il peut réaliser différents types d'audits en fonction de son périmètre d'activité (tests d'intrusion, audit de code, revue de configuration, etc.).

Il réalise plusieurs missions principales, depuis la réalisation d'audits, la réalisation ou le pilotage de scans de vulnérabilités, ainsi qu'une activité de veille technique. Au quotidien, l'auditeur de sécurité technique est ainsi chargé de :

Concernant le volet réalisation des audits :

· Adopter une vision globale du système d'information à auditer
· Définir les plans d'audits au sein du système d'information de l'organisation
· Exécuter et documenter des audits de sécurité sur différents environnements informatiques en s'assurant du respect du cadre réglementaire encadrant ces pratiques
· Collecter les éléments de configuration des équipements à auditer et réaliser une revue des configurations (audits de configuration)
· Collecter les éléments d'architecture des systèmes à auditer et réaliser une revue de l'architecture (audit d'architecture)
· Réaliser une revue du code source des composants de l'environnement (audit de code)

· Définir les scénarios d'attaques et réaliser des attaques sur l'environnement cible (tests d'intrusion)

Concernant le volet réalisation ou pilotage de la mise en œuvre de scans de vulnérabilités et de contrôles techniques, en continu et de manière automatisée :

· Procéder à des interviews des équipes pour évaluer les impacts pour l'organisation des vulnérabilités détectées
· Rédiger des rapports intégrant une analyse des vulnérabilités rencontrées et une identification des causes ; mettre en évidence et évaluer les risques de sécurité et les impacts pour les métiers
· Définir les recommandations permettant de remédier aux risques découlant des vulnérabilités découvertes
· Collaborer avec les équipes informatiques pour mettre en œuvre les recommandations techniques
· Produire des tableaux de bord du niveau de sécurité et de conformité

Concernant la veille technique :

· Assurer une veille permanente vis-à-vis des scénarios d'attaques, des nouvelles menaces et des vulnérabilités associées et vis-à-vis du développement de nouveaux contextes de tests
· Elaborer des outils utilisés pour les audits
· Identifier de nouveaux moyens pour détecter des failles qui peuvent toucher un système

Compétences

Exercer en qualité d'auditeur de sécurité technique suppose de disposer de solides compétences en sécurité des systèmes d'information, en cyberdéfense ainsi qu'en droit informatique .

Ainsi, les compétences coeur de métier de l'auditrice de sécurité technique sont les suivantes :

· Sécurité des systèmes d'exploitation
· Sécurité des réseaux et protocoles
· Connaissance des couches applicatives
· Connaissance de la gouvernance, des normes et des standards : maîtrise des méthodologies d'audits
· Tests d'intrusion : maîtrise des techniques d'audits techniques de sécurité
· Cyberdéfense : connaissance des techniques d'attaques et d'intrusion
· Cyberdéfense : connaissance des vulnérabilités des environnements
· Connaissance en rétro-ingénierie de systèmes (reverse engineering)
· Scripting
· Connaissance juridique en matière de droit informatique lié à la sécurité des systèmes d'information et à la protection des données
· Veille technologique en cybersécurité et étude des tendances

Études

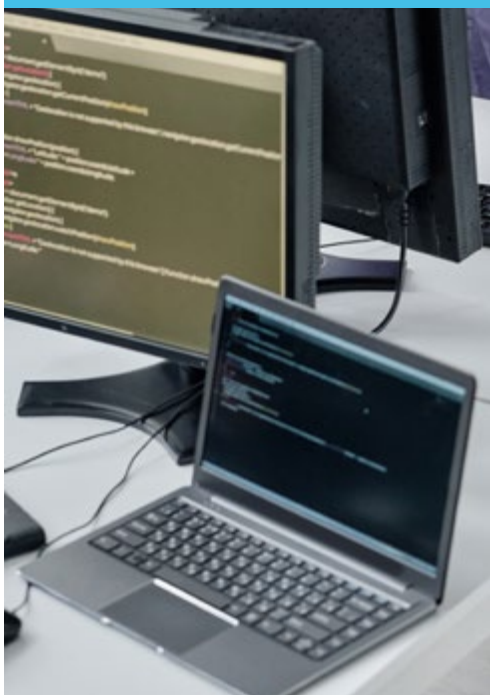
Pour faire carrière en tant qu'auditeur de sécurité technique, vous devrez justifier d'un diplôme informatique de niveau Bac+3 à Bac+5 et d'une spécialisation en cybersécurité.

Ce métier est accessible avec l'obtention d'une certification PASSi (Prestataire d'Audit de Sécurité des Systèmes d'information).

QUALITÉS

· Capacité de synthèse et de vulgarisation pour des publics non techniques
· Rédaction de rapports adaptés à différents niveaux d'interlocuteurs
· Sens éthique
· Capacité de travail en équipe
· Rigueur

L'auditeur de sécurité technique est un professionnel de la cybersécurité qui réalise des évaluations techniques de la sécurité d'environnements informatiques. Son rôle est d'identifier les vulnérabilités du système d'information et de proposer des actions de remédiation. Pour ce faire, l'auditeur de sécurité technique réalise plusieurs missions principales, depuis la réalisation d'audits, la réalisation ou le pilotage de scans de vulnérabilités, ainsi qu'une activité de veille technique.



Salaire

La rémunération d'un auditeur de sécurité technique diffère en fonction de la typologie de l'entreprise où il est amené à exercer, selon les missions qui lui sont confiées et va dépendre de son niveau d'expérience professionnelle.

Le salaire médian pour les auditeurs de sécurité techniques en France est de 5 073 euros brut par mois. Débutant, il sera rémunéré environ 3 165 euros par mois soit approximativement 38 000 euros annuels, les profils confirmés pouvant prétendre jusqu'à 10 040 euros mensuels soit environ 120 500 euros annuels.

À l'international, en Suisse par exemple, il peut percevoir un salaire annuel moyen de 130 000 CHF. Aux Etats-Unis, un auditeur de sécurité sera rémunéré en moyenne 70 000 dollars annuels.

Où travailler ?

Les auditeurs de sécurité techniques interviennent au sein d'organisations publiques comme privées. Ils peuvent par exemple exercer dans les secteurs industriels ou pour des sociétés de services. Voici un exemple d'entreprises et institutions qui font appel à des auditeurs de sécurité techniques :

· Editeurs de logiciels et entreprises informatiques
· Secteur bancaire
· Secteur des télécommunications
· Sociétés de conseil en Hautes Technologies

Évolution de carrière

L'auditeur de sécurité technique peut être amené à réaliser des audits plus ambitieux de type red team qui visent à simuler des attaques en grandeur réelle dans le but de tester les défenses de l'organisation. Il peut aussi faire des audits dans une approche purple team afin d'entraîner les équipes de détection des incidents de cybersécurité.

Avoir été auditeur interne de sécurité technique constitue souvent une passerelle afin de pouvoir évoluer vers des postes de responsable sécurité ou encore consultant mais aussi auditeur tierce partie et auditeur interne QSE (qualité, sécurité, environnement).

Freelance

L'auditeur de sécurité technique peut exercer en tant que freelance. Il devra créer un statut d'auto-entrepreneur ou une société individuelle auprès de la Chambre de Commerce. Il lui sera ainsi possible de facturer ses prestations à tout type de clients.

Le tarif journalier moyen d'une auditrice de sécurité technique freelance est de 600 euros. Ce tarif peut grimper jusqu'à 1 200 euros par jour pour les profils les plus expérimentés.

Avantages et inconvénients

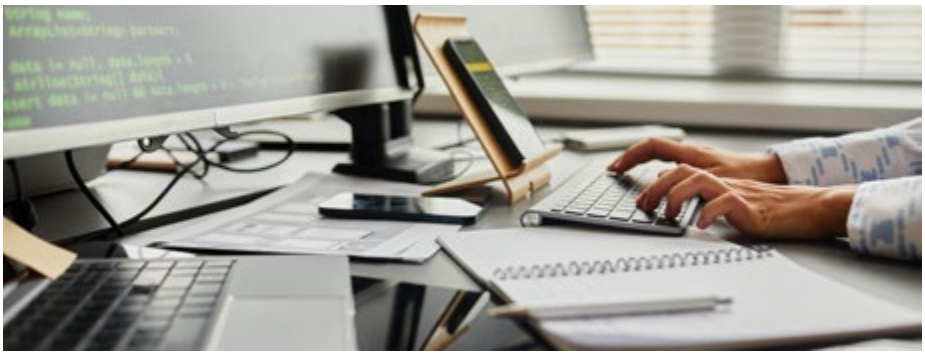
L'auditeur de sécurité technique doit parfaitement comprendre les besoins du client et définir sa problématique technique en analysant son système d'information. Il sera alors en mesure de trouver des solutions pour définir et mettre en œuvre une politique de sécurité adaptée. C'est un métier dynamisant qui demande de faire preuve de créativité afin de solutionner des problèmes rapidement

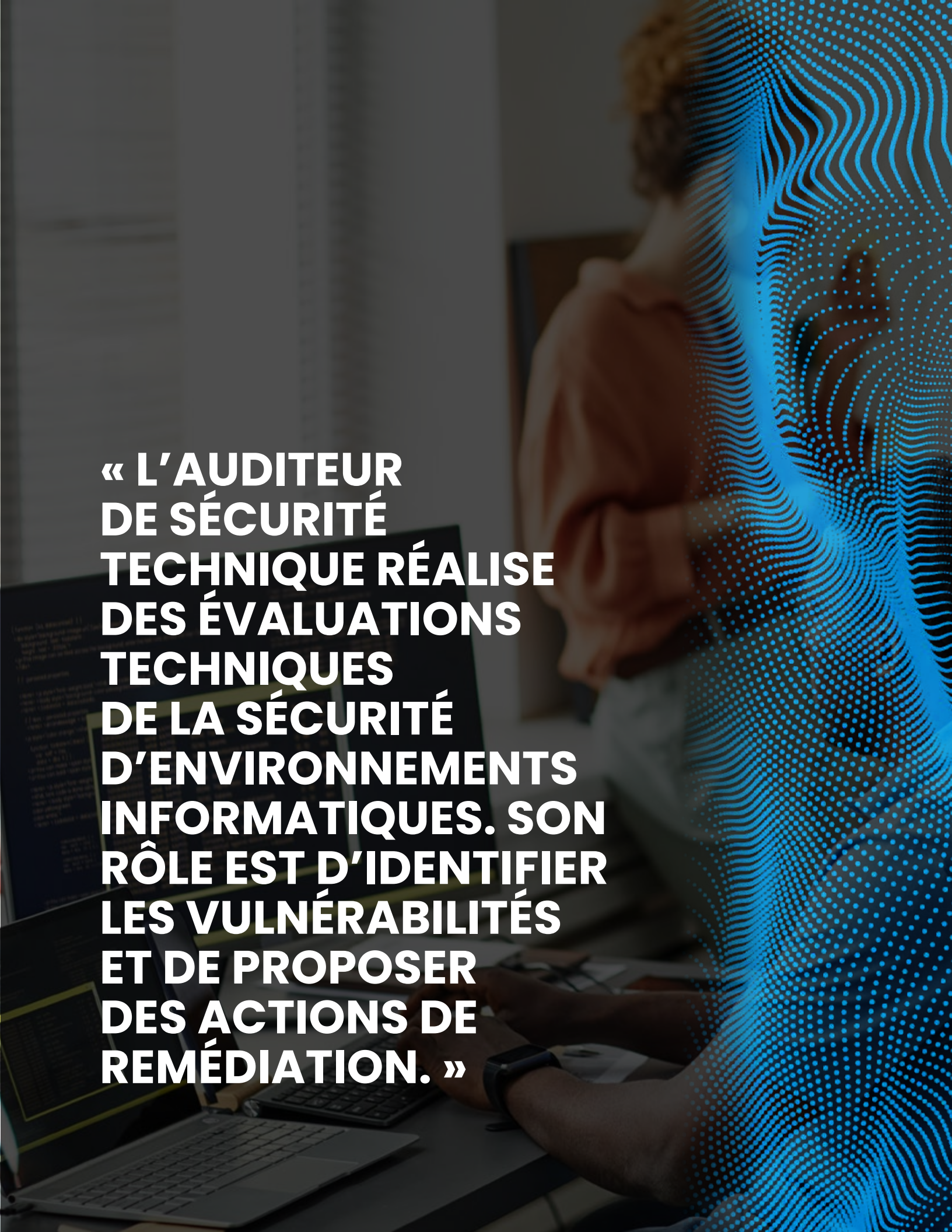
Il intervient souvent dans des situations de crise stressantes pour les entreprises, aussi il devra faire preuve de recul et de pédagogie auprès de clients affectés par une situation de cybermenace.

Ce métier est en perpétuel changement dans la mesure où les cybermenaces à traiter sont toutes différentes et inédites selon les entreprises auditées. L'auditeur de sécurité technique s'ennuie donc très rarement dans son quotidien professionnel !

Comment le devenir ?

Faire le choix de devenir auditeur de sécurité technique suppose l'obtention d'un diplôme informatique de niveau Bac+3 à Bac+5 avec une spécialisation en cybersécurité. Le salaire médian pour les auditeurs de sécurité technique qui exercent en France est d'environ 60 000 euros annuels. L'auditeur de sécurité technique exerce un métier qui demande une grande réactivité et une capacité à communiquer avec différents collaborateurs au sein d'une organisation. L'avantage de ce poste est que les missions sont variées et à chaque fois différentes en fonction des entreprises et des situations de sécurité informatique à traiter. Avoir été auditeur de sécurité technique constitue souvent une passerelle pour évoluer vers des postes de responsable sécurité ou encore consultant mais aussi auditrice tierce partie et auditeur interne QSE (qualité, sécurité, environnement).





« L'AUDITEUR DE SÉCURITÉ TECHNIQUE RÉALISE DES ÉVALUATIONS TECHNIQUES DE LA SÉCURITÉ D'ENVIRONNEMENTS INFORMATIQUES. SON RÔLE EST D'IDENTIFIER LES VULNÉRABILITÉS ET DE PROPOSER DES ACTIONS DE REMÉDIATION. »

28

DEVSECOPS

Niveau d'études : Bac+5

Spé Conseillée : Scientifique

Employabilité : Bonne

Salaire débutant : 3 000 €

Code ROME : M1802 - Code FAP : M2Z

VOUS AVEZ UN SENS DU DÉTAIL À TOUTE ÉPREUVE ET SAVEZ PROCÉDER DE MANIÈRE MÉTHODIQUE POUR DÉCELER LA PLUS PETITE TAILLE DANS UN SYSTÈME DONNÉ ? VOUS AVEZ DONC DE BONNES BASES POUR ENVISAGER DE REJOINDRE UNE ÉQUIPE DE SÉCURITÉ INFORMATIQUE EN TANT QUE DEVSECOPS. CE DÉVELOPPEUR TRÈS PARTICULIER A LA MISSION DE GARANTIR UN NIVEAU DE SÉCURITÉ OPTIMALE TOUT AU LONG DU CYCLE DE VIE D'UN PRODUIT INFORMATIQUE, D'UN LOGICIEL, D'UN PROJET WEB OU D'UN SYSTÈME DE DONNÉES. IL JOUE DONC UN RÔLE DE PILIER POUR TOUTES LES QUESTIONS DE QUALITÉ FINALE, DE SATISFACTION DES UTILISATEURS ET DE PROTECTION DES ENTREPRISES. VOICI COMMENT REJOINDRE LE CERCLE PRIVÉ DE CES GARANTS PERMANENTS DE LA STABILITÉ.

Missions

La mission du DevSecOps consiste à intégrer la dimension « sécurité » à toutes les étapes d'un projet informatique et à l'automatiser. Son objectif final est clair : il s'agit d'assurer le meilleur niveau de sécurité à tous les niveaux afin de contrer d'éventuelles attaques.

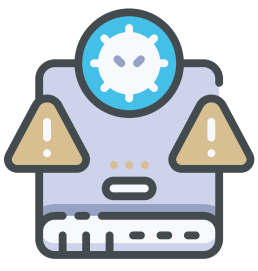
Le DevSecOps est notamment amené à procéder à des audits d'architecture applicative, à des audits de code et à l'évaluation de maturité de divers processus DevSecOps. Il doit être préparé pour contribuer à l'élaboration de nombreux schémas directeurs et de trajectoires de mise en conformité, suite à l'analyse des risques.

Compétences

On peut découper les missions du Spécialiste en développement sécurité selon trois niveaux d'intervention : la conception, le soutien aux équipes de développement et le partage de connaissance, assorti d'un travail de veille technologique.

En matière de conception, le DevSecOps devra :

· Définir ou contribuer à la définition des guides de développement sécurisé
· Et contribuer au choix des solutions de revue de code



Auprès des équipes de développement, il est tenu de :

· Contribuer à la rédaction des exigences de sécurité applicative
· S'assurer du respect des bonnes pratiques de sécurité du développement sur les projets
· Prendre part, en phase d'intégration, aux sprints visant à suivre les revues sécurité pour les développements en méthode agile
· Prendre en main la formation des développeurs aux techniques de développement sécurisé et aux risques de sécurité
· Former les développeurs aux outils de revue de code
· Évaluer la bonne mise en œuvre des exigences de sécurité en conduisant des audits applicatifs ainsi que des revues de code
· Définir les priorités face aux vulnérabilités rencontrées et accompagner les développeurs dans la bonne prise en compte des mesures correctives

Sur le plan du partage de connaissances et de la veille technologique, ce spécialiste de la sécurité a pour fonction :

· D'assurer une veille technologique portant sur les techniques de développement sécurisé
· Et de proposer des solutions afin d'améliorer la sécurité sur son périmètre d'expertise

Lorsque la mission est conduite dans le cadre d'une démarche agile, le spécialiste en développement sécurisé contribue à définir les users stories et les abusers stories, afin d'assurer un meilleur suivi et une meilleure prise en compte des anomalies. C'est le propre de la démarche DevSecOps.

Au-delà des pures compétences en sécurité applicative, le métier requiert des connaissances en sécurité des middlewares. Il doit aussi être parfaitement au fait des différents langages de conception et de la pratique des codes embarqués.

Études

La fonction de DevSecOps est accessible aux détenteurs d'un Bac+5. La validation d'une spécialisation en développement est un pré-requis quasiment obligatoire ; une spécialisation en cybersécurité est un plus fortement apprécié par les recruteurs.

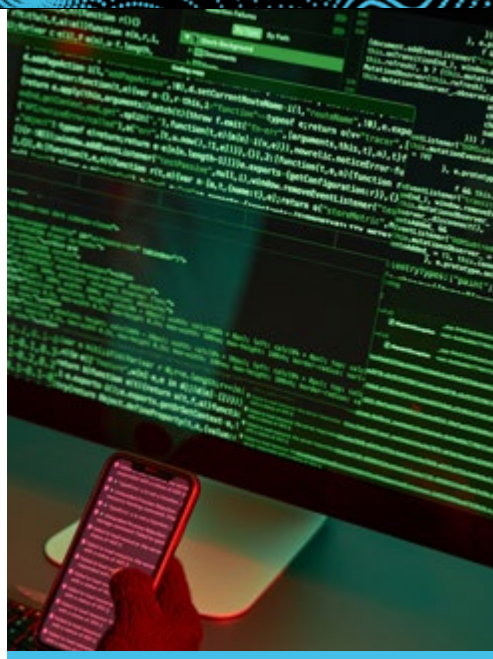
Par ailleurs, une première expérience en Développement est souvent la manière la plus naturelle d'accéder à un poste de ce niveau.

Salaire

Le salaire moyen d'un DevSecOps peut avoisiner 3 000 euros brut mensuels en début de carrière. En moyenne, le salaire haut, après 5 années passées sur ce type de poste, se situe aux alentours de 5 600 euros brut mensuels. Pour un technicien aguerri justifiant de spécialisations et de plus de 10 années d'exercice, le chiffre peut grimper jusqu'à 6 800 euros brut par mois.

0110101
110101

« SA MISSION : METTRE EN PLACE DES INDICATEURS QUI PERMETTENT DE CONNAÎTRE LA VULNÉRABILITÉ DU PROJET À L'INSTANT T. »



QUALITÉS

· L'acuité technique, avec une grande curiosité et un goût pour la mise à jour perpétuelle des connaissances, afin de ne manquer aucune menace de sécurité ;
· Des qualités d'observation indéniables, alliées à une capacité de concentration de niveau supérieur et un sens du détail sans faille ;
· Un sens de la pédagogie avéré, afin de mobiliser efficacement tous les autres spécialistes intervenant sur ou affectés par les incidents de sécurité.

Un bon DevSecOps doit donc faire preuve de constance et de vigilance soutenue. Il doit par ailleurs trouver le juste équilibre entre une compétence technique de haut niveau et des aptitudes relationnelles et communicationnelles indispensables.

Où travailler ?

Il existe une forte demande de DevSecOps, dans une grande variété de domaines, et cela s'explique de manière très simple : la fonction revêt une importance de premier plan pour toutes les entreprises de taille raisonnable opérant dans la sphère informatique ou en lien direct avec le web. Leur nombre étant colossal à cette heure, les DevSecOps ont un large choix au moment de la recherche d'emploi.

Les sociétés développant des logiciels et des projets numériques sont à surveiller de très près, de même que celles qui produisent des jeux vidéo. On pourra aussi s'intéresser aux structures liées à des activités de recherche, mais aussi aux agences actives sur les questions de cyberdéfense et aux fournisseurs de services de banque et assurance, entre autres.

Évolution de carrière

Le spécialiste en développement sécurité peut tout à fait envisager de bifurquer sur un poste de spécialiste sécurité d'un domaine technique. À ce titre, il assurera un rôle de conseil, d'assistance, d'information, de formation et d'alerte sur son domaine de prédilection : système, réseau, composants industriels, IoT, active directory, cloud, IAM ou intelligence artificielle, par exemple. Une formation complémentaire peut s'avérer nécessaire pour accéder à ce type de poste.

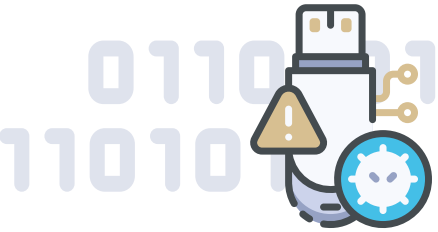
Il est également envisageable de viser un poste d'architecte sécurité, après validation d'une formation complémentaire.

L'évolution la plus naturelle consiste néanmoins à prendre la fonction d'un chef sécurité de projet. Les compétences en pédagogie, en communication et en compréhension transversale des enjeux techniques prédisposent les DevSecOps bénéficiant de plusieurs années d'expérience à endosser ces responsabilités.

Avantages et inconvénients

Pour Leo A., être DevSecOps, c'est une opportunité assez rare de faire jouer à plein sa curiosité et d'échapper au sentiment des missions trop répétitives. La fonction nécessite en effet une mise à jour régulière des connaissances et une intégration des nouveautés techniques, dans le but de maintenir un niveau de sécurité optimale sur tous les systèmes de l'entreprise.

L'un des principaux défis tient à l'obligation de haute concentration et de vigilance permanente, afin de ne passer à côté d'aucune vulnérabilité qui mettrait en danger l'intégrité des systèmes d'information.



Niveau d'études : Bac+3

Spé Conseillée : Scientifique

Employabilité : Bonne

Salaire débutant : 3 000 €

Code ROME : M1802 - Code FAP : M2Z

VOUS AVEZ UNE APPÉTENCE ÉVIDENTE POUR LA DÉFINITION D'AXES STRATÉGIQUES, LES PROJETS PARFAITEMENT CIBLÉS ET LES DÉFIS DE TRANSFORMATION ? LE MÉTIER DE DIRECTEUR DE PROGRAMME DE SÉCURITÉ EST PEUT-ÊTRE FAIT POUR VOUS. POUR RÉUSSIR À CE POSTE, VOUS DEVREZ ÉGALEMENTPOSSÉDER UN DON PARTICULIER POUR SUPERVISER ET COORDONNER LES ÉQUIPES, AINSI QUE POUR COMMUNIQUER DE MANIÈRE LARGE SUR LES AVANCEMENTS EN MATIÈRE DE PROTECTION CYBER. VOUS VOUS RECONNAISSEZ DANS CETTE ÉBAUCHE DE PROFIL ? VOICI LES PRINCIPALES RESPONSABILITÉS ET OPPORTUNITÉS QUI VOUS ATTENDENT.

Missions

Le directeur de programme de sécurité doit se montrer pro-actif et opérationnel sur des tâches ayant trait à la fois à la direction de projet, à la gestion de ressources et à la communication.

Sur le plan de la direction de projet, il doit notamment être en mesure :

· De déterminer une politique de cybersécurité à même de réduire la menace, à la fois pour les systèmes informatiques et pour les différentes composantes métiers
· De cadrer et d'organiser un portefeuille pertinent de projets de cybersécurité
· D'assurer le déploiement du programme et des opérations de cybersécurité au sein de tous les départements et toutes les équipes intervenant de manière directe ou indirecte dans la cohérence globale de la politique de cyberdéfense
· D'assurer une coordination fluide et opérationnelle entre ces différentes parties prenantes
· Et de réorienter les actions chaque fois que cela s'avère nécessaire pour intégrer l'évolution de la nature et de l'intensité des cybermenaces.

Sur la question de la gestion des ressources, il devra :

· Mettre en œuvre la gouvernance et le mode de pilotage du programme nécessaires à sa réussite
· Assurer le suivi des plannings ;
· piloter les budgets des projets de sécurité
· Assurer une veille des risques et la gestion des actions correctives qui en découlent

Enfin, sur le terrain de la communication, le directeur de projet sécurité a pour mission :

· De prendre en main le reporting dans le but d'informer le commanditaire et le management de l'avancement et de la couverture des risques de sécurité assurée par le programme
· De mettre en forme des tableaux de bord, en recherchant la clarté à travers des exemples concrets, dans le but d'informer le top management de toutes les avancées et des défis à venir

Compétences

Ce poste implique des compétences techniques fortes, mais aussi des compétences en gestion de projet et management d'équipe.

Les compétences premières du Directeur de projet sécurité incluent notamment :

· Une bonne connaissance des enjeux organisationnels et des métiers qui s'y rattachent
· Une bonne maîtrise des connaissances de base concernant les principaux domaines des systèmes de sécurité informatique
· Une approche précise des enjeux actuels de cybersécurité
· Une connaissance suffisante des technologie liées à la sécurité cyber ;
· Une aptitude confirmée à la gestion de projets transversaux

Études

Un Bac+5 minimum est requis pour prétendre aux fonctions de directeur de programme sécurité. Pour accéder à un poste de ce niveau de responsabilité, 5 à 10 années d'exercice au plus près de la gestion de programmes informatiques sont exigées.

Salaire

Le salaire d'entrée moyen d'un directeur de projet sécurité est de 2 900 euros brut mensuels environ. Un professionnel confirmé pourra espérer toucher jusqu'à 4 900 euros brut par mois en moyenne. Ce salaire est celui proposé en règle générale aux spécialistes ayant déjà exercé 5 ans sur des projets de sécurité informatique. Pour une expérience de 3 ans, le salaire s'approche plutôt de 4 500 euros brut. Pour 10 ans d'expérience et plus, on peut espérer une rémunération légèrement supérieure, pouvant aller jusqu'à 5 100 euros brut mensuels environ.

Où travailler ?

N'importe quel grand groupe – qu'il se distingue dans le secteur de la banque, de la mode, de l'assurance, de l'agro-alimentaire, du textile ou des services numériques, par exemple – a besoin d'un ou plusieurs directeurs de programme de sécurité pour protéger son business. Les professionnels cherchant à évoluer sur cette ligne bénéficient donc d'un choix large et peuvent faire jouer sans problème leurs affinités avec un secteur en particulier.

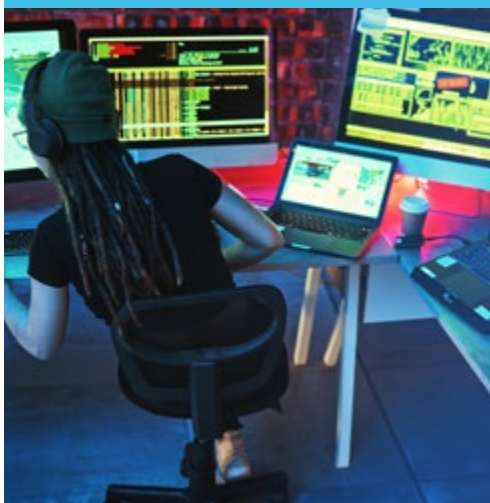
Parmi les structures les plus demandeuses en Directeurs de projet de sécurité au cours des dernières années, on peut notamment citer :

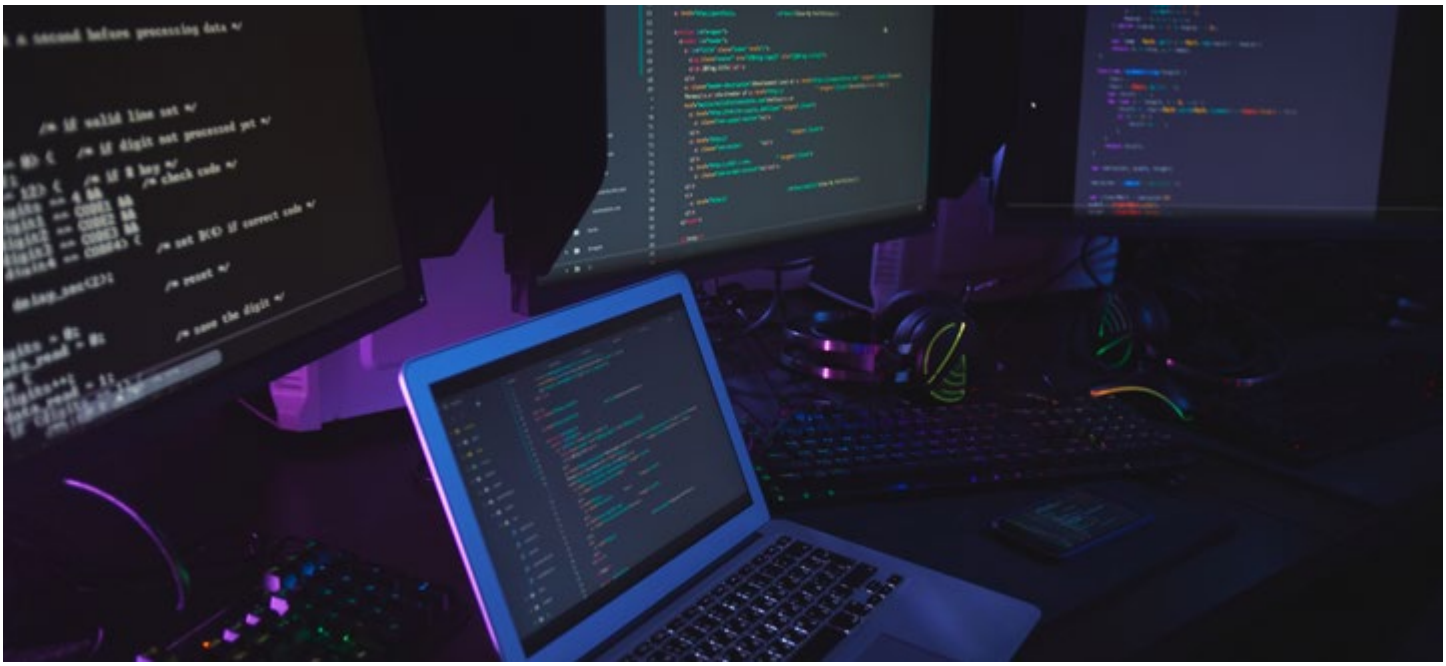
· De grandes références du luxe, à l'image du groupe LVMH ou de références associées, comme Louis Vuitton, Chanel ou Christian Dior
· Des enseignes de la grande distribution et des acteurs de l'industrie agro-alimentaire, comme les magasin E. Leclerc, le groupe Auchan ou Mondélez
· De très nombreux acteurs de la sphère numérique et du conseil, comme Cap Digital, Atos ou Alten
· Des grands noms de l'audiovisuel, comme le groupe TF1, Netflix ou le groupe Banijay

QUALITÉS

Le directeur de programme sécurité doit faire preuve :
· D'une grande aisance dans la gestion des équipes, et notamment des équipes nombreuses ;
· Et d'une capacité de communication solide, à l'oral comme à l'écrit, afin de restituer les enjeux et les avancées au management.

En raison de son interaction avec des enjeux humains et techniques, le directeur de projet sécurité doit être capable, tout à la fois, de rigueur et de souplesse :
· La rigueur est la condition d'un traitement optimal de tous les incidents cyber et de l'adoption des bonnes mesures correctives, ainsi que de la politique cyber appropriée ;
· De souplesse, afin d'embarquer toutes les équipes opérationnelles intervenant au sein de différents départements, avec des fonctionnements et des automatismes propres – et d'obtenir l'adhésion du management aux solutions préconisées.





« LA PRIORITÉ DU DIRECTEUR DE PROGRAMME DE SÉCURITÉ EST DE DÉFINIR ET METTRE EN PLACE UNE TRAJECTOIRE DE SÉCURITÉ À TRAVERS UN PORTEFEUILLE CONCRET DE PROJETS DE DÉFENSE. CES PROJETS DOIVENT ÊTRE DIRECTEMENT RELIÉS À UNE CIBLE, À DES OBJECTIFS DE SÉCURITÉ MÉTIERS, À DES OBJECTIFS IT STRATÉGIQUES AINSI QU'À L'AUGMENTATION DU RISQUE CYBER SOUS TOUTES CES FORMES. »

Évolution de carrière

Un directeur de programme de sécurité souhaitant franchir une nouvelle étape dans sa carrière peut évoluer naturellement vers un poste de Directrice de programme informatique. Pour réussir à ce poste, il s'agira d'élargir et d'affiner plus encore ses connaissances des défis de la cyberdéfense et sa capacité à l'analyse stratégique. Être accepté à ce poste suppose aussi de connaître parfaitement les enjeux propres à la structure dans laquelle le professionnel évolue.

Il est aussi envisageable de briguer un poster de responsable de la sécurité des services d'information (RSSI). Il s'agit d'un niveau de responsabilité supérieure. Il peut consister à déployer une politique concrète de cybersécurité sur un périmètre donné mais, la plupart du temps, la personne qui se voit confier ce poster a la charge d'assurer la cohérence de cette politique de défense à travers l'ensemble des corps de métier et dans tous les départements. Les aptitudes communicationnelles, déjà essentielles sur le poste de directeur de projet de sécurité, sont ici plus essentielles que jamais.

Avantages et inconvénients

Les entretiens conduits avec des directeurs de programme de sécurité justifiant de 3 à 7 ans d'expérience laissent émerger une conclusion unanime : le principal défi inhérent à la fonction tient à la nécessité d'assurer en tout temps, à chaque instant, une parfaite circulation des informations et une communication sans faille avec les instances dirigeantes d'une part, et les équipes exécutrices d'autre part. *« Plus encore que l'attention qui doit être portée aux détails techniques, c'est une vigilance ayant trait à l'humain – à la bonne implication de tous, sur la base des bonnes informations – qui prédomine »*, précise Martial R., 7 ans d'expérience et des passages par le secteur de l'aéronautique et de l'audiovisuel à son actif.

C'est cette même double casquette – entre performance technique et performance relationnelle – qui fait de toute évidence la fierté et la satisfaction première des professionnels interrogés !

ANALYSTE CYBERSÉCURITÉ

Niveau d'études : Bac+5

Spé Conseillée : Scientifique

Employabilité : Très bonne

Salaire débutant : 3 350 €

Code ROME : M1802 - Code FAP : M2Z

VOTRE SENS DE L'ANALYSE ET VOTRE COMPRÉHENSION DE LA SPHÈRE DIGITALE SONT LARGEMENT RECONNUS ? LES DÉFIS TECHNIQUES NE VOUS FONT PAS PEUR ET PARTICIPER À DES DÉCISIONS STRATÉGIQUES EST UN POINT QUI VOUS MOTIVE ? LE MÉTIER D'ANALYSTE EN CYBERSÉCURITÉ POURRAIT DONC RÉPONDRE À VOS COMPÉTENCES ET À VOS ASPIRATIONS. DANS UN CONTEXTE DE MONTÉE EN PUISSANCE EXPONENTIELLE DES CYBERATTAQUANTS, MENAÇANT LA PÉRENNITÉ DES ENTREPRISES, LA SÉCURITÉ DE STRUCTURES DE SERVICE PUBLIC ET L'INTÉGRITÉ DE LA VIE PRIVÉE DE MILLIERS DE CITOYENS, CE SPÉCIALISTE DES ARCANES DU MONDE CYBER EST DESTINÉ À JOUER UN RÔLE DE PLUS EN PLUS INCONTOURNABLE.

Missions

L'analyste cybersécurité assume un double rôle : il doit être force de proposition pour prévenir les risques cyber et le moteur de la réaction lorsqu'une faille de sécurité a été exploitée par un attaquant.

Dans le cadre de son activité de prévention, plusieurs tâches incombent à l'analyste en menace cyber :

· Opérer une veille sur les menaces émergentes en matière de cybersécurité
· Communiquer de manière pédagogique auprès de tous les décisionnaires et acteurs décisifs de la structure sur les enjeux de la cybermenace en général
· Dresser un panorama des menaces susceptibles d'affecter l'organisation et déterminer son niveau d'exposition au risque
· Collecter, vérifier et analyser les données brutes relatives aux attaques informatiques, en élargissant au maximum les sources d'information ;
· Entretenir un rapport d'échange et d'émulation avec d'autres experts n'appartenant pas à la structure
· Mettre à jour des bases de données et de connaissances sur l'ensemble des sujets concernés.

Face à une attaque bien concrète, l'analyste est tenu de :

· Rédiger des documents d'alerte et des rapports d'analyse destinés à faciliter la compréhension des menaces détectées
· Communiquer sur la possible évolution de la menace auprès de toutes les parties impliquées et émettre différentes hypothèses quant à cette évolution

· Déterminer, a posteriori, les nécessaires mises à jours des outils de détection existants et préconiser, si besoin, la mise en place de nouvelles défenses.

En résumé, l'analyste en cybersécurité apporte un support dans la compréhension des incidents rencontrés. Il analyse les modes opératoires et techniques d'attaque identifiés, dans le but d'améliorer les capacitéS de détection de la structure.

Sur plan particulièrement technique, c'est l'analyste cybersécurité qui a la charge de transmettre au CERT (Computer Emergency Response Team) ou au CSIRT (Computer Security Incident Response Team), ainsi qu'aux SOC, des données fiables et bien contextualisées. C'est de cette manière que pourront être ajustés les outils de défense.

Compétences

Le métier d'analyste en menace de cybersécurité se nourrit de compétences techniques très solides. Il requiert également une aptitude à cerner les enjeux globaux : ceux de la cyberdéfense en général, ainsi que les enjeux propres à la structure défendue. À ce titre, il sera essentiel de bien connaître les métiers existants au sein de la structure et leur lien avec les problématiques de sécurité informatique.

L'analyste sécurité doit aussi être en mesure :

· D'utiliser des sources ouvertes de manière sécurisée
· De construire des plans de veille opérationnels sur plusieurs questions et plusieurs secteurs en parallèle
· D'assurer une veille géopolitique et géostratégique, en plus de la veille purement technique, afin de mesurer l'évolution des risques cyber en provenance de l'extérieur

Études

La détention d'un Bac+5 est un prérequis minimum pour se positionner sur un emploi d'analyste en menaces cyber. Une spécialisation en cybersécurité ou, éventuellement, en intelligence économique est par ailleurs un atout de taille pour faire valoir sa candidature.

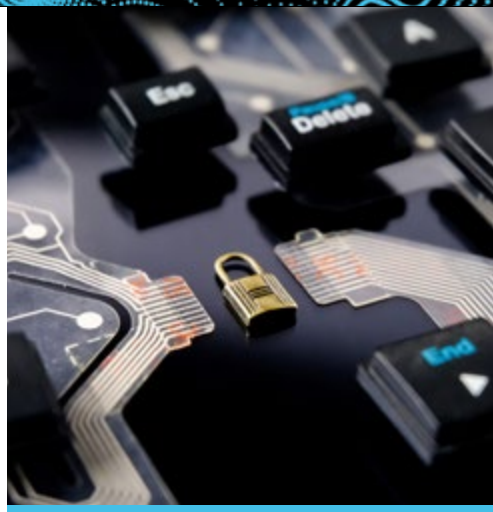
Salaire

En moyenne, un analyste en cybersécurité peut espérer débuter sa carrière avec un salaire de 3 350 euros mensuels brut. L'ajout de spécialisations techniques spécifiques – sur un langage ou un code particulièrement recherché, par exemple – sera un argument pour une majoration de salaire, pouvant avoisiner les 3 600 voire 3 800 euros mensuels brut. À un niveau senior, l'analyste peut gagner jusqu'à 8 450 euros brut par mois environ. Des échelonnements de salaire à partir de 6 200 euros brut sont à prévoir, en fonction de l'expérience et des spécialisations.

L'AVIS DU PROFESSIONNEL

« L'analyste en cybersécurité, c'est un peu le profiler ou le mentalist qui s'infiltre dans l'esprit d'une catégorie de fauteurs de troubles bien spécifiques : les hackers. »

Rémi L.
Analyste en cybersécurité



QUALITÉS

L'analyste en cybersécurité doit principalement faire preuve :
· D'une rigueur à toute épreuve, aussi bien dans l'analyse des éléments techniques que dans la transmissions des informations clés ;
· D'une grande capacité de synthèse, qui est à la condition incontournable d'une réponse rapide face à un incident ;
· D'une aisance de contact – notamment à l'écrit – et d'une facilité d'approche avérée pour construire des réseaux d'experts ou s'intégrer dans des réseaux d'experts déjà existants, dans le but de mener un échange d'informations fructueux et d'optimiser sa veille technologique.

Où travailler ?

Sans grande surprise, en raison de leur contribution stratégique, les professionnels préparés aux fonctions d'analyste en cybersécurité peuvent viser des horizons professionnels larges. Que ce soit auprès d'un GAFAM ou d'une licorne, d'un grand groupe du secteur bancaire ou d'une startup qui lance une application, les analystes en menaces de cybersécurité sont désirables partout où existe un enjeu de protection de données personnelles ou de sécurisation d'un système informatique vital pour la vie d'une entreprise ou d'une structure publique. En d'autres termes, ces professionnels peuvent se positionner dans une multitude de secteurs, au gré de leurs envies et des évolutions de la menace numérique.

Pour trouver un poste plus rapidement ou espérer pouvoir jouer sur les niveaux de salaire, on pourra en effet mener une étude préalable des domaines les plus fortement soumis au risque cyber, afin de faire valoir des atouts stratégiques.

De manière générale, toutes les entités disposant d'une structure de type SOC ont besoin d'analystes en cybersécurité !

À l'heure actuelle, on note un boom des assureurs en risque cyber, dont le nombre se multiplie, notamment en France. Il s'agit de structures particulièrement friandes en analystes cybersécurité, puisque ce sont ces derniers qui pourront proposer aux clients l'analyse de situation et l'arsenal de protection adapté pour faire face aux menaces extérieures. Parmi les autres recruteurs en puissance, on repère également :

· Des géants du divertissement et des réseaux sociaux, comme Facebook et Meta, le groupe auquel il appartient, Netflix ou Banijay, gros producteur et diffuseur de contenus audiovisuels
· Des incontournables des services grand public comme Enedis
· De nouveaux venus dans le domaine du e-commerce, un type d'entreprise qui n'arrête pas sa multiplication depuis une dizaine d'années
· Ainsi qu'une multitude d'acteur du secteur bancaire, comme BNP Paribas ou Axa, notamment

Évolution de carrière

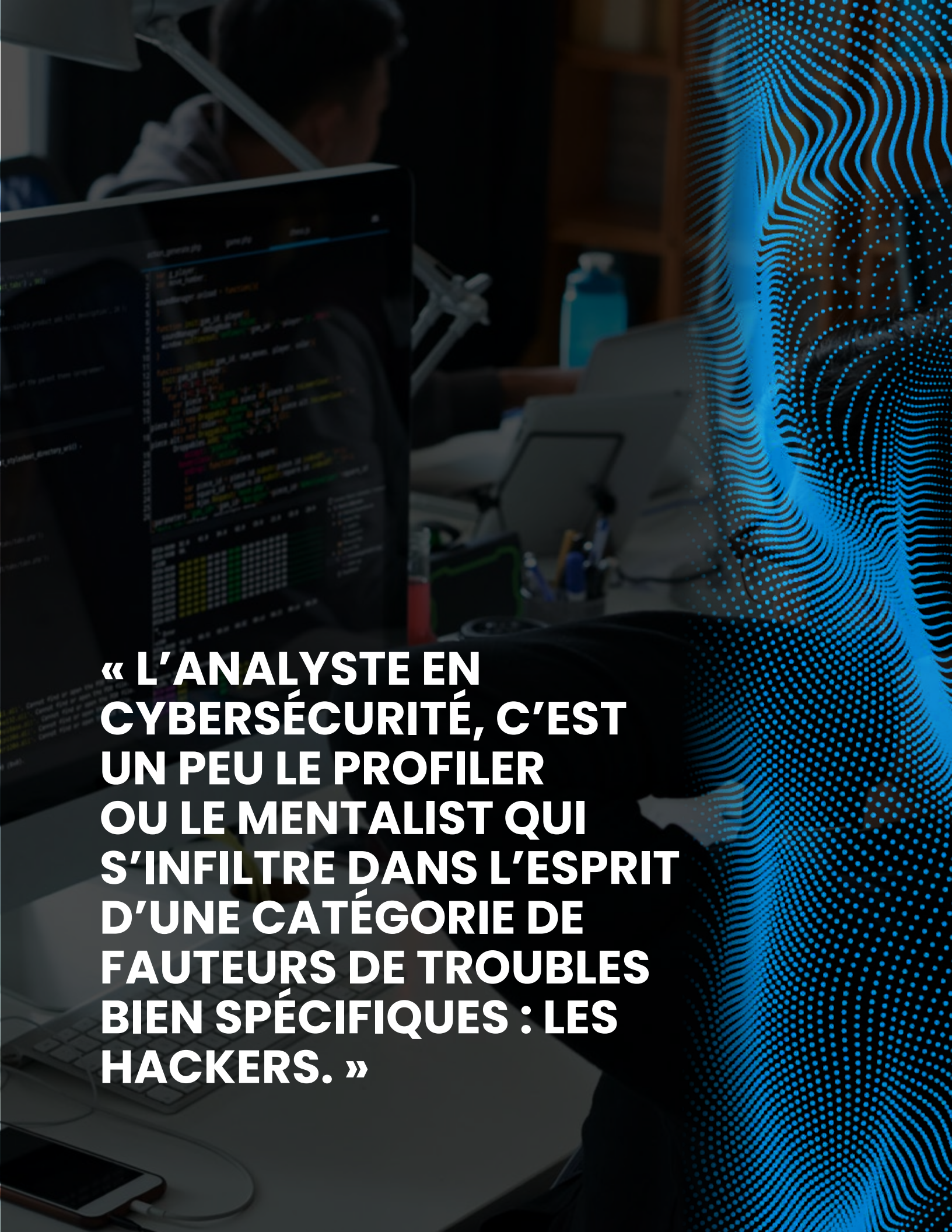
L'analyste cybersécurité est particulièrement bien placé pour se reconvertir en consultant en cybersécurité, dès lorsqu'il dispose de plus de 10 ans d'expérience et qu'il maîtrise parfaitement les enjeux stratégiques liés :

· À la cyberdéfense en général
· Et à la structure qu'il conseille en particulier

En tant que consultant, il retrouvera un rôle déjà abordé lorsqu'il endossait le costume d'analyste, mais dans une dimension plus puissante : il sera avant toute chose celui qui apporte un diagnostic, définit des méthodes, apporte des outils et des solutions, en intégrant les pratiques en vigueur sur le marché et en comprenant les spécificités propres à la structure défendue.

Avantages et inconvénients

« Ce qui représente un défi est aussi ce qui représente une motivation, dans le métier d'analyste en cybersécurité : être en permanence à jour sur les nouvelles menaces, savoir anticiper les nouveaux risques, c'est à la fois beaucoup de concentration et beaucoup d'épanouissement pour ceux qui n'aiment pas la répétition », explique Rami N., qui est passé par Facebook et Enedis avant de passer du côté des assureurs en cybersécurité, *« parmi les plus dynamiques sur ces questions »*, selon lui.



« L'ANALYSTE EN CYBERSÉCURITÉ, C'EST UN PEU LE PROFILER OU LE MENTALIST QUI S'INFILTRE DANS L'ESPRIT D'UNE CATÉGORIE DE FAUTEURS DE TROUBLES BIEN SPÉCIFIQUES : LES HACKERS. »

MANAGER DE RISQUES

Niveau d'études : Bac+3

Spé Conseillée : Scientifique

Employabilité : Bonne

Salaire débutant : 3 300 €

Code ROME : M1802 - Code FAP : M2Z

SAVOIR PRENDRE LA BONNE DÉCISION AU BON MOMENT, MENER DES ÉQUIPES NOMBREUSES DANS LA BONNE DIRECTION ET NE JAMAIS PERDRE DE VUE LES URGENCES STRATÉGIQUES : CETTE LIGNE DE CONDUITE VOUS EST FAMILIÈRE ? VOUS DISPOSEZ DONC PEUT-ÊTRE DES CODES INDISPENSABLES POUR RÉUSSIR AU POSTE DE MANAGER DE RISQUES SPÉCIALISÉ EN CYBERSÉCURITÉ. À L'HEURE OÙ LES ATTAQUES INFORMATIQUES N'ONT JAMAIS ÉTÉ AUSSI DANGEREUSES, SUR LE PLAN DE LA QUANTITÉ ET DE L'INVENTIVITÉ, LA PERSONNE EN CHARGE DE MANŒUVRER POUR ACTIVER LA DÉFENSE REVÊT UN RÔLE CENTRAL – ET QUI DEVRAIT, À L'AVENIR, S'INTENSIFIER ENCORE ET ENCORE.

Missions

Le manager de risques en cybersécurité est l'un des premiers remparts de la protection et l'un des premiers maillons de la réaction en cas d'attaque avérée contre les systèmes informatiques. Le diagnostic des risques potentiels et des risques avérés est un exercice que ce professionnel réalise à tous les instants, dans un but précis : faire en sorte que l'apparition d'un risque cyber soit toujours contenu sur le plus petit laps de temps possible, en visant la durée zéro. Le manager de risques est, à tout instant, le point de référence des spécialistes de la technique et des instances décisionnaires lorsqu'il s'agit de faire face à une crise de type cyber.

C'est à lui que revient la mission d'évaluer l'ampleur d'une crise, lorsqu'elle survient, et de mettre en place, le plus rapidement possible, toutes les actions devant permettre sa résolution.

Il endosse un rôle essentiel de gestion des équipes, notamment des équipes techniques : à lui de s'assurer que tous les agents sur le front appliquent ses recommandations et la politique de sécurité à la lettre et qu'ils mènent une action de réponse cohérente.

Gérer un risque cyber, c'est aussi se prêter à une mission de conseil auprès des directions métier afin de les inciter à prendre les bonnes mesures préventives, à s'adapter à la politique de cyberdéfense globale de la structure et à réagir sans attendre lorsqu'un incident est détecté.

En un mot, le manager de risques est l'un des piliers de la résolution des crises de cybersécurité et son aide est essentielle pour aider une entreprise – ou toute autre structure – à se prémunir contre des menaces cyber de plus en plus présentes et impactantes.

Compétences

Le manager de risques cyber assume un double rôle : il doit être force de proposition pour prévenir les risques cyber et le moteur de la réaction lorsqu'une faille de sécurité a été exploitée par un attaquant.

Dans le cadre de son activité de prévention, il est attendu de ce manager bien particulier :

· Qu'il conseille le management et tous les décisionnaires impliqués sur les sujets cyber en matière de politique de défense
· Qu'il définisse concrètement les outils de gestion des crises potentielles, en pointant les procédures et les ressources nécessaires, entre autres
· Qu'il s'assure que tous les jalons de préparation des crises ont bien été posés et que les outils de réaction sont bien disponibles
· Prendre en charge la formation des techniciens de support et autres intervenants techniques impliqués dans la gestion des crises de sécurité

C'est aussi et surtout au manager de risques qu'il revient de tester et confirmer la capacité de la structure à réagir efficacement à une attaque.

Face à la détection d'une tentative d'attaque ou d'une attaque réussie, il se devra :

· De mettre en place un mécanisme de gestion de crise efficace
· D'animer la cellule de gestion de crise en impliquant de manière proportionnée les différentes parties impliquées et en organisant les équipes d'intervention ;
· D'assurer la bonne circulation des informations entre toutes parties prenantes, dans un but d'efficacité et de réactivité
· De vérifier la consistance et la cohérence du message transmis aux différents acteurs impliqués
· D'assurer le suivi de toutes les actions correctives prises suite à l'incident ;
· De faire le lien avec les autorités et instances de dépôt de plainte, ainsi qu'avec les divers experts et assureurs pouvant être sollicités
· De planifier des réunions de revue post-crise afin d'enregistrer et de tirer partie des difficultés et particularités relevées pendant l'intervention, ce qui permettra à terme d'améliorer les mécanismes de prévention, de détection et de traitement des attaques de type cyber

L'AVIS DE LA PROFESSIONNELLE

« Le gestionnaire de risques cyber, c'est un peu le chef d'orchestre qui s'assure qu'il n'y ait pas de fausses notes dans la partition de défense. Et c'est lui qui gère les accords à la baguette dès lors qu'un hacker a réussi à exploiter une faille ! »

Samira N.
Manager de risques cyber

QUALITÉS

Le gestionnaire en risques liés à la cybersécurité doit principalement faire preuve :
· D'une capacité à la gestion d'équipes dans un climat de haute tension
· D'une compréhension précise des systèmes d'information et des enjeux de la cybersécurité
· D'un esprit de rigueur permettant la gestion pertinente d'une documentation multiple et importante
· D'un esprit de synthèse à toute épreuve, garantie d'une communication efficace et d'une transmission rapide des informations
· Et d'une organisation sans faille, dans tous les domaines, celui de la gestion de l'information comme celui de la gestion humaine

Études

Le diplôme minimum requis pour se positionner sur un poste de manager des risques cyber est un Bac +5. On appréciera fortement une spécialisation sur les questions cyber. Les professionnels combinant de bonnes bases techniques (de niveau Bachelor) avec un Master davantage axé sur le management tirent souvent leur épingle du jeu.

On demande en règle générale 5 ans d'exercice sur des postes relatifs à la question cyber avant d'accepter de confier des responsabilités de manager du risque.

Salaire

Un manager de risques qui fait ses premiers pas peut valoriser ses compétences à 3 300 euros brut mensuels minimum. Toute spécialisation de niveau avancé en cybersécurité peut donner lieu à une majoration – on visera, dans ce cas, un salaire d'entrée de 3 450 euros brut par mois environ.

Un manager de risques qui dispose de connaissances solides propres au secteur qu'il rejoint peut lui aussi viser un salaire supérieur à la moyenne. Prenons un exemple concret : vous candidatez à un poste de gestionnaire du risque cyber auprès du groupe BPCE et, en plus de plusieurs années d'expérience sur des métiers cyber, vous maîtrisez parfaitement les mécanismes de base de la machine bancaire. Vous êtes un manager de risque d'autant plus légitime sur le poste en question et, à ce titre, vous pouvez espérer débuter avec 3 550 euros brut mensuels environ.

Un manager des risques fort de plus de 10 ans d'expérience peut gagner jusqu'à 6 750 euros brut mensuels environ. À noter que parmi les managers de risques cyber les mieux rémunérés, on trouve souvent d'anciens spécialistes des questions techniques, armés d'un MBA en management : ils disposent de toutes les cartes pour sécuriser au maximum les environnements et faire valoir, par conséquent, un haut salaire.

Où travailler ?

Sans grande surprise, tous les secteurs sous haute tension cyber, c'est-à-dire fortement soumis au risque d'attaque informatique, sont demandeurs de managers de risques performants. Sont concernés tous les domaines en contact avec un volume important de données personnelles, comme les sites de e-commerce, les banques et assurances, les opérateurs de téléphonie mobile et de services internet, tout comme les plateformes de streaming et autres diffuseurs de divertissement.

On peut ajouter à cette liste les acteurs de la sphère numérique au sens large, et notamment les créateurs d'applications en tous genres.

Divers ministères et structures publiques au rôle stratégique prennent également soin de s'attacher les services d'un expert en management du risque cyber, là où l'on se contentait il y a encore quelques années de recruter de « simples » experts en gestion de crise.

Parmi les recruteurs à surveiller de près, on peut inclure sans hésitation :

· Des géants de l'industrie du transport et de la construction de véhicules, comme Airbus, le groupe Bosch ou Naval Group
· Des leaders de la transformation digitale, comme Atos
· France Cyber Maritime, association créée à l'incitation des pouvoirs publics pour contribuer au renforcement de la cybersécurité d'un secteur vital pour le fonctionnement et l'économie du pays
· Des assureurs cyber et des cabinets spécialisés dans les questions de cybersécurité, à l'image de FIDENS ou d'ALLISTIC
· Natixis, la Société Générale et le groupe BPCE, parmi d'autres références du secteur bancaire
· Ou encore Framatome, un des leaders de l'énergie nucléaire

Évolution de carrière

Après plus de 5 ans au cœur de la gestion de risque cyber, si vous brillez réellement par vos compétences, vous pouvez envisager de prendre les rênes du CSIRT – un organe avec lequel vous aurez travaillé main dans la main au jour le jour, dans un climat de tension, pendant des années.

Pour réussir à ce poste, des connaissances techniques plus complètes et plus solides que celles exigées en tant que manager des risques sont cependant indispensables.

Avantages et inconvénients

Pour Samira N., le métier de gestionnaire de risque cyber est « *par essence vivant : le contexte de tension ou de possibilité de forte tension a quelque chose de stimulant. Mais c'est là aussi le vrai défi : savoir résister à la pression, tous les jours – ou presque* ».

« LES GRANDS GROUPES ONT PRIS L'HABITUDE DE RECRUTER UN MANAGER DES RISQUES POUR LE PLACER DIRECTEMENT AUPRÈS DE LEUR CERT OU DE LEUR CSIRT. PLUS LA TAILLE D'UNE ENTREPRISE EST IMPORTANTE – OU PLUS LE VOLUME DE DONNÉES TRAITÉES EST CONSÉQUENT, PLUS IL EST PROBABLE DE RENCONTRER CE MÉTIER PARFAITEMENT INTÉGRÉ DANS L'ENTREPRISE. »

INCIDENT RESPONSE TEAM MEMBER

Niveau d'études : Bac+5

Spé Conseillée : Scientifique

Employabilité : Bonne

Salaire débutant : 3 300 €

Code ROME : M1802 - Code FAP : M2Z

SI VOUS AIMEZ AVOIR UN IMPACT CONCRET – ET MESURABLE AU JOUR LE JOUR – ET QUE L'UNIVERS INFORMATIQUE ET SES PIÈGES VOUS PASSIONNENT, LE MÉTIER D'INCIDENT RESPONSE TEAM MEMBER POURRAIT BIEN ÊTRE FAIT POUR VOUS. TRAQUEUR DE MENACES ET ANALYSTE CHEVRONNÉ DES OCCURRENCES DE HACKING, CE TECHNICIEN QUI N'A PAS PEUR DES DÉTAILS JOUE UN RÔLE TRÈS CONCRET ET ABSOLUMENT CENTRAL DANS LE MÉCANISME DE PROTECTION ET DE DÉFENSE DE NOS STRUCTURES. PASSONS EN REVUE LES FORCES QU'IL DOIT APPORTER ET LES PERSPECTIVES QUI S'OFFRENT À LUI.

Missions

L'incident response team member a un triple rôle :

· D'anticipation et prévention ;
· D'analyse détaillée ;
· Et de conseil.

En effet, ce professionnel clé de la bulle cyber est tenu à la fois de capter les tendances des risques cyber à l'échelle globale et à l'échelle de la structure elle-même, de décrypter les symptômes d'une attaque lorsque celle-ci survient et, enfin, de réorienter la politique de cyberdéfense de l'entreprise et d'améliorer les outils de protection existants.

Concernant le volet de prévention, l'Incident Responder a pour mission de :

· Conduire une veille complète et proactive sur l'apparition de nouvelles vulnérabilités système, de nouveaux types d'attaques et de nouvelles technologies prisées des hackers
· Mettre à jour les bases de données sur le suivi des attaques potentielles ;
· Mettre à jour les outils d'investigation du risque cyber et en proposer, si possible et pertinent, de nouveaux
· Mettre en place des indicateurs de compromission

Concernant l'analyse-même des attaques cyber, il devra :

· Analyser les relevés techniques émanant du CERT ou du CSIRT dans le but de déterminer le mode opératoire de l'attaquant, son objectif, ainsi que l'étendue de la compromission
· Remettre des rapports d'investigation, nourris d'éléments techniques et de parties explicatives, sur la base des données collectées.

« EN TANT QUE SPÉCIALISTE EN CHARGE DE RÉPONDRE AUX INCIDENTS DE SÉCURITÉ, L'INCIDENT RESPONSE TEAM MEMBER A POUR VOCATION DE CONDUIRE TOUTE UNE SÉRIE D'ANALYSES TECHNIQUES SUR LES SYSTÈMES D'INFORMATION. CE TRAVAIL DOIT PERMETTRE DE REPÉRER DE POSSIBLES FAILLES, À CORRIGER AVANT UNE TENTATIVE D'ATTAQUE. »

À travers ces travaux d'analyse, l'incident response team member renforce ses compétences en conseil et se trouve parfaitement préparé pour :

· Préconiser des mesures de contournement et de correction de l'incident
· Préconiser des mesures d'amélioration des capacités d'analyse, notamment grâce à l'extraction des indicateurs de compromission
· Préconiser des axes d'amélioration des outils de protection cyber

Compétences

Pour être opérationnel, un analyste de réponse aux incidents doit être armé de plusieurs compétences élémentaires. Il doit notamment :

· Maîtriser parfaitement les mécanismes relatifs aux systèmes d'information en général et ceux des SI de sa structure en particulier
· Connaître tous les détails de l'architecture du système d'information de sa structure
· Bien connaître les outils d'analyse des vulnérabilités et des virus informatiques ;
· Savoir analyser les flux de réseaux
· Avoir une vision claire et sans cesse à jour du panorama des techniques d'attaque
· Maîtriser les techniques du scripting.

Études

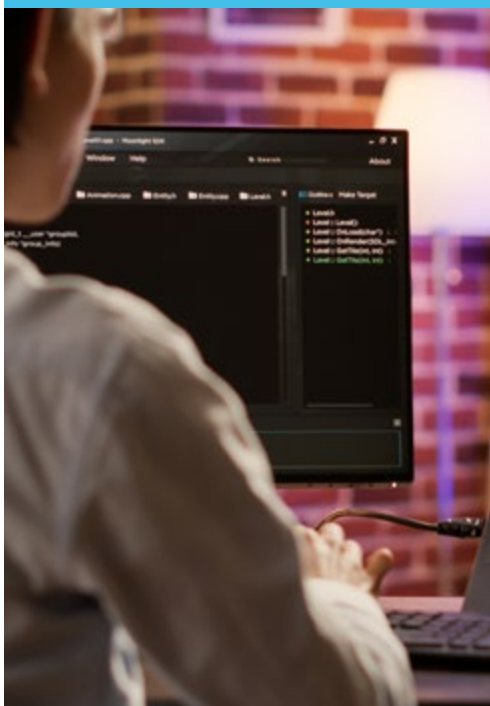
Il est nécessaire d'avoir atteint un niveau Bac+5 pour intégrer l'équipe d'un CERT ou d'un CSIRT sur ce type de poste. Comme souvent, une spécialisation en cybersécurité sera fortement appréciable, en plus des compétences indispensables sur le plan de l'informatique et de la technique pure.

Salaire

Si l'on observe la moyenne des salaires au moment de la première prise de poste, un incident response team member peut espérer gagner environ 3 300 euros brut par mois. Cette rémunération peut être revue à la hausse dès lors que le professionnel justifie d'une formation en cybersécurité particulièrement poussée. La même règle s'applique lorsqu'apparaît la maîtrise d'un code ou d'un langage rare ou, par exemple, une spécialisation précise en tant qu'analyste réseau, analyste système ou analyste de codes malveillants. Pour un niveau senior, on relève un salaire mensuel moyen de 6 250 euros brut.

QUALITÉS

Un bon analyste réponse aux incidents de sécurité – c'est-à-dire un analyste efficace et épanoui dans ses fonctions – doit faire preuve d'un goût pour le travail en équipe très prononcé. Il doit se montrer apte à transmettre, dans toutes ses communications écrites, des informations d'une précision et d'une clarté sans faille. Cette compétence en communication écrite s'avère notamment essentielle pour la rédaction de rapports adaptés à différents types d'interlocuteurs – techniciens comme décisionnaires.
L'aptitude à la vulgarisation ne doit pas être sous-estimée : elle est cruciale pour embarquer l'ensemble de la structure dans la construction d'un système de défense opérationnel.
Comme sur de nombreux postes ayant trait aux enjeux sensibles de la sphère cyber, l'incident response team member doit faire preuve d'un sens éthique inaltérable. Il doit par ailleurs pouvoir maintenir un niveau de qualité et de pertinence constant, même pendant les périodes de crise et de tension, dès lors qu'une intrusion imminente ou avérée met en péril les systèmes.



Où travailler ?

L'incident response team member va jouer un rôle déterminant auprès de tous les grands acteurs du secteur industriel, tout comme auprès des acteurs du secteur des assurances ou de la banque. L'ensemble des plateformes faisant usage, au quotidien, de données personnelles d'utilisateurs sont elles aussi d'importants recruteurs potentiels : des sites de divertissement tous azimuts – jeu vidéo, streaming vidéo ou musical – aux services de e-commerce, tout le monde est concerné. Les assureurs en cybersécurité, de plus en plus nombreux, sont une autre piste à surveiller de très près.

Dans l'ensemble des secteurs mentionnés précédemment, on peut signaler plusieurs structures cherchant à renforcer régulièrement leurs équipes d'analystes réponse aux incidents. Parmi celles-ci, on trouve notamment :

· Axa et la CACIB dans le secteur bancaire
· Spotify, Netflix et Disney+ du côté du divertissement et du streaming
· Bouygues Telecom
· Orange Cyberdefense
· le groupe Thales, le groupe Dassault et le groupe PSA
· de nombreux acteurs du jeu vidéo, comme Ubisoft ou Nintendo

Évolution de carrière

S'il n'a pas abordé son premier poste en ayant déjà une spécialisation, l'incident response team member peut gravir une sorte d'échelon supérieur en corrigeant cela : il peut faire valoir une compétence supérieure – et renégocier son salaire en conséquence – en se spécialisant, dans ses fonctions ou à travers une formation, en tant que spécialiste réseau, spécialiste système ou expert en codes malveillants (comme déjà évoqué précédemment).

À un niveau similaire, l'analyste incidents peut choisir une fonction d'analyste en menace de cybersécurité, qui le conduira à avoir une vision plus globale des problèmes de cyberdéfense, plutôt que d'être concentré sur des incidents et des menaces définis de manière plus précise.

En développant de manière substantielle ses capacités stratégiques et managériales, ce professionnel peut aussi espérer évoluer sur un poste de gestionnaire de crise de cybersécurité. Parfaitement familier de tous les détails techniques, il pourra pleinement se concentrer – en cas de crise – sur la définition de plans de réaction à même d'embarquer toute la structure en un temps record.

Les analystes réponse aux incidents de sécurité justifiant d'une longue carrière peuvent, à terme, espérer occuper les fonctions de responsable du CERT ou du CSIRT, un groupe dont ils auront été des éléments centraux pendant des années.

Avantages et inconvénients

« Être la personne en charge d'organiser la réponse aux attaques et aux incidents, cela veut dire être toujours en embuscade. Donc maintenir, en permanence, un certain niveau de tension. La responsabilité est grande, même si d'autres gèrent l'orchestration de cette réponse. », explique Adrien M. Parmi les avantages listés fréquemment, on note un renouvellement fréquent des connaissances et des défis intellectuels. Cela implique immanquablement une notion d'effort intellectuel qui, à l'occasion, peut être rangé du côté des difficultés du poste. Nombreux sont les professionnels qui mettent en avant une absence de monotonie au quotidien, mais un besoin d'évoluer et de passer à d'autres mécaniques de travail après 7 à 10 années d'exercice.

« L'INCIDENT RESPONSE TEAM MEMBER, C'EST LE SOLDAT QUI FAIT EN SORTE QU'UNE ATTAQUE CYBER NE SOIT PAS UNE FATALITÉ. »

Niveau d'études : Bac+5

Spé Conseillée : Scientifique

Employabilité : Très bonne

Salaire débutant : 3 100 €

Code ROME : M1802 - Code FAP : M2Z

VOUS AVEZ L'ÂME D'UN CRYPTOLOGUE DES MYSTÈRES TECHNIQUES ? VOUS FAITES PREUVE D'UNE MOTIVATION INFATIGABLE LORSQU'IL S'AGIT DE REMONTER AUX ORIGINES D'UN PROBLÈME ? VOUS DISPOSEZ DE TOUTE ÉVIDENCE DES QUALITÉS ESSENTIELLES POUR DEVENIR ANALYSTE FORENSIC. AU CŒUR DE CE MÉTIER D'INGÉNIEUR ET D'EXPERT TECHNIQUE SE TROUVENT DEUX MOTS D'ORDRE : PRÉCISION ET EXHAUSTIVITÉ. VOICI LES CONDITIONS À RÉUNIR POUR ABORDER AVEC SUCCÈS LES MISSIONS QUI S'Y RATTACHENT.

Missions

L'analyste forensic prend une part active à toutes les missions d'investigation et de réponse à incidents, généralement gérés par un CERT (Computer Emergency Response Team) ou un CSIRT (Computer Security Incident Response Team). Dans ce cadre, l'ingénieur spécialisé en questions forensiques s'intéresse à tous les sujets de menace de la sécurité cyber, de threat intelligence – pour évaluer les risques de cybermenace – ou de reverse engineering – dans le but de comprendre le fonctionnement interne d'un système, parmi d'autres thématiques connexes.

De manière générale, l'analyste forensic sera conduit à :

· Déterminer les causes racines des incidents identifiés
· Évaluer l'impact de l'incident en cause sur le plan technique et pour les différents métiers, dans le champ cyber et au-delà
· Livrer une analyse aussi détaillée que possible sur les actions menées par l'attaquant sur le périmètre compromis ;
· Mettre au point et mettre à jour des outils d'aide à l'analyse du risque, en s'alignant sur les dernières avancées technologiques
· Décrypter des malwares et analyser les protocoles réseau en procédant par reverse engineering
· Rechercher les vulnérabilités potentielles de solutions software et hardware
· Prendre part à des projets de développement d'outils de cybersécurité internes
· Établir une chronologie forensic

permettant de suivre l'évolution des menaces et des contre-attaques
· Assurer une veille et une investigation numérique sur tous les systèmes d'exploitation existants.

Compétences

Sur le plan des compétences purement techniques, plus le nombre d'environnements informatiques qu'il maîtrise est important, plus un analyste forensic prend de la valeur aux yeux des entreprises et des employeurs potentiels. Son aisance au sein de différents systèmes cryptés est un atout de taille pour assurer une réactivité complète, face à tous les dangers cyber.

· Un bon analyste forensic devra notamment être opérationnel sur les points suivants :
· Maîtrise du système d'information, de l'urbanisation et de l'architecture du SI (système d'information)
· Connaissance des outils d'analyse post-mortem, pour assurer la compréhension de chaque incident
· Capacité à la gestion des crises de sécurité
· Capacité de veille opérationnelle et de synthèse pour capter les tendances et facteurs d'évolution du métier
· Parfaite connaissance des techniques d'attaque et d'intrusion informatique ;
· Parfaite connaissance de la vulnérabilité propre à chaque environnement
· Pratique avérée de l'analyse des flux de réseau
· Capacité à automatiser les tâches récurrentes dans un langage de scripting.

La connaissance des procédures légales est également très fortement appréciée : la caractérisation de l'incident doit, dans l'idéal, être accompagnée d'un conseil précis sur les actions de recours juridiques possibles contre l'attaquant.

L'analyste forensic – souvent désigné sous le nom d'analyste réponse aux incidents de sécurité – a par ailleurs la possibilité de se spécialiser en tant qu'analyste système, analyste réseau ou analyste de codes malveillants, chacune de ces fonctions allant de paire avec un certain nombre de compétences plus spécifiques.

Études

Les postes d'analyste forensic sont ouverts à des ingénieurs et spécialistes techniques détenteurs d'un Bac +5 au minimum. Une spécialisation en cybersécurité peut être un plus au moment du recrutement.

Salaire

En France, le salaire moyen d'un analyste forensic varie en moyenne entre 3 100 euros brut mensuels pour un débutant et 4 800 euros pour un profil confirmé. Le niveau de salaire peut augmenter, notamment pour les profils confirmés, lorsque l'ingénieur justifie d'une spécialisation :

· Sur une question précise, en tant qu'analyste système, analyste réseau ou analyste de codes malveillants
· Sur les questions juridiques
· Sur la gestion des crises de cybersécurité en général.

Dans ce cas de figure, on relève des salaires pouvant atteindre 5 100 euros brut par mois.

« L'INGÉNIEUR SPÉCIALISÉ EN FORENSIQUE EST CHARGÉ DE COLLECTER ET D'ANALYSER UN ENSEMBLE DE DONNÉES BRUTES – FICHIERS EFFACÉS, SAUVEGARDES, JOURNAUX DU SYSTÈME OU DISQUES DURS, ENTRE AUTRES – AFIN DE COMPRENDRE CE QU'IL S'EST PASSÉ ET D'EN TIRER DES CONCLUSIONS UTILES EN MATIÈRE DE CYBERSÉCURITÉ. »

QUALITÉS

L'analyste forensic doit présenter un goût prononcé pour le partage des connaissances et la mise en commun des idées. Il doit notamment faire preuve d'une capacité solide à la restitution et à la vulgarisation des connaissances pour des publics non spécialistes des questions techniques. C'est là la condition indispensable pour permettre :
· La compréhension exacte de la menace cyber pouvant affecter l'entreprise, qu'elle soit potentielle ou avérée
· Le développement des bons outils de protection cyber, répondant aux attentes de tous les départements
· La conduite d'actions juridiques appropriées suite à un incident.
Dans cette lignée, il doit également présenter des qualités rédactionnelles solides pour préparer des rapports adaptés à différents niveaux d'interlocuteurs. Il doit également disposer de qualités comportementales et communicationnelles développées, afin d'être efficace et exhaustif dans sa collecte des données suite à un incident.
L'analyste forensic doit être tout aussi à l'aise pour le travail en autonomie que pour le travail en équipe. Sa capacité à résister aux situations de crise et à la pression doit être évidente, de même que son sens éthique.

Où travailler ?

Toutes les structures de taille importante, qu'elles dépendent du secteur public ou privé, sont susceptibles de s'attacher les services d'un ou plusieurs analystes forensic. La fonction revêt notamment une importance de premier plan dans les structures conduites à gérer un volume non négligeable de données personnelles : sociétés de l'internet et de la téléphonie en général, plateformes de streaming, groupes liés aux activités de banque et d'assurance, services hospitaliers, entre autres.

Parmi les entreprises régulièrement à la recherche d'analystes forensic, on relève notamment :

· Les services croisés banque et assurance, comme AXA ou le groupe La Poste
· Les grands groupes liés aux secteurs de l'aviation, de l'aéronautique ou de la technologie mécanique, comme Airbus ou Thales
· Les opérateurs de téléphonie mobile et fournisseurs d'accès à internet comme Orange, Bouygues ou SFR, et plus particulièrement Orange Cyberdefense, référence en matière de services de cybersécurité
· Tous les grands acteurs de la transformation digitale et des services numériques à grande échelle, ainsi que des spécialistes du conseil, tels Atos, Capgemini, Sopra Astoria ou Accenture.

Évolution de carrière

En tant qu'élément central de l'équipe du CERT (Computer Emergency Response Team) ou du CSIRT (Computer Security Incident Response Team), l'analyste spécialisé dans la réponse aux incidents de sécurité peut tout à fait envisager de gravir les échelons pour prendre la tête d'une de ces équipes en tant que Responsable.

Nombreux sont les analystes forensic qui, désireux de changement, passent sur un poste d'opérateur analyste SOC, bien que l'évolution soit plus pertinente et plus fréquente dans le sens opposé.

En raison de leurs responsabilités et compétences transversales, ils peuvent également envisager de compléter leur formation pour endosser un rôle de conseil, pour devenir notamment :

· Conseiller juridique en sécurité
· Consultant en sécurité organisationnelle
· Consultant en sécurité technique.

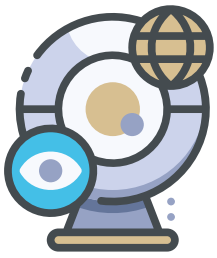
Avantages et inconvénients

Pour Omar H., l'une des motivations premières liées au poste d'analyste forensic tient au renouvellement permanent des problèmes rencontrés : si chaque incident nouveau représente en soi un défi et un challenge intellectuel, il mobilise aussi des mécanismes positifs de curiosité et de mise à jour permanente des connaissances. Cela rime avec une absence de monotonie évidente, en dépit des tâches récurrentes de veille technologique.

La fonction est par ailleurs particulièrement valorisante, puisque l'analyste occupe une place stratégique dans le rouage de défense et de pérennisation de l'entreprise. La combinaison de capacités hautement techniques et d'aptitudes relationnelles et communicationnelles contribue également à un métier complet et équilibré, susceptible d'apporter de nombreuses clés d'épanouissement professionnel. L'entretien de ces compétences complémentaires ouvre par ailleurs des perspectives lorsque se présente une évolution vers un autre poste ou un autre secteur.

Parmi les principaux inconvénients, Omar H. relève principalement le besoin de résister au stress : la possibilité de voir surgir un incident de manière imminente conduit à maintenir un niveau de vigilance qui peut être particulièrement énergivore, sur le plan nerveux en particulier. Lorsque survient une crise de manière concrète, l'ingénieur spécialiste en forensique doit faire preuve d'un sang froid sans faille. Il est le pilier central de la compréhension du problème, donc de sa résolution et du maintien du niveau de défense. En d'autres termes, c'est la survie de l'entreprise et, par conséquent, des dizaines et des dizaines d'emplois qui se trouvent – en grande partie – entre ses mains.

« L'ANALYSTE FORENSIC – PARFOIS SIMPLEMENT APPELÉ 'FORENSIC' – EST L'EXPERT TECHNIQUE EN CHARGE D'EXAMINER TOUT OU PARTIE D'UN SYSTÈME D'INFORMATION APRÈS LA DÉTECTION D'UNE CYBERATTAQUE, PEU IMPORTE SI ELLE EST RESTÉE AU STADE DE TENTATIVE OU SI ELLE A ÉTÉ CONCLUANTE. »



34

RESPONSABLE DES ASSURANCES

Niveau d'études : Bac+5

Spé Conseillée : Scientifique

Employabilité : Bonne

Salaire débutant : 2 800 €

Code ROME : M1802 - Code FAP : M2Z

À L'HEURE OÙ LES ATTAQUES DE TYPE CYBER SE PERFECTIONNENT ET SE MULTIPLIENT DE MANIÈRE EXPONENTIELLE, IL EST DEVENU IMPÉRATIF POUR LES ENTREPRISES DE PENSER DES STRATÉGIES DE DÉFENSE SOLIDES ET, POUR CE FAIRE, DE FAIRE APPEL À DES EXPERTS CONFIRMÉS. EN RÉPONSE À CES ENJEUX, ET EN PARALLÈLE D'ENTREPRISES DE PLUS EN PLUS MENACÉES, LA GALAXIE DES ASSUREURS CYBER A CONNU UNE GRANDE EXPANSION AU COURS DES DERNIÈRES ANNÉES. DANS CE CONTEXTE, FAIRE LE CHOIX DU BON CONTRAT D'ASSURANCE, COUVRANT TOUS LES BESOINS SPÉCIFIQUES À UNE STRUCTURE DONNÉE, EST UNE MISSION À PART ENTIÈRE. IL CONVIENT DE LA CONFIER À UN STRATÉGISTE HORS PAIR, EN PRISE AVEC LA RÉALITÉ CONCRÈTE DU PRÉSENT ET À MÊME DE SENTIR LES TENDANCES À VENIR : LA FONCTION DE RESPONSABLE DES ASSURANCES CYBER EST, DE CE FAIT, DEVENUE ESSENTIELLE POUR LES ENTREPRISES DÉSIREUSES D'ÊTRE EN PHASE AVEC LE MONDE MODERNE – ET DE LUI RÉSISTER. VOYONS ENSEMBLE COMMENT S'ARTICULE CE MÉTIER DESTINÉ À GAGNER DE PLUS EN PLUS EN IMPORTANCE ET EN RECONNAISSANCE.

Missions

De manière plus générale, le responsable des assurances est celui qui assure la cohérence des politiques de protection contre le risque cyber. *« Il est la boussole qui pointe le meilleur contrat d'assurance possible pour l'entreprise, en fonction de sa base technique et du taux de risque auquel elle fait potentiellement face »,* précise Cécile P., responsable des assurances.

Il est de plus en plus commun de voir les entreprises choisir un responsable des assurances externe à la structure : elles se dirigent vers des professionnels indépendants en contact avec différents univers professionnels, et de ce fait à même de proposer plus rapidement une solution d'assurance adaptée.

L'intégration de la fonction au sein même de l'entreprise, tantôt auprès du service juridique, tantôt auprès des services techniques, reste cependant la norme.

De l'importance de l'assurance cyber

Pourquoi s'attacher les services d'un professionnel spécifiquement dédié à la question des assurances en cyber-risques est aussi essentiel ? Selon les dernières enquêtes du CESIN (le Club des experts de la sécurité de l'information et du numérique), l'impact des cyberattaques sur la santé des entreprises a tendance à s'aggraver depuis plusieurs années. En 2020, 61 % des entreprises se sont déclarées affectées de manière importante suite à une attaque informatique, soit une augmentation de 3% par rapport à l'année précédente.

Dans la majorité des cas (21%), les

structures voient leur production perturbée. Le deuxième problème le plus important (14% des cas) est lié à une compromission des informations, des processus et des savoir-faire. Dans la même proportion de 14%, les entreprises signalent que c'est l'indisponibilité de leur site web, suite au piratage, qui impacte de façon négative la relation avec les clients. En troisième place du podium (11%), on trouve les retards de livraison, suite à la perturbation des systèmes.

Parmi les autres conséquences préjudiciables des cyberattaques, il faut encore noter la perte d'image ou un impact médiatique négatif, la réalisation de transactions frauduleuses ou encore un arrêt de la production sur un laps de temps significatif.

Dans la plupart de ces cas, la, cyberattaque se traduit par une perte de chiffre d'affaires, pouvant à l'occasion mettre en danger la pérennité de l'entreprise.

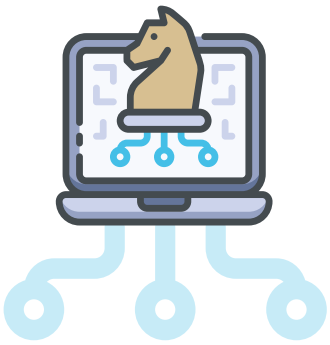
À titre informatif, en 2020 toujours, les pertes financières générées par les cyberattaques ont dépassé la barre de 1 000 milliards de dollars, ce qui correspond à une augmentation de 50 % par rapport à 2018. C'est par ailleurs l'équivalent de plus 1% du PIB mondial.

C'est pourquoi, plus que jamais, mettre en place un garde-fou pour choisir les bonnes couvertures d'assurance et ne pas en faire un sujet secondaire est une évidence à intégrer dans les logiques d'entreprise.

Compétences

Pour apporter l'expertise attendue, un bon responsable des assurances devra :

· Avoir une compréhension globale des enjeux globaux de la cybersécurité et des risques cyber, à l'échelle de l'entreprise, mais aussi à l'échelle nationale et internationale
· Être expert dans la collecte d'informations stratégiques auprès des acteurs impliqués sur le sujet, à la fois au sein de l'entreprise et du côté des assureurs
· Déployer une forte capacité d'analyse afin de déterminer la meilleure équation d'assurance possible
· Opérer un travail de veille soutenu, auprès des professionnels de l'entreprise et à travers des sources externes (presse et assureurs concurrents, notamment) afin de s'assurer que le contrat d'assurance reste pertinent dans le temps, compte tenu de l'évolution des facteurs de risque.



L'AVIS DE LA PROFESSIONNELLE

« La personne responsable des assurances met en place un système de soutien adéquat qui permettra à la structure d'être épaulée comme il se doit dans ses finances. Et c'est cela qui lui permettra très certainement de ne pas sombrer. »

Cécile P.
Responsable des assurances

QUALITÉS

Le responsable des assurances doit impérativement faire preuve :
· D'une qualité de contact supérieure, ce qui lui permettra d'obtenir les informations les plus pertinentes, à la fois auprès des professionnels impliqués dans l'approche des sujets cyber au sein de l'entreprise, afin de sécuriser leurs besoins, et auprès des assureurs eux-mêmes, afin de cerner avec la plus grande précision leurs propositions
· D'un talent pour la négociation, de sorte à parvenir au meilleur équilibre possible entre la force de l'assurance souscrite et le coût tarifaire qui lui est associé.

Les qualités de dialogue du responsable des assurances lui permettront également de conduire des échanges fluides avec l'assureur en dehors des périodes d'incidents : de cette manière, il sera possible de vérifier que le contrat souscrit reste toujours pertinent dans le temps, en fonction de l'évolution des facteurs de risque. En cas contraire, ce lien de qualité garantit que le contrat pourra être modifié et mis à jour sans perdre de temps.

Études

On exige, en règle générale, que les prétendants au poste de responsable des assurances aient décroché un Bac+5 minimum. La spécialisation en cybersécurité est par ailleurs un passage quasi obligé. Certains professionnels qui se démarquent par une expérience probante dans le domaine de la cybersécurité ou un talent particulier dans le relationnel et la négociation réussissent à décrocher un premier emploi sur la base d'un Bac+3. Il s'agit cependant d'une situation relativement rare, prenant en compte les qualités exceptionnelles de certains candidats.

Salaire

Pour une première prise de poste, un responsable des assurances peut réussir à négocier un salaire mensuel brut de 2 800 euros environ. Il pourra assez facilement prétendre à un salaire plus élevé dès lors qu'il dispose d'une expérience conséquente :

· Sur des postes stratégiques ou techniques liés à la cyberdéfense
· Dans des fonctions juridiques
· Dans le domaine de l'assurance et, mieux encore, de l'assurance cyber. C'est la case à cocher pour demander un salaire maximal.

Un professionnel confirmé pourra faire évoluer son salaire jusqu'à 4 650 euros brut par mois environ.

Où travailler ?

On pense, à tort, que la fonction de responsable des assurances cyber est le fait exclusif des grandes entreprises et des grands groupes. De fait, les structures de taille importante ont peut-être plus facilement tendance à intégrer ce métier dans leur propre structure. Mais on n'est pas en reste du côté des start-ups. Certes, ces dernières cherchent parfois leur « référence en assurance » auprès de consultants externes, mais il n'est pas rare de voir un poste créé sur ce point, quitte à l'enrichir d'autres attributions, toujours en connexion avec la stratégie de défense cyber.

Sur cette base, il est possible de s'orienter vers une multitude de secteurs : de la start-up spécialiste des applications de rencontre ou de commerce en ligne à la grande banque d'investissement, en passant par l'enseigne de luxe ou l'industrie automobile, par exemple.

Les publications les plus vues pour des postes de responsable des assurances font apparaître des noms comme :

· Airbus et Bosch, sur le terrain de la construction de véhicules et du transport
· Le groupe Auchan
· Le groupe LVMH dans le domaine du luxe
· Le groupe BPCE et la Société Générale, du côté des banques
· Ou encore Softeam, société de conseil qui accompagne la transformation des entreprises.

Évolution de carrière

S'il souhaite donner un autre tournant à sa carrière, le responsable des assurances devra viser un autre poste lié à la compréhension globale des enjeux de cybersécurité et à la vision stratégique qui doit en découler. Son expérience passée le conduira naturellement vers des fonctions de conseil.

Si, avant son poste de responsable des assurances, il a fait partie de forces opérationnelles et techniques, il pourra sans grande difficulté se reconvertir en consultant en cybersécurité ou en formateur en cybersécurité.

Sans spécialisation technique, il existe une évolution naturelle vers un poste de responsable du plan de continuité d'activité, avec la charge d'assurer la poursuite sans encombre des activités de l'entreprise en cas d'incident majeur.

Un responsable des assurances pourra aussi se replacer, sans grande surprise, chez un assureur spécialisé en cybersécurité ! L'importance de soigner son réseau est donc double : il en va de l'intérêt de l'entreprise pour laquelle est souscrite l'assurance, mais aussi des perspectives futures de l'employé.

Avantages et inconvénients

« Même si le poste de responsable des assurances est stratégique et absolument décisif, on a l'avantage d'être à l'abri de la pression directe : les décisions se font dans le calme et la réflexion à froid. Bien entendu, en cas d'un mauvais choix d'assureur, la responsabilité qui pèse sur nous est extrêmement lourde. Mais nous échappons à proprement parler à la partie la plus désagréable des situations de crise », explique Cécile P. Parmi les autres avantages fréquemment cités, on retient l'importance du relationnel – qui permet de se bâtir un réseau pouvant se révéler très bénéfique – et le côté valorisant des actes de négociation.

L'AVIS DE LA PROFESSIONNELLE

« Le ou la responsable des assurances, dans la sphère cyber comme ailleurs, c'est la personne qui sécurise le périmètre. Non pas pour se protéger contre les incidents et les attaques informatiques : nous avons des experts de la technique pour ça. Mais, si une attaque vient à frapper l'entreprise, cela ne nous expose pas seulement à des problèmes techniques : il y a un coût économique et, en règle générale, il n'est pas des moindres. »

Cécile P.
Responsable des assurances

35 RESPONSABLE DU CONTRÔLE INTERNE

Niveau d'études : Bac+5

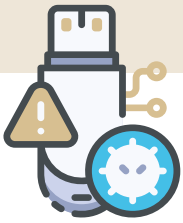
Spé Conseillée : Eco. et Soc.

Employabilité : Très bonne

Salaire débutant : 4 850 €

Code ROME : M1402 - Code FAP : L5Z

VOUS AVEZ L'ÂME D'UN CAPITAINE DE NAVIRE ET VOUS NAVIGUEZ SANS PROBLÈME PARMI LES CODES ADMINISTRATIFS ? VOUS POURRIEZ BIEN FAIRE UN PARFAIT RESPONSABLE DU CONTRÔLE INTERNE. FACE AUX NOUVELLES CATÉGORIES DE MENACES PROPRES À L'ÉPOQUE CYBER, CE MÉTIER N'A JAMAIS ÉTÉ AUSSI CRUCIAL POUR LA PROTECTION DES ENTREPRISES. CERTES, LES DÉFIS À RELEVER SONT PLUS NOMBREUX. MAIS C'EST AUSSI CE CONTEXTE DE TENSION ACCRUE QUI REND LE MÉTIER PLUS PASSIONNANT. VOYONS ENSEMBLE COMMENT TRACER SA VOIE JUSQU'À CE POSTE À HAUTE RESPONSABILITÉ.



Missions

Avant toute chose, le responsable du contrôle interne aide à définir les jalons et points d'attention qui permettront de vérifier que les systèmes de défense sont bien en place. Il collabore, pour ce faire, avec les organes dirigeants et chefs de département : en un mot, toutes celles et tous ceux qui connaissent le bon fonctionnement de la structure, mais aussi les spécialistes de la stratégie cyber.

Une fois cette politique de contrôle bien définie, c'est au responsable du contrôle interne d'assurer le déploiement opérationnel des dispositifs de contrôle et de gestion de risques opérationnels. Il lui revient également d'évaluer l'efficacité de ce dispositif et, si besoin, de proposer des mises à jour et des améliorations.

Le responsable du contrôle interne est impliqué dans trois types de tâches, ayant trait à de la conception pure, de l'accompagnement et de l'évaluation. S'ajoutent des missions de gestion de service et de transmission d'informations.

Il revient tout d'abord au responsable du contrôle interne :

· De définir tous les éléments permettant d'organiser le contrôle interne, de la politique de contrôle générale à la charte plus précise, en passant par le processus de pilotage et le rôle attribué à chaque acteur de la chaîne
· Et de mettre à disposition de toutes les parties intéressées un référentiel de contrôle interne, ainsi que des guides méthodologiques, qui nécessiteront des mises à jour au fil du temps

Ce spécialiste des bons processus est

« LE CONTRÔLE INTERNE EST UNE FONCTION CRUCIALE POUR TOUTES LES ENTREPRISES : C'EST ELLE QUI RÉALISE L'ADÉQUATION ENTRE L'ATTEINTE DES OBJECTIFS QUI ONT ÉTÉ FIXÉS ET LA MAÎTRISE DES RISQUES LIÉS À LA POURSUITE DE CES MÊMES OBJECTIFS. »

aussi un accompagnant. C'est lui qui doit sensibiliser la direction générale aux bonnes pratiques de contrôle interne. Il doit par ailleurs déployer une véritable culture du contrôle interne, assurer une harmonisation des pratiques des différentes unités impliquées et être la boussole de l'attitude à tenir face à un risque. Le responsable devra aussi :

· Participer pleinement à la conduite du changement, en anticipant les améliorations nécessaires au maintien des activités et à la maîtrise des risques
· Animer le réseau des différents agents de contrôle interne
· Aider les différents managers à adapter, si besoin, les mesures de contrôle interne à la situation particulière de leur équipe ou de leur département
· Airiger le programme d'auto-évaluation du contrôle interne dans chaque unité

En matière d'évaluation, le professionnel du contrôle interne doit alimenter la cartographie des risques. Il doit également mettre en place un certain nombre d'indicateurs de suivi de l'efficacité du système de contrôle et organiser des vérifications sur le terrain : le contrôle interne, c'est aussi du concret !

Le rôle revêt également une dimension de dialogue et de communication :

· En interne, en rendant compte aux instances dirigeantes, notamment au comité d'audit, du niveau de maîtrise des risques
· Et au-delà, en préparant des communications externes sur la gestion du contrôle interne dans la structure

Enfin, le responsable du contrôle interne assume de pures fonctions de gestion de service. Il est tenu d'administrer l'outil de contrôle interne, c'est-à-dire la base de données réunissant le référentiel de contrôle, le guide des bonnes pratiques et les indicateurs de suivi, entre autres. Il doit assurer une veille réglementaire sur les normes de contrôle interne et soumettre des rapports à ce sujet aux instances décisionnaires.

Compétences

Dans le contexte cyber, on attend du responsable du contrôle interne une certaine familiarité avec les grandes lignes techniques propres à la sécurité informatique. Cela lui permettra d'affiner les systèmes de contrôle de manière intuitive et de mener sans problème les dialogues utiles avec toutes les parties prenantes de la sécurité informatique.

Les principales aptitudes requises concernent cependant la gestion d'entreprise et la connaissance des processus classiques d'audit. De fortes capacités analytiques sont la base pour réussir à ce poste.

Études

Il faudra présenter un Bac +5 pour postuler à une offre de responsable du contrôle interne. Une expérience préalable à un poste élevé d'administration des entreprises ou sur des missions d'audit sera un atout de taille.

QUALITÉS

Le responsable du contrôle interne doit principalement faire preuve :
· D'un sens de l'organisation à toute épreuve
· D'une qualité de contact à même d'embarquer toutes les parties prenantes dans la grande mission de contrôle interne
· D'un goût infatigable pour les détails
· D'une capacité d'initiative qui se révélera précieuse pour faire évoluer le système de contrôle
· De réactivité, en cas d'ajustement nécessaire

Salaire

La hauteur que prend la mission du responsable du contrôle interne le place directement à un niveau de salaire de 4 850 euros brut par mois pour un premier poste. Ce salaire peut être ajusté à la hausse en fonction de la teneur des expériences passées. Un professionnel ayant touché à l'audit ou ayant analysé de près les questions cyber pendant plusieurs années sera valorisé. En fin de carrière, on peut s'attendre à des salaires avoisinant les 8 330 euros brut mensuels.

Où travailler ?

La fonction de responsable du contrôle interne est relativement commune dans le monde de l'entreprise. On pourra donc s'orienter vers une multitude de secteurs, selon ses appétences personnelles et les opportunités du moment. Les spécialistes du secteur de la santé – assureurs et entreprises de service – cherchent fréquemment des professionnels capables de prendre en main le contrôle interne, en raison de la sensibilité de leurs données. Le même constat s'applique au secteur de l'assurance et de la banque. On pourra aussi surveiller de près les grands groupes pharmaceutiques, les entreprises axées high tech et innovation en règle générale, ainsi que les instituts de recherche et les revendeurs en ligne.

Parmi les recruteurs recherchant activement des responsables du contrôle interne sur la période récente, on notera :

· La plateforme de recrutement HelloWork
· Bastide Groupe, spécialisé dans les services de santé
· Le conseiller en recrutement AdSearch
· Manpower
· Le CNRS et l'Inserm, du côté des structures publiques.

Évolution de carrière

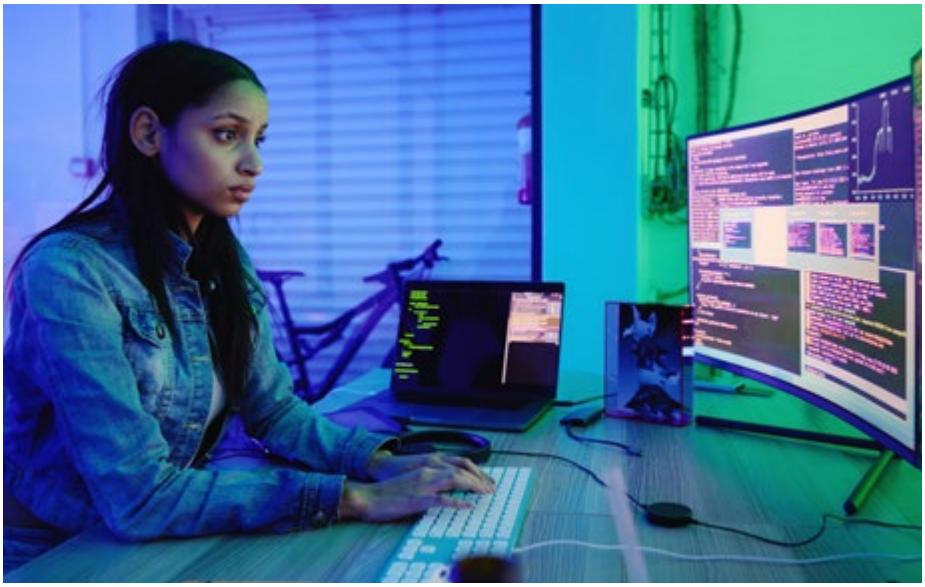
La connexion directe avec les missions d'audit et de gestion globale du risque cyber offrent au responsable du contrôle interne de bonnes dispositions pour se reconvertir en consultant en cybersécurité. Pour avoir une vraie légitimité et une assurance de réussite à ce poste, il est cependant préférable de bénéficier d'une expérience préalable particulièrement forte sur les points techniques ou de suivre les bonnes formations complémentaires.

Les profils techniques les plus solides pourront même prendre à des fonctions de responsable de la sécurité des systèmes d'information (RSSI). Ce n'est cependant pas le chemin de carrière le plus fréquent.

Les transferts vers le « risk management » sont courants. Un repositionnement en tant qu'auditeur en cybersécurité est aussi possible, à condition, une fois de plus, de disposer des ressources techniques indispensables. Dans ce dernier cas, l'exercice en tant que professionnel indépendant est la voie la plus naturelle, afin d'obtenir des niveaux de rémunération supérieurs et de dessiner une véritable évolution de carrière.

Avantages et inconvénients

Nathalie M. en est à son troisième poste de responsable du contrôle interne. Après une courte intervention auprès d'une grande plateforme de e-commerce, elle est passée dans le secteur bancaire. Ses sept années d'expérience lui donnent le recul nécessaire pour analyser les défis et les plaisirs de ce métier : *« Prendre les rennes du contrôle interne, c'est savoir jongler avec certaines contradictions. Il s'agit à la fois de ne pas sortir des sentiers battus et, en même temps, de surprendre : il faut à la fois maintenir des mécanismes de sécurité vus et revus, parce qu'ils sont efficaces et nécessaires, mais aussi sentir la tendance du risque et s'assurer que sont mises en place des protections pour des menaces qui n'existent pas encore. Un compromis entre l'administrateur dans tout ce qu'il a de plus carré et rébarbatif, et le devin ! »* Pour Nathalie M., le poste revêt dans tous les cas de figure un aspect nettement valorisant. À l'époque du tout-cyber, le poste a par ailleurs tendance à s'élargir dans ses responsabilités et à se renouveler, avec de belles opportunités de formations complémentaires à la clé.



« LE CONTRÔLE INTERNE FAIT PARTIE DE TOUTES CES FILIÈRES QUI CONTRIBUENT À LA DÉMARCHE GLOBALE DE CYBERSÉCURITÉ SANS EN FAIRE DIRECTEMENT PARTIE : LES SUJETS DE CONTINUITÉ D'ACTIVITÉ, DE PROTECTION DES DONNÉES À CARACTÈRE PERSONNEL, DE « RISK MANAGEMENT », DE SÛRETÉ OU ENCORE D'ASSURANCE SONT À RANGER DANS LA MÊME CASE. »

56

MALWARE ANALYST

Niveau d'études : Bac+5

Spé Conseillée : Scientifique

Employabilité : Très bonne

Salaire débutant : 5 170 €

Code ROME : M1802 - Code FAP : M2Z

ON AURAIT TENDANCE À DIRE QUE CE MÉTIER EST FAIT POUR LES GEEKS DANS L'ÂME, LES DÉVELOPPEURS CHEVRONNÉS ET LES PETITS GÉNIES EN HERBE. MAIS LA FONCTION DE MALWARE ANALYST EST BIEN PLUS QUE ÇA. FACE À DES VIRUS INFORMATIQUES SANS CESSE RENOUVELÉS, TOUJOURS PLUS NOMBREUX ET TOUJOURS PLUS PERFECTIONNÉS, CETTE MISSION EST DEVENUE LE NERF DE LA GUERRE POUR LES STRUCTURES QUI DOIVENT SE DÉFENDRE CONTRE LES HACKERS ET LES PROGRAMMES MALVEILLANTS. ANALYSTES DE DÉTAIL, INGÉNIEURS VITAUX POUR LA SURVIE DES ENTREPRISES, LES ANALYSTES DE MALWARES SONT DESTINÉS À ÊTRE DE PLUS EN PLUS SUR LE DEVANT DE LA SCÈNE. ET DEVRAIENT BÉNÉFICIER DE PERSPECTIVES DE SALAIRES – ET DE CARRIÈRES – TOUT AUSSI PROMETTEUSES. FAISONS ENSEMBLE LE TOUR DE CE MÉTIER D'AVENIR.

Missions

Bien qu'ils ne soient généralement pas considérés comme faisant partie de l'équipe de réponse aux incidents à proprement parler, et bien qu'ils ne soient pas tout à fait en première ligne de défense, les malware analysts sont souvent appelés à la rescousse pour les premières étapes de réaction à une attaque. Leur rôle, alors, est de clarifier sans attendre le type d'intrusion mis en œuvre. L'analyste de logiciels malveillants jouera aussi un rôle important dans les efforts d'atténuation et de récupération, une fois le mode d'attaque identifié et la menace contenue. *« Le malware analyst, c'est ce geek très sérieux – institutionnalisé pourrait-on dire – qui passe au microscope les virus informatiques pour en comprendre le fonctionnement et penser un vaccin, en quelque sorte. Il s'agit de savoir comment cet organisme technologique fonctionne, quelles sont ses cellules nocives, quelle est la gravité de sa toxicité. »* C'est en passant par le parallèle biologique que Cyril F. définit la mission quotidienne qui est à la sienne, au sein d'un entreprise qui pense des solutions de cybersécurité pour les paiements en ligne.

La mission principale de cet ingénieur très spécialisé est de passer au crible, suite à une attaque, l'outil – autrement dit, le logiciel malveillant ou « malware » – qui a provoqué l'incident. *« Son but est de fournir des éléments de compréhension aussi approfondis que possible sur les méthodes de l'attaque. Si elles sont nouvelles, l'examen devra être encore plus poussé, pour comprendre quelles sont les nouvelles pistes techniques en vogue chez les hackers. Le malware analyst, c'est en réalité un œil de lynx technologique »*, confie Cyril F.

Compétences

Il est important de préciser, d'entrée de jeu, que chaque structure est susceptible de rechercher un ensemble de compétences uniques, correspondant à ses besoins propres. Toutes les entités ne sont pas soumises aux mêmes types de menaces cyber ou au même niveau de risque. Les fiches de poste pour recruter un nouveau malware analyst peuvent donc être très variées d'une structure à l'autre, mais aussi au sein d'une même structure. Tout dépend du contexte du moment.

On peut néanmoins lister un certain nombre de compétences essentielles que devra réunir n'importe quel analyste de logiciels malveillants. Sur le plan technique, celui-ci doit notamment :

· Être familier de différents débogueurs d'immunité, notamment IDA Pro, WinDbg ou OllyDbg
· Avoir une solide connaissance du langage C/C++ et de Windows API
· Être capable de reconstruire des formats de fichiers et des structures de données inconnus
· Savoir reconstruire des protocoles TCP/IP inconnus
· Comprendre les techniques de déballage, de désobscurcissement et d'anti-débogage
· Être à l'aise avec les outils de scripting Python, Perl et Ruby

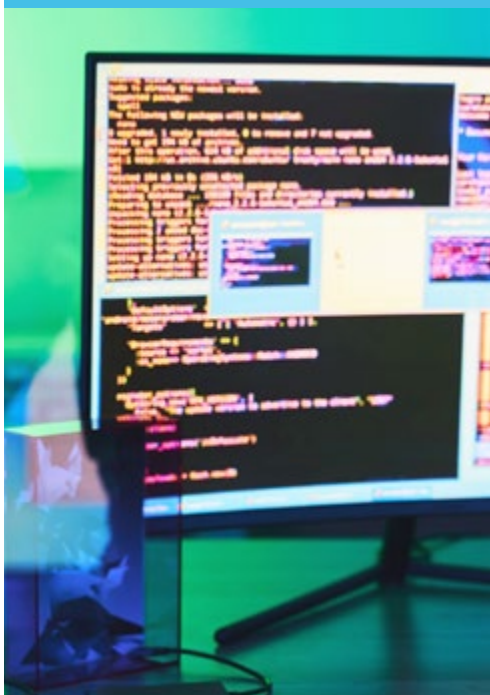
Parmi les autres compétences clés figure la capacité à rédiger des rapports techniques, en s'adaptant si possible à différents publics (expert et expert confirmé).

D'un point de vue général, le malware analyst est aussi chargé :

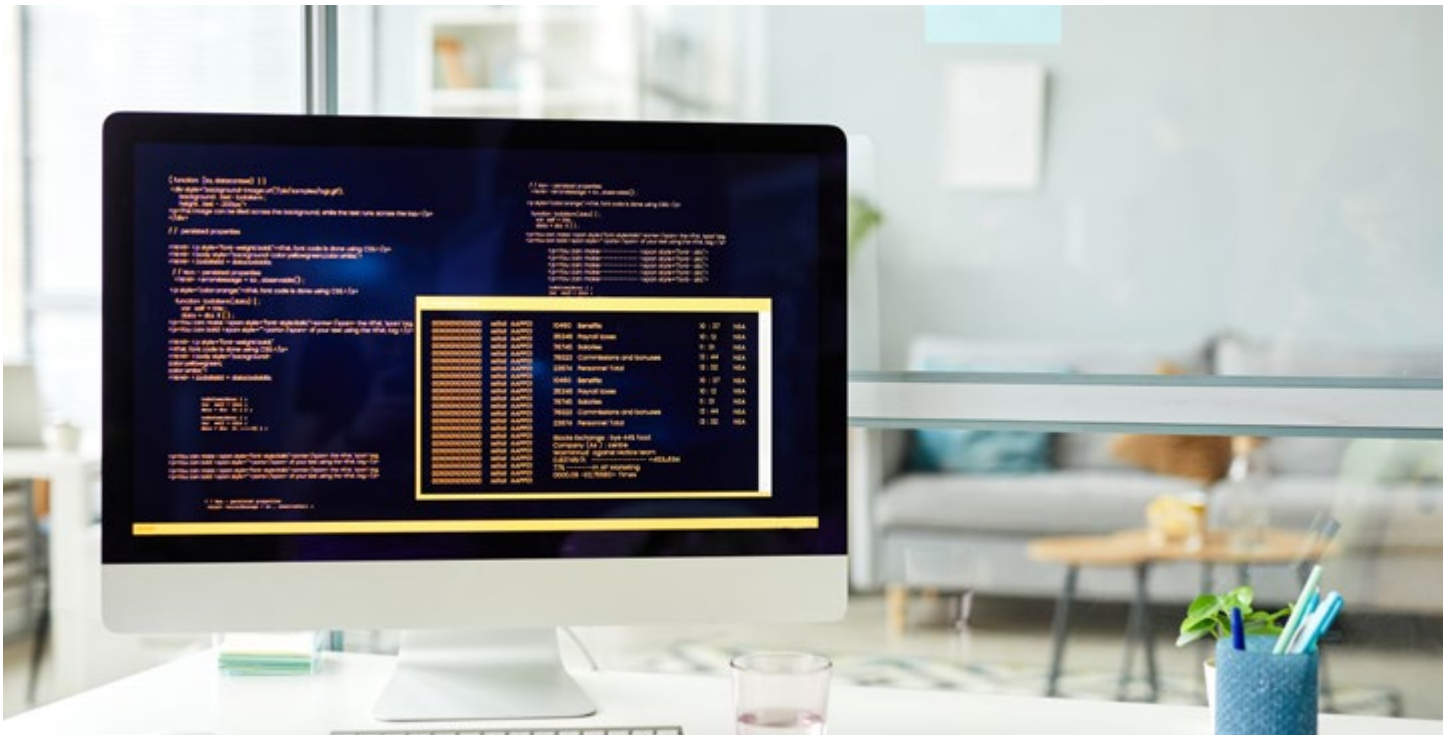
· D'enregistrer les menaces de logiciels malveillants repérées au niveau de la structure
· D'identifier les systèmes de protection pouvant aider à les éviter
· D'examiner les programmes et les logiciels malveillants à l'aide de programmes d'analyse afin de cerner la technologie en présence et leur fonctionnement
· De tenir une classification des logiciels malveillants en fonction de leurs ressorts techniques et de leur potentiel de nuisance, parmi d'autres caractéristiques
· De mener un travail de veille sur les derniers logiciels malveillants et d'enclencher une mise à jour des logiciels employés au sein de la structure afin de se prémunir contre les nouvelles menaces
· De rédiger des alertes afin de tenir l'équipe de sécurité informée
· d'aider à la création de documents qui serviront à affiner les politiques de sécurité
· Être attentif aux menaces de type zero-day et aux outils qui les accompagnent

QUALITÉS

Pour être opérationnel et trouver sa place au sein d'une équipe, le malware analyst doit se démarquer par :
· Une forte capacité de concentration, sur le temps long, qui sera la base de la pertinence de ses analyses et de sa réactivité en cas d'incident
· Une aptitude à emmagasiner et garder en mémoire une très grande quantité d'informations, afin de recouper les données rapidement et de décrypter le plus vite possible les logiciels d'attaque encore inconnus
· Une capacité rédactionnelle confirmée, qui doit permettre la préparation de rapports techniques à la fois complets et lisibles en peu de temps
· Une grande disponibilité d'esprit, pour maintenir toutes les compétences citées à leur niveau maximal.



« LE RÔLE DE MALWARE ANALYST OCCUPE UNE PLACE DE PLUS EN PLUS DÉTERMINANTE AU SEIN DE LA HIÉRARCHIE DES MÉTIERS CYBER. C'EST CE PROFESSIONNEL DE HAUT NIVEAU TECHNIQUE QUI EST CHARGÉ DE TRAQUER, COMPRENDRE, PARER ET ANTICIPER LES LOGICIELS MALVEILLANTS ET LES ATTAQUES QUI LEUR SONT LIÉES. »



Études

La condition de base pour accéder à un poste de malware analyst est, comme sur la très grande majorité des postes cyber, l'obtention d'un Bac +5 minimum. Bien entendu, présenter un diplôme de niveau supérieur, témoignant d'un degré plus poussé de formation technique ou de travaux de recherche sur des questions informatiques, donnera un large avantage aux candidats concernés.

Salaire

Le premier salaire pour un analyste malware se situe en règle générale autour de 5 170 euros brut par mois. Les professionnels justifiant d'une spécialisation particulière ou d'une connaissance approfondie d'un type de virus donné se trouvent en bonne position pour négocier un salaire légèrement supérieur, notamment si les virus en question revêtent une importance stratégique pour l'entreprise. Il en va de même pour tous les ingénieurs et analystes au fait des derniers penchants techniques des hackers : leur capacité à anticiper les risques à venir peut faire l'objet d'une valorisation dûment méritée. La marge de manœuvre entre le début et la fin de carrière est de l'ordre de 3 000 euros : on peut viser un salaire de 8 550 euros brut par mois, en moyenne, avec un profil senior.

Où travailler ?

Le malware analyst trouve une utilité dans tous les domaines susceptibles de susciter l'intérêt des hackers – autrement dit, tous les secteurs et toutes les structures, ou presque ! Plus le champ d'activité est sensible, plus le rôle du malware analyst est essentiel. Les grands groupes en général, et toutes les entreprises faisant face à un traitement important de données personnelles ou à la gestion de mannes financières importantes, sont des employeurs potentiels à surveiller de très près. Au cours des dernières années, on a pu par ailleurs relever de nombreuses offres d'emploi auprès des professionnels de la santé, du e-commerce ou du paiement en ligne. Les banques et assurances ne sont pas en reste, de même que les grands acteurs du divertissement (chaînes de télévision et plateformes de streaming en tête).

Parmi les entreprises en recherche fréquente d'analystes de logiciels malveillants, on retiendra notamment :

- Gatewatcher
- Atos
- Thales
- Cyberdian
- CyberTee
- Orange Cyberdefense
- Squad
- ANSSI (Agence nationale de la sécurité des systèmes d'information)

« SPÉCIALISTE HYBRIDE, ENTRE L'INGÉNIEUR EN SÉCURITÉ ET L'EXPERT EN ANALYSE FORENSIC, MAIS AUSSI UN PEU PROGRAMMEUR DANS L'ÂME, L'ANALYSTE DE MALWARES EST IMPLIQUÉ DANS LA LUTTE CONTRE LA CYBERCRIMINALITÉ DANS CE QU'ELLE A DE PLUS CONCRÈTE ET DE PLUS TECHNIQUE. »

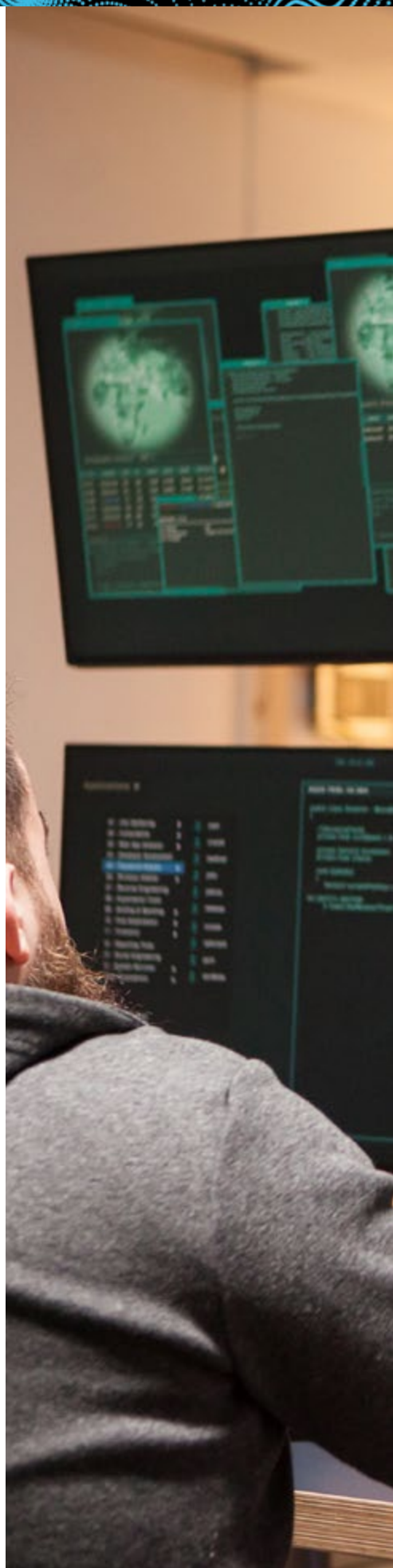
Évolution de carrière

Un malware analyst dispose d'un bagage technique fortement valorisable dans toute la sphère cyber. S'il souhaite rester sur des fonctions analytiques tout en élargissant son spectre et son périmètre de réflexion, il pourra évoluer vers un poste d'analyste en cybersécurité. D'analyste de détail, il passera à analyste stratégique, amené à donner les orientations globales destinées à construire les défenses cyber à l'échelle de la structure. De même, il pourra devenir consultant en cybersécurité, soit au sein d'une structure, soit en proposant ses services en tant que professionnel indépendant, pour maximiser ses revenus.

Après cinq ans de carrière minimum, un analyste malware souhaitant grimper dans la hiérarchie et présentant des qualités managériales évidentes pourra également viser un poste de responsable de la sécurité des systèmes d'information (RSSI) ou de directeur de la cybersécurité. Cela suppose encore une fois, au-delà de la finesse d'analyse technique, une approche globale de la problématique cyber et une vision à 360° des rouages de la structure concernée.

Avantages et inconvénients

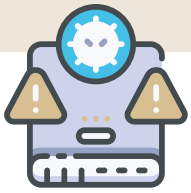
« Être analyste de logiciels malveillants, c'est avoir une compétence dure qui sera toujours valorisée et pourra peser lourd au moment de penser une évolution professionnelle. Cela suppose néanmoins de ne jamais arrêter d'être curieux et d'avoir une grande capacité de captation d'information : il s'agit presque d'aller au devant des nouvelles trouvailles des cyberattaquants, de se mettre à leur place et dans leur tête, pour désamorcer la bombe qu'ils lâchent sur nos entreprises. »
En résumant les points forts et les défis de son métier, Cyril F. rejoint la plupart de ses homologues pour dire qu'être malware analyst, c'est accepter d'être dans l'effort intellectuel soutenu et permanent, tout en bénéficiant d'une sensation d'enrichissement et d'apprentissage continu – la formule parfaite pour ne pas se lasser facilement !



Niveau d'études :	Bac+2
Spé Conseillée :	Scientifique
Employabilité :	Très bonne
Salaire débutant :	2 900 €

Code ROME : M1802 - Code FAP : M2Z

DIFFÉRENTES ÉTUDES CONSTATENT QUE LES ENTREPRISES QUI ONT ADOPTÉ LES PRINCIPES DEVOPS INNOVENT PLUS RAPIDEMENT ET SONT AINSI PLUS COMPÉTITIVES QUE LEURS CONCURRENTS. IL N'EST DONC PAS ÉTONNANT QUE LES DEVOPS SOIENT RECHERCHÉS. EN UN MOT, ILS PERMETTENT D'OPTIMISER LE DÉVELOPPEMENT D'APPLICATIONS ET DE LOGICIELS. UN INGÉNIEUR DEVOPS INTRODUIT EN EFFET DES PROCESSUS, DES OUTILS ET DES MÉTHODES POUR ÉQUILIBRER LES BESOINS TOUT AU LONG DU CYCLE DE DÉVELOPPEMENT, DU CODAGE ET DU DÉPLOIEMENT, JUSQU'À LA MAINTENANCE ET À LA MISE À JOUR.



Missions

Les ingénieurs DevOps travaillent en étroite collaboration avec les développeurs de logiciels, les opérateurs système (SysOps) et d'autres membres de l'informatique de production pour gérer et superviser les versions du code. Ils doivent bien connaître la gestion de l'infrastructure informatique qui fait partie intégrante de la prise en charge du code logiciel dans des environnements cloud dédiés ou hybrides.

Leurs missions étant multiples, ces professionnels doivent être suffisamment agiles pour porter un chapeau technique et gérer différentes opérations simultanément.

Parmi les principales missions et responsabilités de l'ingénieur DevOps, on peut citer :

· Comprendre les exigences du client et les indicateurs clés de performance (KPI – Key Performance Indicators) d'un projet. Mettre en œuvre divers outils de développement, de test et d'automatisation

· Planifier la structure de l'équipe, les activités et la participation aux activités de gestion de projet
· Définir et paramétrer les processus de développement, de test, de mise en production, de mise à jour et de support pour le fonctionnement DevOps
· Avoir les compétences techniques pour examiner, vérifier et valider le code logiciel développé dans le cadre du projet
· Contrôler les processus tout au long du cycle de vie pour s'assurer de leur

respect et mettre à jour ou créer de nouveaux processus pour les améliorer et minimiser les gaspillages
· Encourager et construire des processus automatisés dans la mesure du possible
· Avec la mise en place d'une politique dite DevOpsSecu, il doit identifier et déployer des mesures de cybersécurité en effectuant en permanence une évaluation des vulnérabilités et une gestion des risques
· Sélection et déploiement d'outils CI/CD (Continuous integration/continuous delivery) appropriés

Compétences

Étant donné leurs différentes missions, ces ingénieurs maîtrisent tous les aspects techniques et les processus IT pour des opérations intégrées. Ils sont censés connaître les différents outils d'automatisation et les tests des processus.

Les diplômés en informatique ou en technologie informatique peuvent apporter certaines des compétences techniques nécessaires pour devenir un ingénieur DevOps. Cependant, les compétences requises pour gérer les opérations sont généralement acquises par l'expérience ou en s'inscrivant à des programmes de développement spécifiques, qui peuvent aider à faire avancer la carrière dans la direction définie.

Pour réussir la mise en œuvre de l'approche DevOps, ces ingénieurs DevOps doivent connaître les meilleures pratiques de la méthodologie DevOps :

Continuous Integration

Cette pratique exige des développeurs qu'ils fusionnent les modifications apportées à leur code dans un référentiel central, après quoi il exécute les constructions et les tests automatisés. L'intégration continue (ou IC en angalis) vise à identifier et à corriger les bugs plus rapidement, à améliorer la qualité des logiciels et à réduire le temps de validation et de diffusion des mises à jour logicielles.

Continuous Delivery

Dans cette pratique, les modifications du code sont construites, testées et préparées automatiquement pour la mise en production. Il s'agit de l'étape successive à l'intégration continue dans laquelle toutes les modifications du code sont déployées dans un environnement de test et/ou un environnement de production après la phase de construction.

Surveillance et journalisation

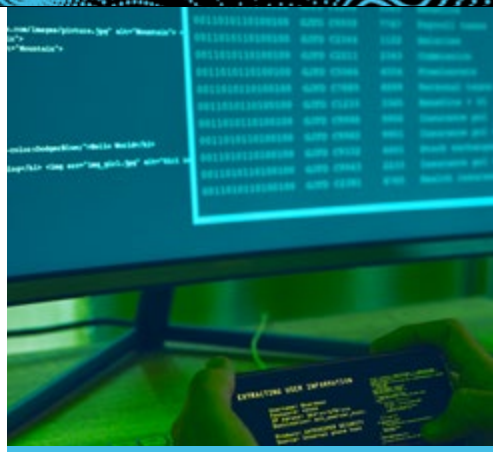
Elles sont essentielles pour vérifier et mesurer les métriques des applications et de l'infrastructure et voir comment leurs performances affectent l'expérience utilisateur d'un produit/service.

Architecture microservices

Il s'agit d'une approche de conception utilisée pour développer une application unique en tant que composant de petits services. Dans cette conception, les services individuels exécutent leurs propres processus tout en communiquant avec d'autres services via une interface bien définie (généralement une API basée sur HTTP).

Dès lors, les qualifications suivantes sont nécessaires :

· Connaissance des systèmes d'exploitation Linux, UNIX et Windows
· Configuration de divers logiciels de serveur tels que tomcat, apache, Nginx, Redis, MySQL
· Connaissance de différents langages de programmation et de script (Java, Python, Ruby, JavaScript, Scala, etc.)
· Principes d'équilibrage de charge et de haute disponibilité
· Principes de réseau et protocole TCP/IP.
· Connaissance des containers Docker et une bonne compréhension de Kubernetes (du design du cluster et des manifestes de déploiements), ainsi qu'une connaissance du fonctionnement des Messages broker (RabbitMQ)
· Connaissance d'Azure Devops (Chaîne CI/CD), du Cloud Public (Azure, AWS, GCP) et de l'Observabilité (Elastic Stack)



QUALITÉS

L'époque où chacun travaillait dans son coin est révolue. Les métiers de l'IT exigent aujourd'hui d'échanger en permanence avec d'autres services. Les DevOps n'échappent pas à cette règle, car ils gèrent des équipes et des opérations. Un DevOps doit donc être capable de collaborer avec les équipes d'exploitation et de développement. Un bon esprit d'équipe est donc indispensable !
Mais les tests représentent un ensemble de compétences important pour les DevOps. Si vous envisagez de faire carrière dans ce domaine, travaillez votre capacité d'analyse de la qualité.

Études

Bien que le concept DevOps soit relativement nouveau, il ne nécessite pas une formation ou des connaissances hyper spécifiques pour y accéder. La plupart des ingénieurs DevOps sont titulaires d'une licence en informatique ou en ingénierie, ou ont une expérience préalable de l'écriture de scripts avec Bash, Golang, Java, JavaScript, Perl, Python ou Ruby ou du travail avec Microsoft Linux ou Amazon Web Services.

Un Bac+5 en informatique est idéal pour postuler auprès de grands éditeurs ou d'autres entreprises.

Il est conseillé de suivre une formation supérieure en informatique (Bac +5, école d'ingénieur ou cycle universitaire équivalent, BTS ou DUT). Avoir un goût prononcé pour les mathématiques est indispensable.

Différentes écoles permettent de devenir DevOps, mais beaucoup de ces professionnels ont suivi une formation d'ingénieurs. Mais il est possible de suivre une autre voie en passant par un IUT.

Salaire

Lorsqu'il s'agit des CDI, les salaires des DevOps varient entre 40 000 (pour un débutant) et 75 000 euros brut par an pour des seniors. Un indépendant qui débute peut gagner autour de 500 euros par jour.

Où travailler ?

La démarche DevOps est loin d'être généralisée dans toutes les entreprises. Résultats, les postes à pourvoir se trouvent principalement dans les plus grandes startups, les éditeurs de logiciels et de grands comptes.

Évolution de carrière

Comme différents métiers IT, un jeune ingénieur DevOps peut monter en compétences pour devenir senior.

Freelance

Il est possible d'être indépendant pour proposer ses services de conseil aux start-ups et aux grandes entreprises qui ont des projets de cloud ou de pipeline de livraison de code nécessitant l'aide d'un expert en la matière. Mais la tâche est plus facile si vous avez acquis auparavant une expérience dans une entreprise.

Attention, être indépendant signifie aussi être responsable de sa gestion du temps et de sa quantité de travail.

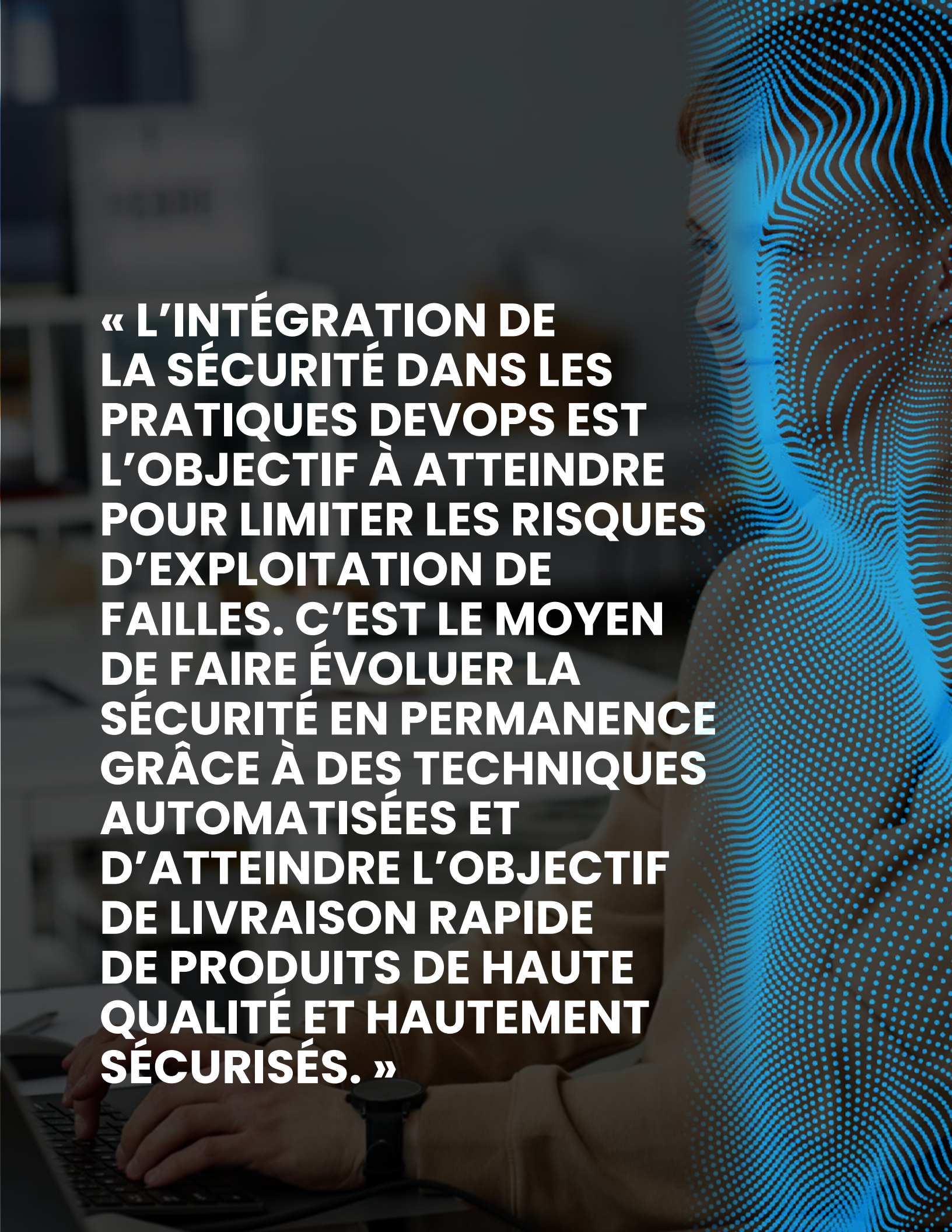
Comment le devenir ?

Un ingénieur DevOps est essentiellement un professionnel de l'informatique possédant une expertise en matière de script, de codage et de l'ensemble des opérations de développement et de déploiement de produits.

Il doit posséder une connaissance approfondie du cycle de vie du développement logiciel (SDLC) et être un expert dans la mise en œuvre de divers outils et processus d'automatisation DevOps pour résoudre des problèmes opérationnels complexes.

Ce rôle exige de transcender les barrières traditionnelles des équipes de développement, de test et d'exploitation des logiciels, et de créer un environnement holistique pour le développement de produits de qualité.

« LES INGÉNIEURS DEVOPS COLLABORENT AVEC LES ÉQUIPES DE DÉVELOPPEMENT ET D'EXPLOITATION POUR CRÉER, TESTER ET DÉPLOYER DES LOGICIELS DANS DES DÉLAIS COURTS ET RAPIDES. »



« L'INTÉGRATION DE LA SÉCURITÉ DANS LES PRATIQUES DEVOPS EST L'OBJECTIF À ATTEINDRE POUR LIMITER LES RISQUES D'EXPLOITATION DE FAILLES. C'EST LE MOYEN DE FAIRE ÉVOLUER LA SÉCURITÉ EN PERMANENCE GRÂCE À DES TECHNIQUES AUTOMATISÉES ET D'ATTEINDRE L'OBJECTIF DE LIVRAISON RAPIDE DE PRODUITS DE HAUTE QUALITÉ ET HAUTEMENT SÉCURISÉS. »

Niveau d'études : Bac+5

Spé Conseillée : Scientifique

Employabilité : Très bonne

Salaire débutant : 5 400 €

Code ROME : M1802 - Code FAP : M2Z

VOUS AIMEZ LES DÉFIS ET LES JEUX DE PISTE QUI REVÊTENT UN INTÉRÊT STRATÉGIQUE RÉEL ? VOUS IMMERGER DANS UN OCÉAN DE DONNÉES POUR Y DÉNICHER DES TRÉSORS D'INFORMATIONS QUI NE VOUS FAIT PAS PEUR ? VOUS POURRIEZ DEVENIR LE SPÉCIALISTE TECHNIQUE QUI AIDE LES STRUCTURES EN TOUS GENRES À RENFORCER LEUR CYBERDÉFENSE FACE À DES ATTAQUES SOUVENT OBSCURES. LE MÉTIER D'OSINTER OU D'OSINT ANALYST EST FAIT POUR TOUTES CELLES ET TOUS CEUX QUI ONT L'INTUITION DES DONNÉES STRATÉGIQUES AU SEIN D'UNE MULTITUDE D'INFORMATIONS OUVERTES AU GRAND PUBLIC. UTILISER L'EXISTANT POUR CHANGER LA DONNE, ET RENDRE ENTREPRISES ET STRUCTURES PUBLIQUES PLUS FORTES QUE LES CYBERATTAQUANTS : TELLE SERA VOTRE MISSION SI VOUS DÉCIDEZ DE DEVENIR ANALYSTE OSINT.

Missions

Les missions d'un OSINT Analyst sont intimement liées aux enjeux de threat intelligence. Ce professionnel est chargé de centraliser et d'analyser un maximum de données en accès public, dans le but de rassembler de nouvelles connaissances sur des attaquants potentiels, leurs motivations, leurs méthodes et leurs outils. À terme, il s'agit d'adapter et renforcer les protections de la structure – entreprise ou entité publique – sur la base de ces données et des tendances suspectées.

Dans la masse des informations rencontrées, il se doit de faire émerger des renseignements :

· Opportuns et pertinents
· Exploitables et de haute qualité, qui serviront au travail des équipes de la stratégie de cyberdéfense et aux techniciens opérant à leurs côtés.

« L'osinter, c'est la personne qui dispose des connaissances et réflexes technico-stratégiques pour repérer, parmi une multitude d'informations insignifiantes, celles qui seront utiles à l'entreprise et à la protection de ses réseaux, de ses données, de ses clients », précise Anouar K., qui occupe ces fonctions au sein d'une grande banque d'investissement.

« Il s'agit d'un métier à très forte composante technique, nécessitant beaucoup de dextérité et d'initiative dans la réflexion. Dans la grande masse des données publiques, qu'on pourrait comparer à une forêt dense, il s'agit de repérer des éléments utiles. Il faut donc avoir un instinct très fort pour savoir où

chercher. Il faut accepter de tâtonner, aussi, mais sachant réorienter ses recherches à temps. » C'est ainsi que Samuel K., OSINT analyst auprès d'une grande structure publique, décrypte ce qui constitue son travail au jour le jour. « *En quelque sorte, il est question d'aller trouver dans la nature – ces fameuses données publiques – des éléments et des matériaux solides qui permettront de consolider nos défenses, à nous, entreprise ou administration.* »

Compétences

L'OSINT analyst est amené à mobiliser des compétences en lien avec l'investigation et l'analyse, mais aussi la gestion de projet et l'approche technique des données.

Les savoir-faire premiers de l'osinter doivent lui permettre :

· De mener des enquêtes mobilisant toutes les capacités d'investigation dont dispose la structure pour laquelle il travaille, ce qui suppose un lien de qualité avec différentes équipes et une aisance technique face aux outils proposés
· De s'orienter de manière efficace parmi toutes les sources possibles de données en accès libre
· D'en extraire des renseignements techniques et stratégiques vérifiés, grâce au croisement de différentes sources
· De contextualiser les éléments recueillis
· De rédiger des rapports sur les faits observés.

L'investigation des sources de données libres inclut un travail particulièrement délicat sur le darkweb : c'est en effet sur le web caché et confidentiel que sont susceptibles d'être captées les informations à forte valeur ajoutée. C'est là que les hackers se « réunissent » souvent pour échanger sur les méthodes d'attaques, pour loger des versions bêta de logiciels malveillants et organiser leurs équipes. Pour une exploitation efficace des éléments en présence, l'Osinter doit déployer des techniques fines de dissimulation afin de ne pas être repéré, de pouvoir récupérer les informations utiles et de ne pas éveiller les soupçons des cyberattaquants – sans quoi ils seraient tenter de modifier leurs techniques d'attaque. Le travail d'enquête de l'Osinter perdrait alors tout son intérêt.

L'OSINT investigator est donc aussi un défricheur de tendances, amené à opérer une veille sur les techniques en vogue chez les hackers. Sa veille doit aussi porter sur les techniques d'investigation utile à ses propres fonctions.

Pour réussir, ce professionnel doit notamment avoir des notions de développement. Python, NodeJS, Typescript et Docker font partie des outils techniques souvent mentionnés dans les fiches de poste.

Sa formation technique doit aussi le rendre opérationnel pour développer des outils de collecte efficaces pour aborder de nouvelles sources d'information. Concernant les autres missions techniques, il devra être en mesure :

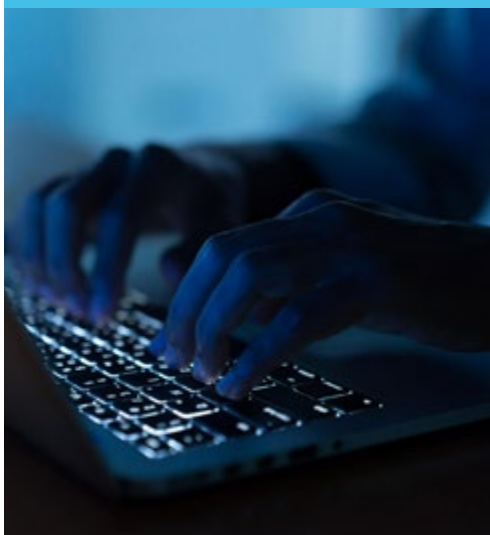
· D'assurer la conception, le développement et la maintenance de scripts utiles à l'investigation
· De manipuler les principaux outils – mais aussi les concepts – de threat intelligence. Cela concerne notamment la gestion de TIP, les référentiels MITRE ATT&CK ou encore la Kill Chain.

En matière de gestion de projet, il devra être apte à :

· Cadrer les missions pour obtenir l'aide de tous les départements intéressés
· Assurer la coordination du travail de tous les analystes mobilisés et des éventuels comités de pilotage mis en place sur des projets spécifiques.

QUALITÉS

Les qualités principales de l'analyste OSINT ont trait à sa grande appétence pour la résolution de problèmes et les situations complexes. Le défi intellectuel doit être une source de motivation majeure pour lui.
La capacité à rassembler rapidement le maximum d'informations sur le problème concerné, à l'ordonner et à en concevoir une compréhension générale, sans perdre de vue aucun détail, est tout aussi essentielle. Doit s'ajouter une qualité rédactionnelle, intimement liée aux capacités d'analyse et de synthèse.
Ils doivent maintenir le même niveau d'intérêt pour la nouveauté (les incidents inédits) et la répétition (les incidents répétitifs et largement connus). Une capacité de concentration à toute épreuve est indispensable. L'osinter doit aussi être particulièrement à l'aise pour mener de front plusieurs projets et doit savoir bien prioriser ses actions.



Études

De même que tous les métiers techniques de la sphère cyber, les fonctions d'analyste OSINT sont accessibles à partir d'un Bac+5. Toute formation technique de niveau supérieur, avec une spécialité en gestion et intelligence des données, sera fortement appréciée, de même que les cursus approfondissant les sujets de cybersécurité de manière générale.

Salaire

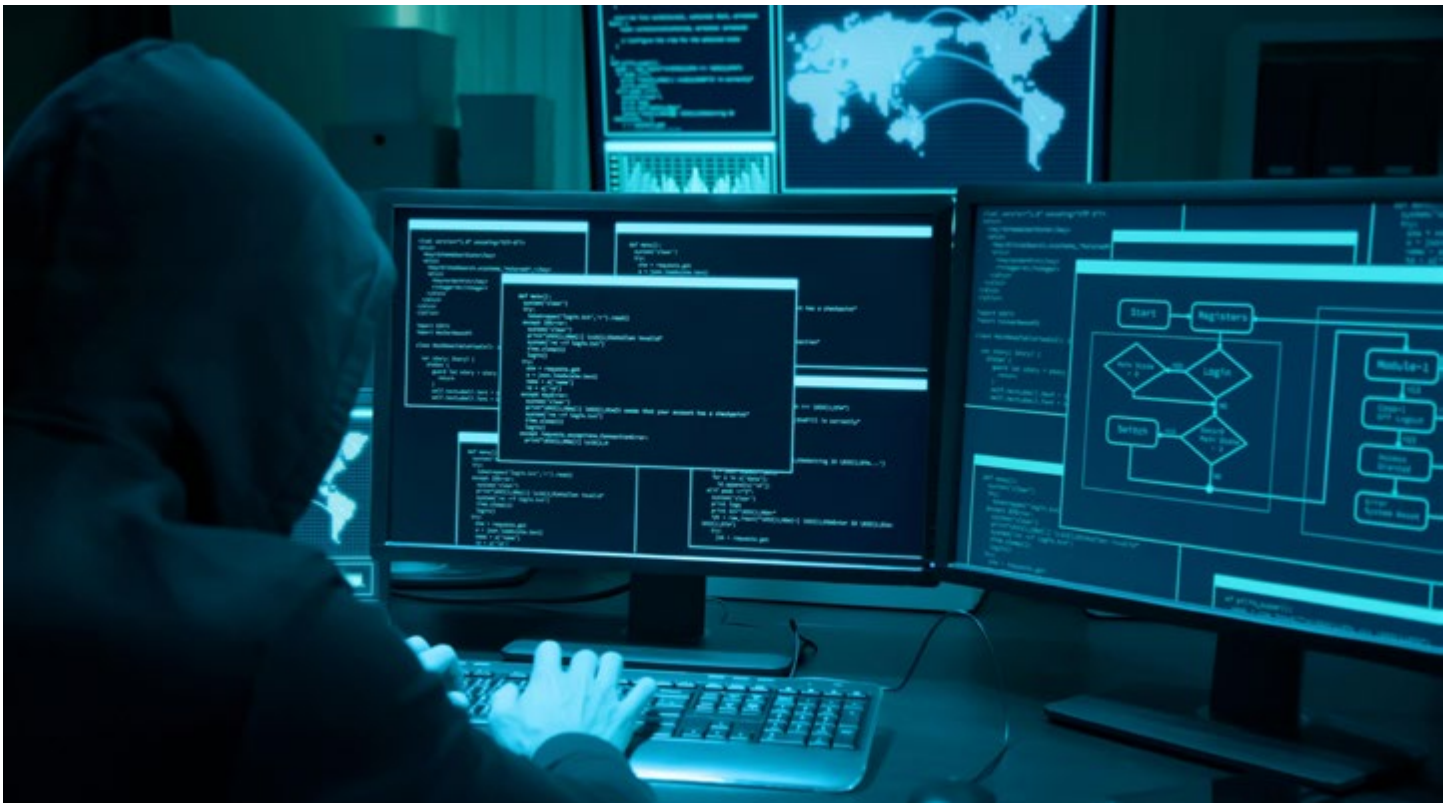
Le salaire de base moyen d'un analyste OSINT est de 5 400 euros brut par mois pour un premier poste. Deux ans de carrière suffisent pour se rapprocher de la frontière des 6 000 euros brut mensuels. En fin de parcours, un analyste OSINT touchera environ 8 200 euros brut par mois. Toute qualification complémentaire sur un point technique considéré comme rare entraîne, dans la plupart des cas, une petite majoration de ces niveaux de salaire.

Où travailler ?

Les spécialistes OSINT peuvent se placer dans toute structure présentant des enjeux de protection importants, soit en raison de la quantité de données sensibles qu'elle renferme ou traite, soit en raison d'enjeux stratégiques autres, liés souvent à un poids financier non négligeable. Les osinters seront particulièrement demandés auprès des banques d'investissement et autres structures bancaires, mais aussi auprès des services d'assurance et des services de santé. Les structures publiques liées à la défense ou aux questions intérieures sont elles aussi particulièrement concernées. Les nouveaux arrivants de la sphère du e-commerce, les entreprises de luxe et les acteurs de la bulle numérique sont d'autres secteurs où les emplois sont fréquents, parmi de nombreux autres domaines.

On détecte de nombreuses offres d'emploi à destination des OSINT analysts auprès :

· De spécialistes de l'audit et de la fiscalité, comme Ey
· Du CEA (Commissariat à l'énergie atomique et aux énergies alternatives) ;
· D'Airbus
· Du spécialiste de la cybersécurité XMCO
· D'EDF.



« CELUI QUE L'ON APPELLE COMMUNÉMENT OSINT ANALYST, OSINT INVESTIGATOR OU ENCORE OSINTER EST UN PROFESSIONNEL DESTINÉ À TRAVAILLER POUR L'OPEN SOURCE INTELLIGENCE, QUI DONNE LE NOM D'OSINT. L'INTELLIGENCE OPEN SOURCE, C'EST L'ACTE DE COLLECTER ET D'ANALYSER UN ENSEMBLE DE DONNÉES DISPONIBLES À GRANDE ÉCHELLE – DES DONNÉES PUBLIQUES – AFIN D'EN TIRER DES AVANTAGES POUR LA PROTECTION D'UNE STRUCTURE DONNÉE. »

Évolution de carrière

De par la nature de son poste, l'osinter peut facilement se positionner sur n'importe quel poste lié aux enjeux de threat intelligence. En développant davantage ses capacités de gestion et de coordination d'équipes dans un climat de haute tension, les OSINT analysts tendent aussi à se reconvertir en gestionnaires de crise de cybersécurité.

En élargissant leur champ de compréhension globale et dès lors qu'ils justifient de nombreuses années d'expérience dans leur métier, ils peuvent prétendre à des fonctions de niveau hiérarchique supérieur. Il n'est pas exclu de prendre la tête d'un CSIRT (Computer Security Incident Response Team) ou du CERT (Computer Emergency Response Team) ou encore de devenir responsable du SOC.

Avantages et inconvénients

« Chez l'analyste OSINT, il pourrait exister une certaine peur de ne pas trouver, ou de ne pas trouver assez bien – au sens d'éléments à valeur suffisamment stratégique pour que l'entreprise en tire parti et que le rôle de l'osinter soit valorisé », explique Samuel K. Mais c'est justement le principe de ce métier bien particulier : *« Savoir faire preuve de patience, souvent, avant de dénicher les éléments qui permettront d'avoir la certitude de n'être passé à côté de rien, de n'avoir laissé filtrer aucune menace. »* Anouar K. précise, pour sa part, que *« l'effet de relative surprise que constitue une découverte sur le darkweb, par exemple, a quelque chose de réellement exaltant – un peu comme si l'on était en mission secrète et que l'on réussissait une opération de sauvetage ! ».* En définitive, ces deux professionnels expérimentés estiment qu'il s'établit un équilibre entre certaines périodes pouvant sembler monotones et d'autres ponctuées de découvertes cruciales.

39 CLOUD SECURITY ANALYST

Niveau d'études : Bac+5

Spé Conseillée : Scientifique

Employabilité : Très bonne

Salaire débutant : 3 300 €

Code ROME : M1802 - Code FAP : M2Z

VOUS AIMEZ ÊTRE PRÉCURSEUR SUR DES TERRAINS ENCORE RELATIVEMENT PEU EXPLORÉS ? VOUS AVEZ ENVIE D'INVENTER LES TECHNIQUES DE CYBERDÉFENSE QUI N'EXISTENT PAS ENCORE À CE JOUR ? VOUS DEVRIEZ DONC REGARDER EN DIRECTION DES TECHNOLOGIES DU CLOUD ET ENVISAGER DE DEVENIR CLOUD SECURITY ANALYST. AVEC LA MONTÉE EN PUISSANCE DE CETTE SOLUTION DE STOCKAGE AUPRÈS DE TOUS LES TYPES DE STRUCTURES, CET EMPLOI STRATÉGIQUE EST PROMIS À UNE BELLE MONTÉE EN PUISSANCE ET PROMET DE BEAUX DÉFIS INTELLECTUELS. PETIT ÉTAT DES LIEUX DES AVANTAGES ET PRÉREQUIS DE CE MÉTIER À L'HEURE ACTUELLE.

Missions

De manière générale, lorsqu'il opère directement au sein d'un service de cloud computing, l'analyste en sécurité cloud est chargé d'aider à la conception et à la construction d'architectures de sécurité cloud, en mettant à jour régulièrement leur niveau de sécurité. Il teste les mesures et processus de sécurité cloud existants et conseille à l'occasion les clients du service sur les meilleures pratiques à adopter pour éviter l'apparition de failles.

Lorsque l'analyste est positionné chez le client, il opère une veille sur les meilleures solutions de cloud computing existant sur le marché – c'est-à-dire les mieux sécurisées. Lorsqu'un service précis de cloud computing a d'ores et déjà été adopté, il peut simuler des attaques à l'encontre des données stockées par son entreprise ou, afin de ne pas mettre en danger les données, établir des comparaisons avec d'autres solutions techniques.

« L'analyste en sécurité du cloud a la lourde de tâche de sécuriser un périmètre qui semble lointain et sans frontière », résume parfaitement Amélie M. Cette experte de 34 ans a d'abord travaillé auprès d'un service de cloud computing (celui de Google Cloud), avant de passer du côté du groupe Thales, afin d'améliorer le niveau de sécurité pour toutes les opérations transitant par le cloud. *« Être cloud security analyst au sein d'une entreprise qui utilise les services du cloud sans les produire ni les gérer, c'est s'assurer que la mise à distance des équipements ne devienne pas une mise en danger pour les données et les outils de l'entreprise »*. C'est également

faire en sorte qu'une solution innovante et moderne ne devienne pas un piège et un terrain de jeu ouvert pour les hackers.

Le but ultime est d'assurer une protection renforcée des données et la détection des menaces en temps réel.

Compétences

Les piliers de la sécurité cloud, que doit maîtriser tout cloud security analyst, sont :

· Les contrôles d'identification
· L'approche Zero-Trus
· La protection des applications via un firewall.

Au quotidien, cet expert technique doit par ailleurs être en mesure :

· D'effectuer des évaluations de risques d'attaque en évaluant chaque service utilisé et chaque technologie de sécurit
· D'analyser et tirer des rapports de ces exercices de testing
· De mettre en place des alertes dans l'environnement cloud afin d'être averti sans délai en cas d'attaque. Cette précaution n'est possible que pour certains types de cyberattaques déjà bien identifiés, sous couvert de non modification des techniques utilisées par les cyberattaquants.

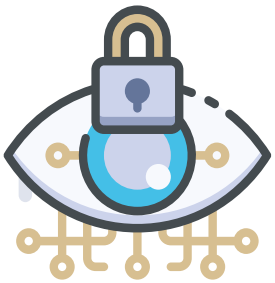
Le cloud security analyst doit également effectuer un travail de veille permanent sur l'évolution des technologies employées par les différents services de cloud computing d'une part, et par les cyberattaquants d'autre part.

Études

Comme n'importe quel métier technique de la sphère cyber, un poste d'analyste de la sécurité du cloud n'est pas envisageable sans un Bac +5 au minimum. Une formation poussée en informatique, incluant une appréhension fine de la problématique cyber, est par ailleurs indispensable.

Salaire

Pour un salaire bas, on peut compter environ 3 300 euros brut mensuels. Le salaire médian d'un cloud security analyst se situe cependant aux alentours de 4 530 euros brut par mois en France. Pour les profils confirmés justifiant d'au moins 7 ans d'exercice, ou pour un professionnel ayant accumulé d'autres expériences dans le domaine de l'analyse de cybersécurité, on pourra viser un salaire atteignant jusqu'à 8 900 brut mensuels. Pour les talents sortant réellement du lot, on a repéré, dans l'Hexagone, sur l'année 2022, des salaires dépassant les 10 000 euros mensuels brut.



« UN CLOUD SECURITY ANALYST EST CHARGÉ DE SÉCURISER LES SOLUTIONS DE STOCKAGE FAISANT APPEL À DES SERVEURS ACCESSIBLES SUR INTERNET, AINSI QUE LES LOGICIELS ET DONNÉES QUI TOURNENT SUR CES SERVEURS. »

QUALITÉS

· Un bon analyste en sécurité du cloud doit combiner une aptitude à la vision globale (des enjeux de cybersécurité) et à l'attention permanente aux détails (ceux propres à la technologie du cloud). Son travail suppose une capacité de compréhension d'enjeux techniques et stratégiques transverses et une aptitude à anticiper les problèmes : au quotidien, il doit faire preuve de curiosité et de capacité d'initiative pour aller au devant des nouvelles techniques qui pourraient potentiellement compromettre la sécurité du cloud et l'intégrité :
· Des données qui y sont hébergées
· Des logiciels et équipements qui y sont rattachés

Où travailler ?

L'équation est simple : puisque toutes les entreprises semblent destinées à adopter la solution du cloud, et qu'elles sont déjà très nombreuses à avoir sauté le pas, les professionnels du cloud ont devant eux de très larges horizons lorsqu'il est question d'options de recrutement. Tous les secteurs sont susceptibles de s'attacher les services d'un cloud security analyst, même si certains se montrent plus dynamiques dans leurs recherches. C'est notamment le cas du secteur de la banque et de l'assurance, de tous les services de santé dématérialisés, du domaine du luxe dans toutes ses composantes ou encore des plateformes de diffusion en streaming. Les acteurs du e-commerce ne sont, eux non plus, pas en reste.

Parmi les entreprises menant des campagnes actives de recrutement de cloud security analysts, on repère notamment :

- Atos
- Le groupe Thales
- Ericsson
- AXA
- Capgemini

Évolution de carrière

Le cloud security analyst a toutes les qualités pour passer sur d'autres fonctions de sécurité. Il peut ainsi devenir, sans rencontrer d'obstacles majeurs, analyste en sécurité – pour gagner une perspective plus globale de la question cyber – ou analyste du SOC. Les mécanismes intellectuels sont les mêmes et on peut compter sur une rémunération elle aussi similaire.

Après plusieurs années d'expérience, et après avoir pris soin, de préférence, d'avoir exercé à d'autres postes techniques et/ou stratégiques, l'analyste en sécurité du cloud peut envisager une reconversion en tant que consultant en sécurité, en indépendant de préférence – dans le cas où son objectif est non seulement un élargissement des sujets et une montée en puissance côté salaire.

Avantages et inconvénients

« En se positionnant sur une technologie d'avenir, le cloud security analyst fait immanquablement le choix d'un métier d'avenir. C'est une évidence pour la très grande majorité des métiers cyber, mais celles et ceux qui s'orientent vers un travail "dans le nuage" ont devant eux de grandes possibilités d'exploration : je suis persuadée qu'il y a mille mondes à inventer dans cette bulle détachée du physique, et cela promet d'être passionnant, pour nous avant tout », s'enthousiasme Amélie M. Parmi les défis du poste, on peut imaginer qu'au cours des années à venir, les hackers devraient devenir de plus en plus performants pour exploiter des failles propres au cloud. Les exigences et la tension subies par les analystes en sécurité spécialisés sur le cloud devraient donc s'accroître. *« Mais ce point peut être perçu aussi bien comme une difficulté à surmonter que comme une motivation et l'occasion de se dépasser intellectuellement »,* estime Amélie M.

SECURITY SERVICE DELIVERY MANAGER

Niveau d'études : Bac+5

Spé Conseillée : Eco. et Soc. ou Scien.

Employabilité : Très bonne

Salaire débutant : 3 750 €

Code ROME : M1802 - Code FAP : M2Z

VOUS AVEZ UN TALENT INNÉ POUR CONVAINCRE ? VOUS JONGLEZ AISÉMENT ENTRE LE DISCOURS COMMERCIAL ET L'ANALYSE TECHNIQUE ? VOUS AVEZ DONC LE PROFIL MULTI-CARTES QUI CONVIENT PARFAITEMENT AUX FONCTIONS DE SECURITY SERVICE DELIVERY MANAGER. TOUTE ENTREPRISE QUI PROPOSE DES SERVICES DE CYBERSÉCURITÉ DOIT S'ASSURER QUE LES SOLUTIONS PROPOSÉES SONT OPÉRATIONNELLES ET À MÊME DE SATISFAIRE LES BESOINS DE LEURS CLIENTS. EN APPORTANT DE NOUVEAUX CLIENTS ET EN ASSURANT UN SUIVI QUALITÉ DES SERVICES DE SÉCURITÉ, LE SECURITY SERVICE DELIVERY MANAGER CONTRIBUE À RENDRE SON ENTREPRISE TOUJOURS PLUS LÉGITIME SUR LES SUJETS DE CYBERDÉFENSE . ET IL PARTICIPE AUSSI, EN UN SENS, AU RENFORCEMENT DES DIFFÉRENTES SOLUTIONS EXISTANT SUR LE MARCHÉ CONTRE LES VÉRITABLES CHALLENGERS : LES HACKERS. VOICI LES PRINCIPALES FICELLES ET DÉFIS DE CE MÉTIER QUI INCORPORE DE PLUS EN PLUS LA DIMENSION CYBER.

Missions

Sur l'ensemble des services dont il assure la supervision, le security service delivery manager est tenu de mettre en place des indicateurs de suivi : ce sont eux qui permettront de déterminer si la qualité attendue est bien au rendez-vous – un point d'autant plus important lorsque le service a été contractualisé auprès d'un client en externe.

Parmi les tâches principales de ce gestionnaire de catalogue de services, on retient notamment :

· Gérer la prestation de services auprès de clients SOC, en suivant une méthodologie de gestion cohérente
· Rédiger des rapports de prestation de services à destination des clients ou de la direction de l'entreprise prestataire, dans le but d'assurer un réel engagement de service
· Assurer une analyse stratégique des concurrents et des autres solutions présents sur le marché
· Impulser les processus d'amélioration nécessaires sur les services de sécurité proposés
· Assurer la cohérence globale des services de sécurité
· Proposer une structuration pertinente de l'offre et une facturation judicieuse des services

Le security service delivery manager est aussi, de manière générale, responsable de l'identification et de la surveillance des résultats des risques de service. C'est encore lui qui assure l'élaboration et l'exécution des plans de correction, ainsi que le suivi des rapports et de la surveillance.

« LE SECURITY SERVICE DELIVERY MANAGER EST EN CHARGE DE PILOTER LES SERVICES DE SÉCURITÉ DONT IL A LA RESPONSABILITÉ, POUVANT ÊTRE MIS À DISPOSITION DE DIFFÉRENTS MÉTIERS ET DÉPARTEMENTS AU SEIN DE LA STRUCTURE DANS LAQUELLE IL OPÈRE. »

On attend également de lui qu'il garantisse la rentabilité du service et alerte toutes les parties intéressées en cas de situation dégradée. Il doit par ailleurs augmenter cette rentabilité en identifiant de nouvelles opportunités commerciales auprès des clients existants. La mise en place d'un programme de satisfaction client, sur la base d'un processus déterminé par les soins du security service delivery manager, est un autre point essentiel.

Enfin, il s'agit d'alimenter une documentation précise sur le fonctionnement et les performances des services, en y joignant toutes les bases de données nécessaires.

La fonction de security service delivery manager fait partie de ces métiers qui, à l'origine, ne sont pas spécifiques à la cybersécurité, mais peuvent être déclinés, réorientés et spécialisés en prenant en compte les enjeux de cette dernière. Ces métiers sont rencontrés presque exclusivement au sein des grands groupes et des grandes entreprises.

Dans le cas présent, le security service delivery manager effectuera toutes les tâches qui lui incombent habituellement, en rajoutant certains points d'attention cyber.

Compétences

En matière technique, on attend surtout du security service delivery manager une parfaite maîtrise d'outils bureautiques certes très classiques, mais essentiels pour lui au quotidien. Le tableur Excel est certainement son arme numéro un pour gérer ses catalogues clients de manière efficace et conduire avec la plus grande précision ses suivis d'analyses qualité. La maîtrise des outils de présentation de type PowerPoint est un autre évidence, en raison de la dimension commerciale du poste.

Il doit par ailleurs maîtriser les notions indispensables de gouvernance d'un système informatique. Il peut être en effet amené à mettre en place un dispositif de pilotage du SI. Les indications qu'il transmettra alors aux équipes techniques se doivent d'être justes et précises.

Un certain nombre de connaissances juridiques et réglementaires est requis, afin d'assurer :

· La conformité des services proposés avec les règles en vigueur, à l'échelle nationale ou européenne, notamment
· La juste contractualisation des besoins exprimés par le client et la mise en place des protections nécessaires pour le prestataire en cas de crise ou d'incident

Cette base juridique devra aussi permettre au professionnel de gérer en toute aisance les contestations et litiges commerciaux.

Afin d'assurer une couverture large de la clientèle, une très bonne maîtrise de l'anglais, à l'écrit comme à l'oral, est souvent requise. Cette capacité linguistique est par ailleurs précieuse pour naviguer sans encombre parmi les termes techniques, qu'ils concernent l'outillage informatique en lui-même ou des notions juridiques.

Pour assurer un parfait cadrage de projet, le security service delivery manager doit également disposer de tous les réflexes pour mener une parfaite analyse des besoins du client, ainsi que des risques et des opportunités présentés par chaque projet.

QUALITÉS

Un bon Security service delivery manager doit posséder de très bonnes capacités d'organisation et savoir gérer en parfaite autonomie un certain nombre de routines de gestion quotidiennes et d'opérations de suivi stratégique.
Il doit disposer d'un talent tout particulier pour établir et entretenir d'excellentes relations avec les clients existants et avec de futurs clients potentiels. Le dialogue doit aussi faire partie de ses qualités premières, afin de travailler main dans la main avec ces mêmes clients et de comprendre au plus près leurs besoins commerciaux et leurs besoins opérationnels.
L'esprit d'équipe et un esprit naturel de conseiller est un autre atout de taille, qui permettra de mettre en place une collaboration efficace au sein de l'entreprise afin de gérer :
· La résolution de problèmes rencontrés sur les services de sécurité
· Le suivi qualité sur ces mêmes services
· Ainsi que leur nécessaire mise à jour
Enfin, avoir une âme commerciale – ou des aptitudes de communicant particulièrement développées – est essentiel pour animer, alimenter et entretenir le réseau de clients.

Études

L'obtention d'un Bac +5 est la condition minimale pour accéder au métier de security service delivery manager intégrant une dimension de cybersécurité. Il est possible de suivre le parcours classique, à mi-chemin entre « gestion des entreprises » et « suivi technique », et d'y ajouter une formation spécifique aux enjeux de la cybersécurité pour légitimer son profil.

Salaire

Sur ce type de poste, le salaire mensuel brut d'un débutant se situe aux alentours de 3 750 euros. Dès lors que le professionnel bénéficie, en plus de ses qualités en tant que security service delivery manager, d'une ou plusieurs expériences en lien avec les problématiques de cybersécurité, le salaire est revu à la hausse : il peut atteindre facilement 4 100 à 4 200 euros mensuels brut pour un premier poste. Un profil senior peut espérer toucher jusqu'à 7 500 euros brut par mois en officiant pendant plusieurs années pour la même structure et en apportant, au-delà de ses compétences techniques et non techniques, une connaissance pointue de ses services, et donc une capacité à suggérer rapidement des améliorations pertinentes.

Où travailler ?

Une personne apte à prendre en charge les fonctions de security service delivery manager ne rencontrera pas de limitations particulières quant au choix de son secteur d'activité. La seule règle à respecter est de mener ses recherches d'emploi auprès de grands groupes et de grandes entreprises : les petites structures n'ont pas l'utilité de cette fonction. Les recherches doivent être concentrées sur les pourvoyeurs de services numériques, les assureurs en cybersécurité et autres acteurs de la cyberdéfense.

Parmi les entreprises en recherche soutenue de security service delivery managers qualifiés, on retiendra notamment les noms de :

- ITTrust
- Hellowork
- Capgemini
- Orange Cyberdefense
- Xelians
- Experis France

Évolution de carrière

« Un security service delivery manager qui souhaite faire un pas supplémentaire dans sa carrière, en ne perdant pas de vue la dimension cyber, est obligé de passer par la case formation. Il a besoin d'un renforcement technique qui lui permettra de se positionner sur des postes de formateur ou de consultant en cybersécurité, par exemple. C'est la voie que j'ai suivie », confie Jérôme N., ancien security service delivery manager en poste dans un grand groupe d'aéronautique, aujourd'hui consultant à son compte.

Il est aussi courant de voir les professionnels de cette branche réadapter leurs compétences commerciales pour se diriger vers le métier de communicant en cybersécurité. Il s'agit là d'une autre fonction qui, si elle n'a pas de lien direct avec les sujets cyber, y trouve une application concrète et spécialisée.

Avantages et inconvénients

Jérôme N. a pu profiter de huit années au poste de security service delivery manager pour analyser son métier de manière approfondie. Selon lui, l'une des principales difficultés est de *« faire valoir auprès des clients une légitimité qui peut être mise à mal par l'impression qu'on porte trop de casquettes à la fois : on est un peu technicien, beaucoup commercial, on analyse et communique à la fois – il s'agit de bien faire comprendre qui l'on est ».* Considérée sous un autre angle, cette multiplicité des casquettes – qui correspond aussi à une grande diversité des tâches – est la meilleure alliée contre la monotonie : entre contact humain et pure analyse de chiffres, un équilibre naturel se crée. Sans oublier que les réussites commerciales procurent une satisfaction directe et valorisent le security service delivery manager qui a bien mené ses projets !

« LE SECURITY SERVICE DELIVERY MANAGER EST LE PROFESSIONNEL DE RÉFÉRENCE QUI GARANTIT LA QUALITÉ DES SERVICES DE SÉCURITÉ PROPOSÉS, QUELLE QUE SOIT LA NATURE DE L'INTERLOCUTEUR. »

44 VULNERABILITY RESEARCHER & EXPLOIT DEVELOPER

Niveau d'études : Bac+5

Spé Conseillée : Scientifique

Employabilité : Très bonne

Salaire débutant : 3 250 €

Code ROME : M1802 - Code FAP : M2Z

VOUS ÊTES INFATIGABLE ET FAITES PREUVE D'UNE GRANDE INTUITION LORSQU'IL S'AGIT DE PARTIR À LA RECHERCHE DES FAILLES D'UN SYSTÈME INFORMATIQUE ? PLUS QU'UN INGÉNIEUR-DÉTECTIVE, VOUS ÊTES CELUI QUI EST CAPABLE DE COLMATER LES BRÈCHES EN PROPOSANT DES SOLUTIONS DE CORRECTION EFFICACES ? VOUS POURRIEZ DONC DEVENIR UN PILIER DE LA LUTTE CONTRE LES CYBERATTAQUES AUPRÈS D'UNE STRUCTURE QUI A BESOIN DE RENFORCER SES DÉFENSES. DE FAIT, À CE JOUR, TOUTES LES ENTREPRISES OU PRESQUE – SANS OUBLIER DE NOMBREUX ACTEURS PUBLICS – SONT À LA RECHERCHE DE VULNERABILITY RESEARCHERS & EXPLOIT DEVELOPERS DE TALENT POUR METTRE À JOUR, DE MANIÈRE PERMANENTE, LEUR ARSENAL DE CYBERDÉFENSE. À VOUS DE VOUS DÉMARQUER EN SUIVANT LES BONNES FORMATIONS ET INTÉGRANT TOUTES LES FICELLES DU MÉTIER !

Missions

Pour mener à bien sa tâche, le vulnerability researcher & exploit developer sera amené à conduire des tests d'intrusion, des revues de configuration ou encore des audits de code. Ce sont là les actions d'investigation les plus fréquentes : chaque système informatique, chaque logiciel et chaque application présente cependant ses spécificités propres. *« Cela implique d'adapter les tests et demande de faire part de suffisamment de créativité pour ne manquer aucune faille. Les criminels de la sphère cyber sont des créatifs en puissance : pour infiltrer nos systèmes, ils doivent souvent nous surprendre, en attaquant avec des logiciels que nous ne connaissons pas. Dans le camp opposé, nous nous devons donc d'être au moins aussi inventifs et astucieux pour repérer nos faiblesses cachées »,* nous explique Titouan L.M., Vulnerability researcher pour une société d'opérations techniques en haute mer, en Bretagne.

Le premier volet des missions du Vulnerability researcher prend la forme d'audits pour lesquels il doit :

· Collecter tous les éléments utiles concernant la configuration des systèmes et outils à auditer et effectuer une revue des configurations – on parle d'audit de configuration
· Procéder de même pour les éléments d'architecture – on parle alors d'audit d'architecture
· Mener une revue du code source pour les différents composants de l'environnement en question – c'est l'audit de code

· Imaginer et définir des scénarios d'attaque et les mettre à exécution lors de tests d'intrusion

Ces opérations prennent une dimension unique et ponctuelle, pour chaque environnement ou composant considéré. Au quotidien, le vulnerability researcher doit aussi mener des contrôles techniques et des scans de vulnérabilité, de manière continue et presque automatisée. Pour ce faire, il doit :

· Mener des entretiens auprès de toutes les unités et équipes techniques afin d'évaluer l'impact potentiel d'une attaque donnée
· Livrer des rapports sur les vulnérabilités rencontrées, en proposant une analyse détaillée et notamment une identification des causes, des risques et des conséquences pour chaque département et chaque métier
· Avancer des recommandations pour remédier aux risques inhérents aux vulnérabilités identifiées
· Travailler main dans la main avec les équipes techniques intéressées pour déployer les recommandations et solutions techniques proposées
· Construire des tableaux de bord pour tracer l'évolution du niveau de sécurité et de la conformité

Enfin, le vulnerability researcher & exploit developer assure une mission permanente de veille technique, qui porte sur les possibles scénarios d'attaque, le panorama des nouvelles menaces identifiées, ainsi que les nouveaux types de tests à disposition. Sur cette base, il contribuera à développer de nouveaux outils pour conduire les audits de sécurité.

Compétences

Sans grande surprise, le métier de vulnerability researcher and exploit developer repose sur une série de compétences et connaissances techniques dures. Parmi celles-ci, on compte notamment une parfaite connaissance :

· Des principes de sécurité des systèmes d'exploitation
· Des types de réseaux et protocoles
· Des couches applicatives
· Ainsi que de l'ensemble des normes, standards et principes de gouvernance en vigueur pour la bonne conduite des audits techniques

Est également attendue une parfaite maîtrise de la méthodologie des tests d'intrusion, qui constituent le cœur même de ce métier.

Le professionnel doit par ailleurs disposer de connaissances solides sur divers points liés à la cyberdéfense, notamment :

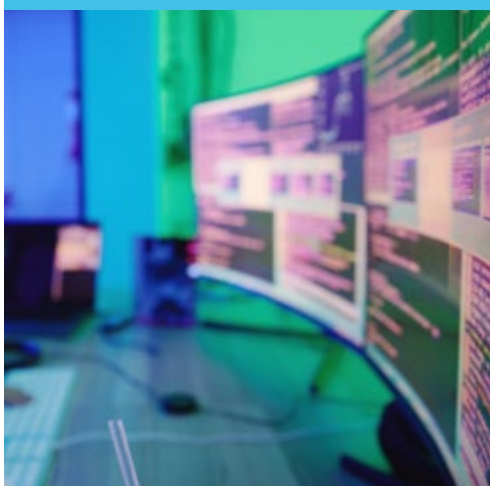
· Les techniques d'attaque et d'intrusion les plus courantes, mais aussi les plus confidentielles
· Les types de vulnérabilités les plus fréquents, pour la plus grande variété possible d'environnements

Des connaissances en reverse engineering et en scripting sont également indispensables. On attend par ailleurs de la part d'un bon Exploit developer qu'il maîtrise les notions de base du droit informatique, en particulier sur les points relatifs à la sécurité des systèmes d'information et à la protection des données.

QUALITÉS

Parmi les qualités indispensables pour réussir et s'épanouir à ce poste, on compte notamment :
· Une grande aptitude au travail en équipe
· Un sens aigu de la rigueur et le souci permanent du détail
· Des capacités rédactionnelles, intimement liée à une capacité de synthèse et de pédagogie, afin de transmettre les informations cruciales de la manière la plus efficace possible, à des publics présentant des niveaux de compréhension technique différents.

« LE VULNERABILITY RESEARCHER & EXPLOIT DEVELOPER EST CHARGÉ DE PASSER AU CRIBLE DIFFÉRENTS ENVIRONNEMENTS INFORMATIQUES STRATÉGIQUES – LE SYSTÈME INFORMATIQUE DE LA STRUCTURE DANS SON ENSEMBLE, UN LOGICIEL, UNE APPLICATION – AFIN DE DÉTECTER DE POSSIBLES FAIBLESSES, EXPLOITABLES PAR DES TIERS MALVEILLANTS. LORSQU'UNE FAILLE EST MISE À JOUR, C'EST À CE PROFESSIONNEL QUE REVIENT LA TÂCHE DE PROPOSER UNE ACTION CORRECTIVE ET LES MISES À JOUR NÉCESSAIRES. »



Études

L'accès à un poste de vulnerability researcher & exploit developer se fait sur la base d'un Bac +5 dans la plupart des cas. Il est possible, néanmoins, de faire valoir son potentiel en disposant d'un Bac +3 uniquement. Dans ce cas, une formation complémentaire, axée spécifiquement sur l'analyse de failles, est requise. Elle peut être pilotée directement avec l'entreprise qui recrute.

Salaire

Le salaire d'entrée pour un vulnerability researcher ayant validé un Bac +5 est de 3 250 euros brut mensuels en moyenne. Pour une prise de poste à Bac +3, on tablera davantage sur un salaire de départ de 2 900 euros brut mensuels. Pour un profil justifiant de 10 ans d'expérience, on peut atteindre un salaire jusqu'à 10 150 euros brut par mois environ.

Où travailler ?

Les traqueurs de vulnérabilités sont fortement demandés auprès de toutes les structures présentant des enjeux stratégiques et traitant des données sensibles. En d'autres termes, le spectre des recruteurs potentiels est particulièrement large. On pourra consulter en priorité les opportunités proposées par les entreprises du secteur des banques et assurances, les sociétés de conseil spécialisées en produits numériques et hautes technologies, le secteur des télécommunications, les services de streaming et les grosses entreprises du commerce en ligne. On n'oubliera pas les GAFAM, mais aussi l'ensemble des licornes émergentes. On pourra aussi faire un tour du côté des assureurs en cybersécurité !

Parmi les noms récurrents des recruteurs, on repère notamment :

- BNP Paribas
- AXA
- Thales
- Orange Cyberdefense
- Groupama
- Hiscox
- Bouygues Telecom
- Airbus
- Capgemini

Évolution de carrière

Il est fréquent pour un vulnerability researcher & exploit developer en quête de changement de se réorienter vers une red team ou une purple team. En tant que red teamer, il sera amené à simuler des attaques en grandeur réelle – une opération qu'il peut déjà être conduit à réaliser sur son poste de départ. En tant que purple teamer, son rôle sera davantage de donner des pistes et orienter le travail des équipes de détection des incidents de cybersécurité.

En tant que fin connaisseur des failles de sécurité, le vulnerability researcher peut envisager une multitude de postes à un niveau hiérarchique supérieur. Il pourra ainsi, après avoir acquis une expérience solide, se repositionner comme chef de projet de sécurité ou, à un niveau ultime, responsable d'un CSIRT (Computer Security Incident Response Team), d'un CERT (Computer Emergency Response Team), du SOC ou de l'ensemble des opérations de cybersécurité. Cela se décide sur la base d'un parcours riche et d'une connaissance transverse des différents enjeux de l'organisation en présence.

Une autre voie possible est celle du consultant en cybersécurité, avec des perspectives de salaire particulièrement intéressantes.

Avantages et inconvénients

« Le niveau de vigilance élevé requis en permanence peut, sur le long terme, être un vrai défi pour l'analyste de failles de vulnérabilité. Il y a aussi l'injonction être toujours plus créatif, perspicace, intuitif pour deviner dans quelle brèche les hackers pourraient s'infiltrer. Mais cet encouragement à sans cesse se renouveler – renouveler sa manière de penser et d'appréhender les problèmes, les logiciels, les systèmes – est ce qui motive chacun d'entre nous au jour le jour : c'est la promesse de ne pas rester bloqué sur ses acquis et de progresser, encore et encore », analyse Titouan L.M. Parmi les autres avantages et inconvénients évidents, on peut mentionner la grande responsabilité qui pèse sur le vulnerability researcher en cas de faille non détectée, qui va de pair avec un haut degré de valorisation lorsqu'il parvient à maintenir les défenses cyber à leur plus haut niveau.

L'AVIS DU PROFESSIONNEL

« La responsabilité du vulnerability researcher et de l'exploit developer, c'est de faire passer la défense de sa structure d'un bon niveau à un très bon - mieux, un excellent niveau. »

Titouan L.M.
Vulnerability researcher & exploit developer

CYBERCOMBATTANT

Niveau d'études : Bac+4 à +5

Spé Conseillée : Scientifique

Employabilité : Très bonne

Salaire débutant : 2 500 €

Code ROME : M1802 - Code FAP : M2Z

VOUS ÊTES CONSCIENT QUE LE MONDE A CHANGÉ EN PROFONDEUR ET QUE LA PROTECTION DES FRONTIÈRES SE JOUE DÉSORMAIS SUR UN TERRAIN INVISIBLE ? NOUS ASSISTONS AUJOURD'HUI À CE QUE L'ON APPELLE LA « GUERRE CYBER » : LES ATOUTS ET LES DONNÉES STRATÉGIQUES DES ÉTATS – ET DE NOMBREUX SERVICES PUBLICS PAR AILLEURS – PEUVENT ÊTRE CAPTÉS PAR DES ORGANISATIONS MALVEILLANTES, QUI EXPLOITENT AUTANT QU'ELLES LE PEUVENT LA DÉMATÉRIALISATION DE CES INFORMATIONS CRUCIALES ET LEUR TRANSIT DANS LA SPHÈRE INFORMATIQUE. DANS CE CONTEXTE A ÉMERGÉ UN NOUVEAU PROFIL : CELUI DU SOLDAT INFORMATIQUE, COMBATTANT NUMÉRIQUE OU CYBERCOMBATTANT. SON ACTION EST TOUT AUSSI CRUCIALE QUE CELLE MENÉE PAR LES ARMÉES CLASSIQUES ET LE RECRUTEMENT DE CES DÉFENSEURS DE LA NOUVELLE ÈRE A LE VENT EN POUPE. VOICI LE PARCOURS À SUIVRE POUR DÉBUTER UNE CARRIÈRE DANS LES RANGS D'UNE ARMÉE 2.0.

Missions

Le cybercombattant est formé pour prendre en main un certain nombre d'opérations techniques, à la dimension principalement défensive, et dans une moindre mesure offensive. Diverses activités de veille complètent le panel de ses missions.

Parmi les tâches techniques, on retiendra notamment :

· Une mission globale d'évaluation des systèmes, qui prendra notamment la forme d'audits, de tests d'intrusion et d'opérations de type red team

· Des missions d'administration système et sécurité

· Une partie d'ingénierie logicielle, consistant à participer à l'expression des besoins, à la conception de solutions techniques et à leur développement

· Une partie de lutte informatique défensive, consistant à évaluer la menace cyber de manière générale puis spécifique, à analyser les traces de tentatives d'intrusion et à prendre en char la supervision dans les SOC lorsque cela est nécessaire

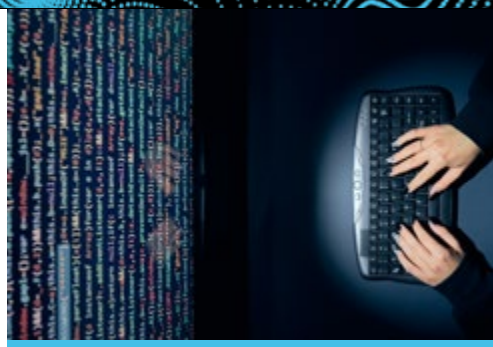
· Des opérations de lutte informatique défensive, lorsque les atouts de la structure sont menacés de manière directe et imminente

La partie veille consiste :

· À passer au crible l'ensemble des informations utiles circulant sur les réseaux sociaux, en s'intéressant notamment aux comptes suspectés d'être détenus par des hackers

· À établir un dialogue, lorsque

« LE TERME DE “CYBERCOMBATTANT” DÉSIGNE PLUS SPÉCIFIQUEMENT LES RECRUES DE L’ARMÉE, DES FORCES DE L’ORDRE ET D’AUTRES SERVICES PUBLICS MOBILISÉS POUR LA PROTECTION DES INTÉRÊTS NATIONAUX DANS LA GRANDE “GUERRE CYBER”. »



les exigences de confidentialité le permettent, avec d’autres instances publiques vigilantes et actives sur les points de cyberdéfense
· À rassembler et analyser l’ensemble des documents et informations pouvant être partagés par ces instances

Compétences

Les cybercombattants doivent être performants et bien formés sur l’ensemble des tâches et sujets techniques suivants :

· La Sécurité des systèmes d’information, ce qui inclut une bonne connaissance des types de menaces et des attaques de bas-niveau en particulier
· L’identification rapide des attaques les plus redoutées, liées notamment au spoofing, au DNS cache poisoning et à la technique Man in the Middle
· Une capacité à rechercher et pointer de manière efficace les vulnérabilités
· Des aptitudes opérationnelles en analyse forensic et en reverse engineering, avec une bonne pratique des environnements de rétro-ingénierie de type IDA ou GDB
· La connaissance de l’architecture interne des principaux systèmes d’exploitation et de leur mécanisme de sécurité, aussi bien sous Windows que sous Linux, MacOS, Android ou iOS
· Une parfaite maîtrise du scripting
· La maîtrise de l’éventail le plus large possible de langages informatiques et d’outils de développement, notamment Shell, C et C++, JAVA, ASM et Python
· La maîtrise des notions essentielles de cryptographie

Ces compétences sont complétées au cas par cas selon l’environnement dans lequel est appelé à évoluer le cybercombattant, le champ d’investigation spécifique qui lui est éventuellement attribué et le contexte de menace observé à l’instant t.

Études

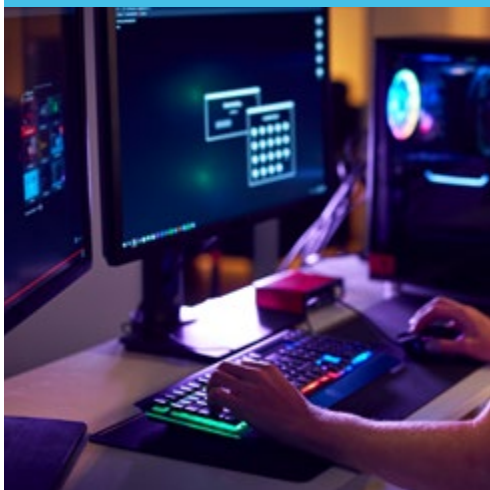
Les cybercombattants peuvent être recrutés à Bac +4 ou Bac +5 selon le type de périmètre confié et la nature de l’équipe à laquelle il est prévu de l’intégrer. En raison du caractère hautement stratégique de la fonction, les services des Armées ont tendance à se concentrer sur des profils d’ingénieurs ou d’experts en cybersécurité ayant validé un Bac +5 minimum. Lorsque les recrutements sont opérés par la Gendarmerie, notamment, on relève une plus grande tolérance pour les candidats munis d’un Bac +4. Ils bénéficient dès lors d’une formation complémentaire sur le terrain, l’objectif étant de disposer de talents aiguisés le plus vite possible.

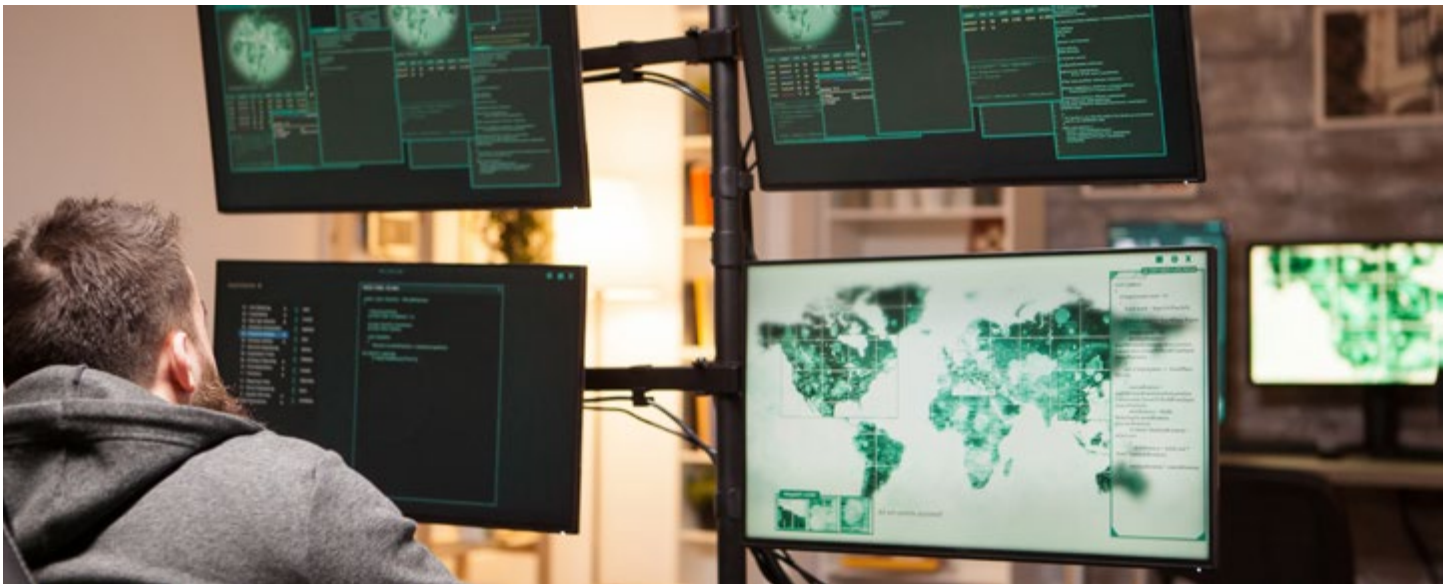
Salaire

Le salaire d’un expert de la lutte informatique est moins important pour une prise de poste dans le secteur public, en comparaison aux pratiques courantes dans le privé. Ainsi, un cybercombattant qui débute tout juste sa carrière, avec un Bac +5 en poche, doit compter avec un salaire approximatif de 2 500 euros brut par mois. Pour un premier poste à Bac +4, le salaire est plus proche de 2 300 euros. Pour un profil confirmé (au moins 10 ans d’expérience), on peut s’attendre à un salaire de 5 200 euros brut par mois environ.

QUALITÉS

La première qualité requise de la part d’un cybercombattant est celle de la confidentialité : la confrontation directe à des sujets d’intérêt public - voire, dans de nombreux cas, de sécurité publique - rend ce point plus essentiel que jamais.
Un sens solide de la hiérarchie et une grande aptitude au travail en équipe sont deux autres traits incontournables lorsque l’on envisage de rejoindre les rangs d’un groupe de défense cyber lié aux instances de l’État.
Comme pour les emplois cyber de nature tactique repérés dans le privé, il s’agira par ailleurs de faire preuve d’une grande rigueur, d’un sens de l’organisation sans faille et d’une curiosité permanente.





Où travailler ?

Envisager la carrière de cybercombattant, c'est dire oui à une carrière dans le public, auprès des unités en charge de la défense nationale principalement. À ce titre, plusieurs corps et sigles sont à suivre de très près pour ne manquer aucune vague de recrutement. Doivent être considérés avec la plus grande attention, au moment de la recherche de poste :

· Les services de l'Armée dans leur ensemble, à travers la DGA (Direction générale des armées)
· Le ministère des Armées
· Le ministère de la Défense
· La DGSE (Direction générale de la sécurité extérieure)
· les services de Gendarmerie et de la Police nationale
· À l'occasion, d'autres services publics stratégiques, pouvant être liés à des intérêts de santé par exemple

À noter que, pour rejoindre la DGSE tout particulièrement, les candidats sont soumis à un ensemble de tests psychologiques et d'enquêtes portant sur leur entourage, leur mode de vie et leur parcours global.

Évolution de carrière

Pour une personne intégrant les forces du cybercombat, franchir une étape supplémentaire dans sa carrière signifie, dans la plupart des cas, se voir confier des sujets plus stratégiques et plus confidentiels. Tout en conservant un poste de cybercombattant, le professionnel voit augmenter ses responsabilités et, en règle générale, son salaire. Il est également possible de monter dans la hiérarchie en se voyant confier la supervision ou la formation d'une équipe. L'étiquette de cybercombattant reste, une fois de plus, de vigueur.

En respectant certaines procédures et règles de confidentialité, un cybercombattant peut envisager une reconversion en tant que consultant en cybersécurité. Pour passer à cette activité dans le privé, il est en général demandé d'observer une certaine période de retrait, pendant laquelle l'ancien cybercombattant n'a pas le droit d'exercer.

Avantages et inconvénients

Rejoindre les équipes de cyberdéfense de la Gendarmerie nationale, de la DGSE ou de l'Armée va de pair avec un devoir de discrétion et de confidentialité important : au jour le jour, cette exigence demande des précautions importantes de la part du cybercombattant, dans ses cercles professionnels comme privés. Ce besoin d'attention soutenu peut être générateur d'une certaine tension et d'une fatigue psychologique. Les professionnels sont néanmoins bien accompagnés, en règle générale, dans la gestion de cet aspect particulier de leur métier. En contrepartie, les cybercombattants jouissent d'une reconnaissance non négligeable et d'une certaine aura de prestige : rattaché à une idée de modernité et de service envers le pays, le métier de cybercombattant est considéré avec beaucoup d'admiration.

43 JURISTE SPÉCIALISÉ·E EN CYBERSÉCURITÉ

Niveau d'études : Bac+5

Spé Conseillée : Scien. ou général

Employabilité : Bonne

Salaire débutant : 2 500 €

Code ROME : K1903 - Code FAP : L5Z90

LES ENTREPRISES INTÈGRENT DE PLUS EN PLUS DE NOUVELLES TECHNOLOGIES POUR AMÉLIORER LE TRAITEMENT DE LEURS DONNÉES. MAIS TOUTES LES DONNÉES N'ONT PAS LA MÊME IMPORTANCE. CELLES LIÉES À LA VIE PRIVÉE DES CLIENTS ET DES SALARIÉS ET AUX INFORMATIONS STRATÉGIQUES DOIVENT ÊTRE TRAITÉES AVEC LA PLUS GRANDE PRUDENCE. L'OBJECTIF EST DE RESPECTER LES RÉGLEMENTATIONS EN VIGUEUR ET DE LIMITER LES RISQUES DE VIOLATION DE DONNÉES. C'EST DANS CE CONTEXTE QU'INTERVIENT UN JURISTE SPÉCIALISÉ EN CYBERSÉCURITÉ.

Missions

Ce juriste apporte assistance et conseil grâce à une veille juridique permanente. Il alerte et rédige des notes et des rapports. Il propose des solutions concrètes et précises en adéquation avec les objectifs de l'entreprise.

Sa mission principale consiste à suivre en permanence l'évolution des règlementations qui concerne son entreprise ou ses clients (s'il travaille au sein d'un cabinet). RGPD, DSP2, PCI DSS..., les règlements sont multiples et complexes.

Il veille en particulier sur l'activité de la Commission européenne au sujet de la data. Il doit donc bien connaitre le RGPD. Ce règlement européen concerne le traitement des données à caractère personnel des clients et des salariés d'une entreprise. Toutes ces données doivent être sécurisées et exploitées en tenant compte des différentes obligations et processus détaillés dans le Règlement général sur la protection des données.

La 2ème Directive européenne sur les Services de Paiements (DSP2) vise à renforcer la sécurité des paiements en ligne et celle de l'accès aux banques en ligne ou aux applications bancaires. Pour cela, la DSP2 rend obligatoire «l'authentification forte», également appelée «authentification à deux facteurs» ou encore «double authentification».

Les mesures de sécurité énoncées dans les normes techniques de règlementation découlent de deux objectifs clés de la DSP2 :

· Assurer la protection des consommateurs

· Renforcer la concurrence et garantir des conditions de concurrence équitables dans un marché en mutation rapide

Quant à la certification PCI DSS (Payment Card Industry Data Security Standard), elle assure aux organismes bancaires et aux utilisateurs de services en ligne un haut niveau de sécurité. Les acteurs manipulant ces données confidentielles répondent à des exigences de sécurité spécifiques définies par cette certification.

Ces quelques exemples montrent que la tache d'un juriste spécialisé en cyber nécessite une bonne connaissance des règlementations et des enjeux en termes de cybersécurité.

Ces autres missions peuvent être regroupées en trois grandes catégories :

· Prévention : il prodigue des conseils à sa direction pour qu'elle mette en place une gouvernance de la donnée efficace et pérenne
· Information : il précise les répercussions pénales et/ou civiles des manquements en matière de sécurité informatique et de règlementation, en particulier en cas de violation de données personnelles. Depuis l'entrée en vigueur du règlement pour la protection générale des données personnelles (RGPD) en 2018, les organismes qui ne respectent pas les mesures indiquées s'exposent à des sanctions plus ou moins lourdes en fonction de la gravité de la violation

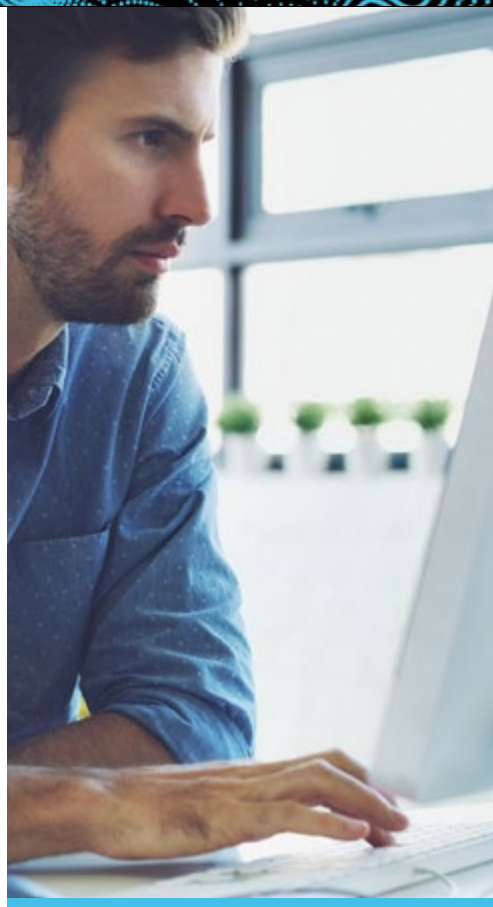
Les sanctions sont de diverses natures :

· Administrative
· Pénales
· Versement de dommages et intérêts
· Déficit d'image
· Gestion des contrats : il participe à la négociation et à la relecture de contrats IT en lien avec la DSI (Direction des systèmes d'information)

Dans le détail, les missions sont les suivantes :

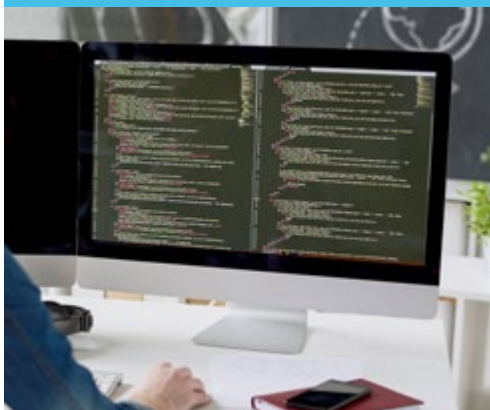
· Analyse, rédaction, révision et négociation des contrats en français et en anglais
· Participer aux contrôles et négociations des réponses aux appels d'offres lancés par le groupe
· Conseiller les opérationnels et analyser les risques sur des problématiques juridiques et RGPD dans le cadre de l'exécution des contrats et la conduite des activités de l'entreprise
· Participer à la gestion des litiges en matière de data, analyse de risques, gestion des relations avec les avocats, collecte des éléments de preuve notamment auprès des opérationnels, rédaction de courriers et de mises en demeure, rédaction et validation de protocoles transactionnels
· Participer à la rédaction et à la mise à jour des contrats types

« FACE AUX DIFFÉRENTES MENACES, LES ENTREPRISES S'APPUIENT SUR DES ÉQUIPES DÉDIÉES À LA CYBERSÉCURITÉ. MAIS LA RÈGLEMENTATION ÉTANT DE PLUS EN PLUS COMPLEXE ET ÉVOLUTIVE, LES ORGANISATIONS EMPLOIENT ÉGALEMENT DES JURISTES SPÉCIALISÉS DANS LE CYBER. »



QUALITÉS

Se plonger dans des textes complexes, comprendre les enjeux liés à la protection des données et à la e-réputation (l'image de marque de l'entreprise), partager son savoir avec sa direction et les autres salariés au travers de formations… telles sont les principales qualités que doit posséder un juriste spécialisé dans le cyber.



Compétences

Ces compétences sont à la fois juridiques et techniques. Un juriste doit en effet maitriser les lois et règlementations en vigueur (droit des technologies de l'information), mais aussi connaitre les différentes techniques employées par les cybercriminels pour lancer des cyberattaques ou des opérations de fraude.

La lecture des différents textes règlementaires détaillant également les processus à mettre en place pour être en confirme, il doit également bien connaitre les différentes méthodes de protection des données comme le chiffrement, la double authentification…

Enfin, un bon niveau d'anglais est un vrai plus.

Études

Pour devenir un juriste spécialisé en cybersécurité, il est recommandé de posséder un master en droit. Ce diplôme doit être, ensuite, complété par des formations dans le domaine de la cybersécurité et des règlementations propres aux secteurs d'activité dans lesquels le candidat souhaite travailler.

Salaire

Il varie selon la taille de la structure, le secteur et l'expérience. Un juriste cyber junior peut prétendre entre 2000 euros et 3 000 euros brut.

Un juriste cyber senior peut prétendre jusqu'à 7500 euros.

Où travailler ?

Le juriste spécialiste de la cybersécurité exerce généralement au sein de sociétés de services comme les ESN (Entreprise de Services du Numérique), les cabinets de conseils, les cabinets d'avocats. De grands comptes, des industriels et des éditeurs de logiciels sont également à la recherche de ce type de profil.

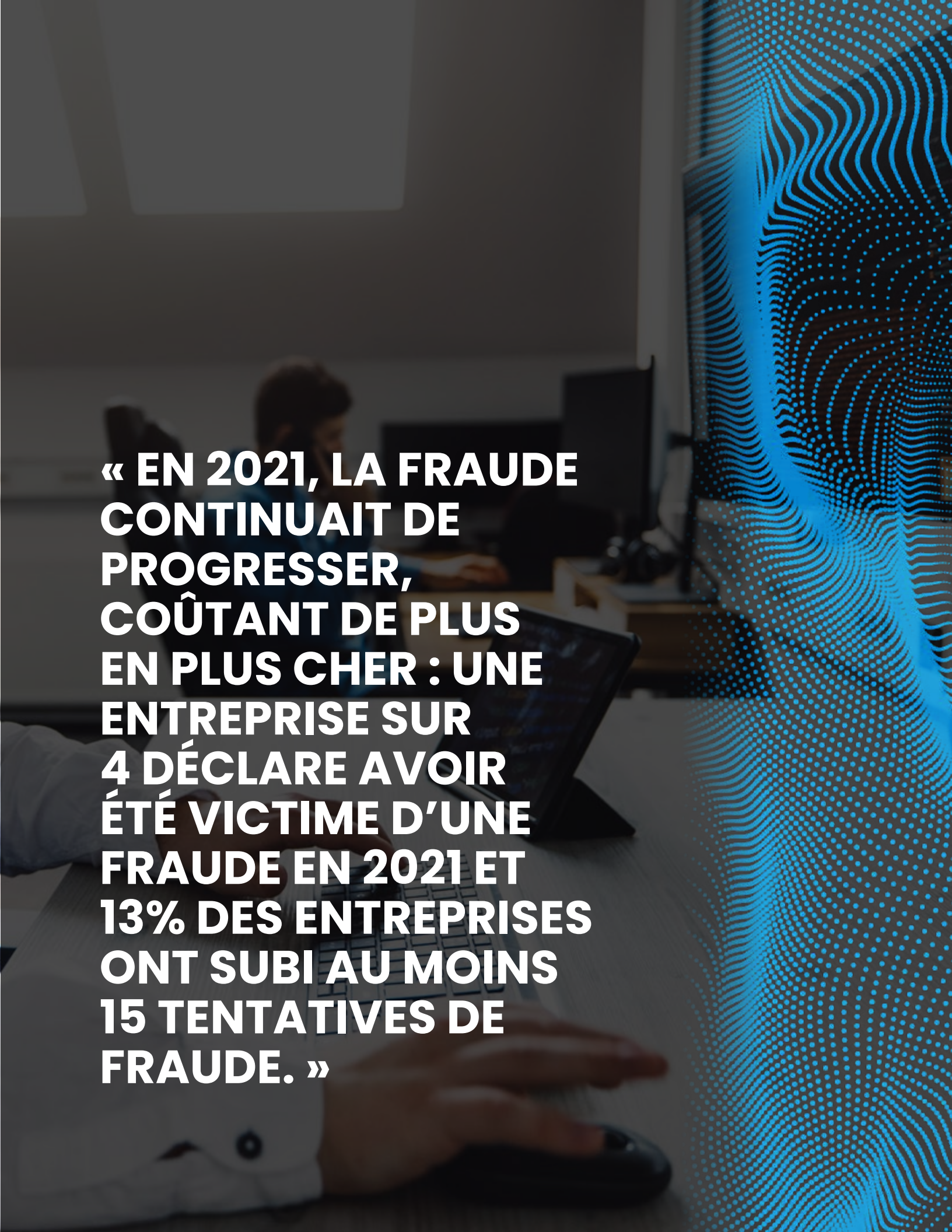
Évolution de carrière

Le cyber juriste peut évoluer vers des missions de plus en plus complexes ou choisir de se spécialiser pour devenir par exemple DPO. Il peut aussi briguer à des postes de directeur juridique, voire de responsable des Ressources humaines.

Comment le devenir ?

En permanence, les entreprises récupèrent, analysent et stockent des données. Certaines sont plus sensibles que d'autres (données personnelles et stratégiques). Elles doivent être traitées par des juristes maitrisant à la fois les règlementations et les techniques liées à l'informatique et aux nouvelles technologies comme le cloud.

« UN JURISTE SPÉCIALISÉ DANS LE CYBER INTERVIENT POUR LIMITER LES IMPACTS D'UNE CYBERATTAQUE ET LES TENTATIVES DE FRAUDES. »



« EN 2021, LA FRAUDE CONTINUAIT DE PROGRESSER, COÛTANT DE PLUS EN PLUS CHER : UNE ENTREPRISE SUR 4 DÉCLARE AVOIR ÉTÉ VICTIME D'UNE FRAUDE EN 2021 ET 13% DES ENTREPRISES ONT SUBI AU MOINS 15 TENTATIVES DE FRAUDE. »

14 CHARGÉ·É DE COMMUNICATION SPÉCIALISÉ·É EN CYBERSÉCURITÉ

Niveau d'études : Bac +2 min.

Spé Conseillée : Littéraire

Employabilité : Très bonne

Salaire débutant : 2 500 €

Code ROME : E1103 - Code FAP : M2Z

LE SECTEUR DE LA CYBERSÉCURITÉ EST UN MARCHÉ TRÈS DYNAMIQUE. IL EXISTE DE NOMBREUSES ENTREPRISES SPÉCIALISÉES DANS CE DOMAINE : ÉDITEURS DE LOGICIELS, CABINETS DE CONSULTANTS, PRESTATAIRES DE SERVICES... TOUS ONT BESOIN DE COMMUNIQUER SUR LEURS ACTIVITÉS AFIN DE TROUVER DE NOUVEAUX CLIENTS EN FRANCE ET À L'ÉTRANGER POUR LES PLUS IMPORTANTS GROUPES. CHARGÉ DE COMMUNICATION SPÉCIALISÉ EN CYBERSÉCURITÉ JOUE DONC UN RÔLE MAJEUR. IL S'ASSURE DE VÉHICULER, À TRAVERS SES ÉCHANGES AVEC LES MÉDIAS, LA MEILLEURE IMAGE POSSIBLE DE SON EMPLOYEUR.

Missions

Un chargé de communication spécialisé en cybersécurité a plusieurs tâches à accomplir. Outre la rédaction des documents de communication (articles de blog, tribunes, posts sur les réseaux sociaux, communiqués de presse...), il doit :

· Préparer des rapports pour l'équipe de direction, y compris des recommandations pour assurer une attitude plus positive
· Rencontrer régulièrement les journalistes pour organiser des entretiens
· Maintenir les archives numériques des médias (photos, vidéos)
· Agir en tant que porte-parole de la marque
· Organiser des conférences de presse pour les annonces essentielles
· Travailler en étroite collaboration avec les responsables du marketing et des produits, les concepteurs et les responsables de sites Web pour recueillir des informations
· Surveiller les retours : il vérifie les parutions afin de s'assurer que le message est passé tel qu'il le souhaitait. Pour cela il effectue une revue de presse quotidienne et conserve tous les articles parus au sujet de son entreprise ou de son client. Il peut ainsi mesurer l'impact de sa communication et la modifier si cela est nécessaire

Un chargé de communication fait plusieurs choses à la fois. Il rédige et distribue du contenu et organise des conférences et des interviews pour promouvoir les produits, la marque ou les activités de son entreprise. Il agit donc

comme un agent de liaison entre la « cible » (grand public pour un éditeur d'antivirus par exemple ou professionnels pour des solutions dédiées), son organisation et les médias pour s'assurer que la communication est efficace.

Ces différentes responsabilités impliquent de connaitre parfaitement l'entité pour laquelle il travaille. Il doit donc organiser un plan de communication pour donner envie aux journalistes d'en parler. En créant une relation privilégiée avec les journalistes, il s'assure que son information est bien relayée auprès de la « cible ».

Compétences

L'une des principales compétences que doit posséder un chargé de communication est de communiquer efficacement. Il est donc aussi à l'aise à l'écrit qu'à l'oral. Pour cela, il doit avoir de bonnes compétences rédactionnelles et se montrer clair lorsqu'il s'exprime. Il emploie également un ton adapté à son entreprise ainsi qu'à son interlocuteur. Une bonne connaissance de l'anglais cyber est un « plus ».

Études

Le niveau Bac +2 est le minimum requis.

Quel diplôme ?

Différents diplômes Bac+5 permettent de disposer d'un bon profil :

· Master mention communication des organisations
· Master mention information, communication
· Manager de la communication (EFAP – Ecole Française des Attachés de Presse)

Quelle école ?

Différentes filières permettent de devenir chargé de communication. Vous pouvez viser un BTS communication, une licence professionnelle métiers de la communication (chargé de communication).

Salaire

Un débutant peut compter sur un salaire mensuel brut compris entre 2 200 à 2 900 euros tandis qu'après quelques années d'expérience, il peut gagner plus de 5 500 euros brut s'il travaille pour un grand compte spécialisé dans la cybersécurité, un éditeur de logiciel spécialisé dans ce domaine ou un grand cabinet de consultants.

Évolution de carrière

Il peut devenir chef du service de presse, directement rattaché au PDG ou dépendant de la direction commerciale ou des relations extérieures. Il peut aussi évoluer pour devenir responsable des attachés de presse.

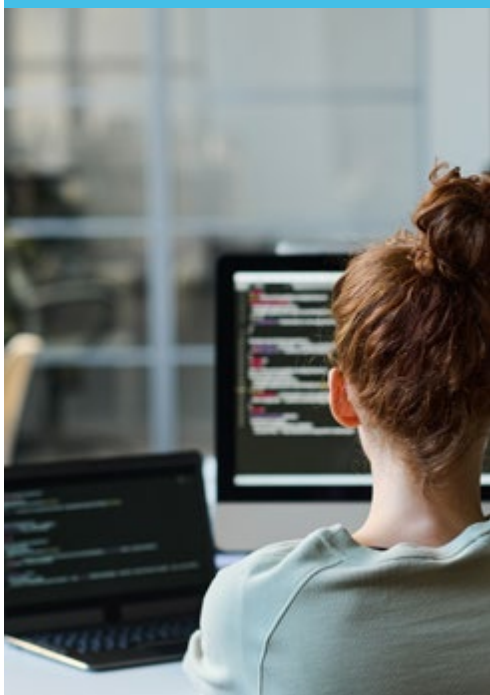
Comment le devenir ?

De plus en plus d'entreprises de ce secteur souhaitent communiquer sur leurs activités et produits. Il existe donc une forte demande pour ce type de profil. S'agissant d'un métier de communication, il est important de maitriser les différents outils (bureautiques, réseaux sociaux) permettant de mettre en valeur l'entreprise. Une bonne connaissance de l'anglais cyber et lié aux réglementations est fortement recommandée.

« POUR LES ENTREPRISES SPÉCIALISÉES DANS LA CYBERSÉCURITÉ, LA COMMUNICATION JOUE UN RÔLE IMPORTANT CAR IL S'AGIT DE VULGARISER DES MÉTHODES ET DES SOLUTIONS QUI SONT PARFOIS TRÈS TECHNIQUES. »

QUALITÉS

Avoir un bon relationnel et des capacités de persuasion sont très importants. L'attaché de presse doit créer une relation avec les journalistes. Il cible ceux qui seront les plus à même de parler de son employeur. Il doit se montrer disponible pour répondre à leurs demandes et véhiculer une bonne image.
C'est en créant une relation privilégiée avec ses interlocuteurs que ces derniers auront envie d'écrire. Il échange aussi beaucoup avec son employeur pour savoir quel produit/service ou quelles informations.
Enfin, il faut être curieux et s'intéresser aux médias et donc connaître leurs périodes de bouclage (à l'origine, processus juste avant l'impression d'un magazine papier. Aujourd'hui, il s'applique aussi aux sites Web) et leur ligne éditoriale.



Niveau d'études : Bac+5

Spé Conseillée : Scientifique

Employabilité : Très bonne

Salaire débutant : 3 250 €

Code ROME : M1802 - Code FAP : M2Z

VOUS ÊTES PRÊT À ASSURER UN TRAVAIL DÉFENSIF HAUTEMENT TECHNIQUE, SANS AVOIR PEUR DE LA RÉPÉTITION ET DE LA PRATIQUE INTENSIVE ? BIENVENUE DANS LE MONDE DE LA RED TEAM ! C'EST ICI QUE DE NOMBREUX PETITS GÉNIES INFORMATIQUES TROUVENT UN TERRAIN DE JEU QUI FAIT HONNEUR À LEURS CAPACITÉS. CES SOLDATS DE LA CYBERDÉFENSE PRENNENT EN CHARGE L'UNE DES PARTIES LES PLUS CONCRÈTES ET LES PLUS TECHNIQUES DE LA CYBERSÉCURITÉ. ILS CONSTITUENT DONC UN SOCLE ESSENTIEL DE LA GRANDE PYRAMIDE DES MÉTIERS CYBER, AUX CÔTÉS DE LA BLUE TEAM ET LA PURPLE TEAM. VOYONS ENSEMBLE LES SPÉCIFICITÉS DES MISSIONS QUI LEUR REVIENNENT.

Missions

Le red teamer est sollicité sur plusieurs tâches, toutes largement reliées à un travail de testing. Il s'agira notamment pour lui :

· De conduire des tests d'intrusion, sous la supervision directe du responsable d'équipe lorsque de nouvelles failles potentielles sont suspectées, et de manière relativement autonome lorsque ces tests entrent dans une routine de vérification, pour des points déjà testés
· D'effectuer des évaluations de violation supposées, impliquant généralement un implant pré-déployé et requérant la mobilisation de toute la red team
· D'examiner l'état d'évolution d'un certain nombre de malwares, notamment celle des ransomwares, le logiciel malveillant le plus couramment utilisé vis-à-vis des entreprises
· D'évaluer la sensibilité de la structure aux menaces des dernières formes de ransomwares repérées dans la sphère cyber
· De tenir un journal des menaces et des attaques les plus courantes et les plus dommageables
· De signaler les nouvelles formes de logiciels malveillants et d'en proposer une analyse rapide d'une part, plus détaillée d'autre part
· De conduire des évaluations d'ingénierie sociale

De manière plus rare, un membre de la red team peut être amené à évaluer des réseaux de différents types (externes ou internes, sans fil), mais aussi des applications web et mobiles. Plus

fréquemment, il assurera des revues de code source, ainsi que des revues d'architecture et de sécurité réseau.

Lorsqu'il travaille pour une entreprise en contact direct avec un nombre important de clients, il peut être demandé au red teamer de prendre part à l'interface qui permettra de gérer les préoccupations, les problèmes ou les escalades liés à la satisfaction client.

Travailler au sein d'une red team, c'est aussi :

· Développer des rapports et des présentations complets et précis pour les publics techniques et exécutifs
· Fournir une expérience de niveau expert pour la création de programmes de sécurité de l'information, afin d'embarquer toutes les parties prenantes – et les clients le cas échéant – dans les pratiques de cyberdéfense

Compétences

En raison de sa dimension hautement technique, les membres de la red team doivent être parfaitement à l'aise sur l'ensemble des sujets suivants :

· La sécurité des systèmes d'exploitation
· La sécurité des réseaux et protocoles
· Les couches applicatives
· Lensemble des méthodologies d'audit, en prenant bien en compte les normes, standards et principes de gouvernance en vigueur
· Toutes les techniques relatives aux audits techniques de sécurité et aux tests d'intrusion
· Les différents types de vulnérabilités pouvant être rencontrés sur les environnements les plus courants
· Les principes de reverse engineering ou rétro-ingénierie des systèmes
· Le panorama complet des techniques d'attaques et d'intrusion les plus courants, en prenant soin de le compléter au fur et à mesure par la connaissance des techniques nouvelles et récentes
· Les mécanismes du scripting

Les red teamers doivent aussi être armés de certaines notions de droit informatique, sur le point précis de la sécurité des systèmes d'information et de la protection des données. Il doit par ailleurs maîtriser l'exercice de veille technologique, afin de mettre à jour les derniers points d'attention en matière de cybersécurité et les tendances repérées dans les pratiques des hackers.

Certaines compétences formelles en gestion de projet peuvent être utiles, notamment lorsque le red teamer est désigné comme référent de l'équipe : ces compétences seront précieuses pour optimiser la conduite des tests et sécuriser plus rapidement les périmètres.

L'AVIS DE LA PROFESSIONNELLE

« En matière de cybersécurité, il y a ceux qui suspectent et ceux qui, concrètement, vont aller s'intéresser de près aux points de suspicion. Les membres de la red team font partie de la deuxième équipe : ils triturent le système, mettent les mains dans le cambouis pour vérifier les intuitions de ceux qui planifient et affinent la défense cyber. Nous sommes sur un métier pratique, en appui des métiers de réflexion stratégique. »

Rhadia M.
Red teameuse

QUALITÉS

Pour trouver sa place au sein d'une red team et en devenir un maillon fort, des qualités supérieures de concentration, de minutie et d'implication sont indispensables. Le red teamer doit avoir un sens de l'organisation particulièrement développé, afin de mener les bons tests dans le bon ordre, au bon rythme. Sa dextérité et sa vivacité d'esprit sont des atouts incontournables pour réagir sous des délais courts et faire en sorte que son action ait un sens : un test d'intrusion doit intervenir avant qu'une attaque ne réussisse. La curiosité et le goût pour la progression – et la mise à jour permanente des connaissances – font également partie du b.a.-ba du métier.

Études

Le Bac +5 est un minimum indispensable pour aborder les exigences du poste de red teamer. L'aspect technique du métier demande des études complètes dans le champ des technologies et de l'informatique, avec une préparation adéquate aux enjeux de la cybersécurité.

Salaire

La fourchette de salaires pour un membre de la red team se situe entre 3 250 et 5 450 euros mensuels brut, ces deux extrêmes correspondant à un profil débutant et à un profil senior. Ces chiffres concernent uniquement le territoire français. En moyenne, un red team justifiant de 3 ans d'expérience touchera environ 3 550 euros brut mensuels. L'ensemble de ces salaires peuvent être revus légèrement à la hausse si le professionnel a enrichi son parcours de passages dans une blue team, une purple team ou s'il a occupé d'autres fonctions stratégiques en lien avec les techniques d'intrusion.

Où travailler ?

Les red team sont particulièrement précieuses et valorisées dans les secteurs du consulting et de l'audit en général, de même que dans la banque, la finance et l'assurance. Les grands acteurs de l'industrie automobile et aéronautique s'appuient également sur elle pour défendre leurs intérêts stratégiques et tendent à renforcer de plus en plus leurs équipes. L'ensemble des entreprises spécialisées dans la haute technologie sont également de très bons recruteurs potentiels, sans oublier tous les fournisseurs de services numériques.

Parmi les entreprises et structures désireuses de renforcer leurs red teams, on voit régulièrement apparaître les noms :

- EY
- KPMG
- AXA
- HeadMind Partners
- SQUAD
- Airbus
- Atos
- Orange Cyberdefense

Évolution de carrière

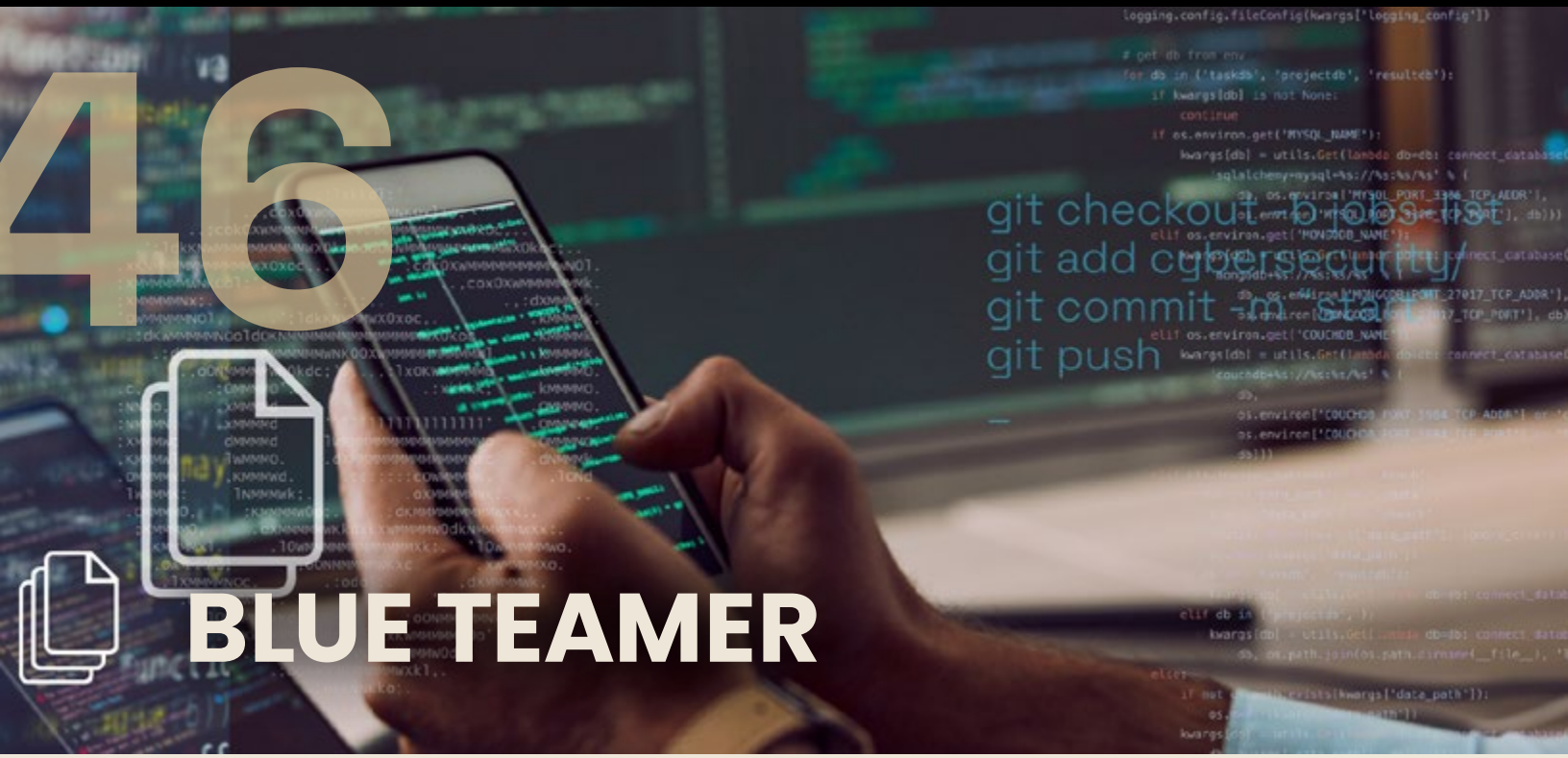
Les anciens red team font en général de très bons consultants en cybersécurité. Ils sont entourés, aux yeux des clients, d'une forte aura de légitimité, liée à leur confrontation quotidienne avec la partie la plus technique de la cyberdéfense. Pour réussir dans ces fonctions d'un autre genre, ils devront cependant s'assurer d'avoir intégré une compréhension transverse des enjeux cyber, pris dans la globalité.

Il est par ailleurs fréquent de voir un membre de la red team passer dans les rangs d'une blue team ou d'une purple team. La priorité, dans ce cas, est de varier son approche technique et sa spécialité.

Pour élargir ses champs de compétences, le red teamer peut aussi devenir auditeur de sécurité technique. À ce poste, il continuera à conduire, de manière ponctuelles, des audits de type red team.

Avantages et inconvénients

Pour Rhadia M., *« le travail en red team suppose de maintenir un niveau de concentration extrême, du moins très élevé, et un sens de la minutie poussé, sans jamais faire d'écart. C'est un travail de précision permanent et il faut tenir le rythme. Le piège serait de se laisser aller à la routine et de baisser le niveau de vigilance parce qu'on a répété et enchaîné les tests d'intrusion. Ce serait une aubaine pour les hackers, dont le premier facteur de réussite est d'ailleurs la défaillance humaine : une attaque réussit en général parce que le niveau d'attention ou de précaution d'une ou plusieurs personnes n'était pas assez fort. Notre défi premier, c'est donc de ne pas se laisser piéger par une fausse sensation de monotonie. Parce que les tests se réinventent, en réalité. Il y a toujours de nouveaux types d'attaques à devancer. Et c'est ça qui fait le sel du métier : se mettre perpétuellement à jour, découvrir de nouvelles technologies et les dompter, pour gagner une course de vitesse. Il y a assurément une bonne part d'adrénaline qui vient contrebalancer les risques de monotonie. C'est dans cet équilibre que l'on apprécie vraiment le métier. »* Cette professionnelle confirmée n'oublie pas de préciser que la couleur très technique du poste est une vraie source de valorisation et un atout à mettre en avant lorsque l'on souhaite se reconvertir.



Niveau d'études : Bac+5

Spé Conseillée : Scientifique

Employabilité : Très bonne

Salaire débutant : 3 050 €

Code ROME : M1802 - Code FAP : M2Z

VOUS AIMEZ LES COMPÉTITIONS ENTRE ÉQUIPES, CELLES QUI ONT POUR BUT DE REPOUSSER LES LIMITES DE CHACUN ET DE FAIRE PROGRESSER ? VOUS FAITES PARTIE DE CES PASSIONNÉS DE TECHNOLOGIE QUI CROIENT ENCORE À L'IMPORTANCE DU FACTEUR HUMAIN ET QUI SAVENT QUE NOTRE CERVEAU PEUT, À L'OCCASION, SE MONTRER PLUS PUISSANT OU PLUS DOMMAGEABLE QU'UNE MACHINE ? VOTRE APPROCHE EST PARFAITEMENT EN PHASE AVEC CELLE D'UN BLUE TEAMER. CES EXPERTS DE HAUT NIVEAU COMPLÈTENT L'ARSENAL PUREMENT TECHNIQUE DÉPLOYÉ PAR LES RED TEAMERS ET S'ASSURENT QUE LEURS SOLUTIONS NE PASSENT PAS À CÔTÉ D'UN DÉTAIL SIMPLE, MAIS POTENTIELLEMENT FATIDIQUE POUR LA SÉCURITÉ D'UNE ENTREPRISE OU D'UNE STRUCTURE PUBLIQUE. DÉCOUVREZ UN MÉTIER PASSIONNANT ET HAUTEMENT STIMULANT.

Missions

Il est impossible de penser le rôle d'une blue team en faisant l'impasse sur sa connexion et ses interactions directes avec la red team. Pour résumer les choses très simplement, les blue teamers apportent une intelligence d'abord humaine là où les red teamers déploient une intelligence avant tout technique. Le rôle de la blue team est de s'opposer et d'affaiblir la red team. En d'autres termes, l'équipe dite « bleue » est là pour mettre à mal les solutions techniques pensés par leurs challengers « rouges », avec un seul objectif en tête : s'assurer qu'en développant des défenses de haut niveau, atteignant une grande technicité, les petits détails les plus insignifiants n'ont pas été oubliés. Un degré de perfectionnement peut en effet faire perdre de vue les voies d'accès les plus évidentes, celles qu'un individu loin d'être un expert ou un ingénieur pourrait exploiter de manière simple. *« En résumé, dans la blue team, on s'assure que la red team n'a pas construit le château fort du siècle, avec porte blindée et pont levis actionné en un millième de seconde, tout en laissant sur le côté un trou de souris qui permettrait à n'importe quelle personne un peu fine - d'esprit - de passer »*, résume très bien Alessio D., qui est déjà passé plusieurs fois de la blue team à la red team au cours de ses 6 ans de carrière.

« Le travail premier de la blue team, c'est concevoir des scénarios d'attaque pour améliorer les compétences globales et de la blue team, et de la red team - et la sécurité de notre équipe commune, à savoir l'entreprise ou l'organisation publique qui nous recrute. »

Les membres de la blue team, soutenue

« AU MÊME TITRE QUE LEURS HOMOLOGUES DE LA RED TEAM, LES BLUE TEAMERS INTERVIENNENT EN TANT QUE TESTEURS DE FAILLES DE CYBERSÉCURITÉ ET AUDITEURS DE PROBLÈMES TECHNIQUES. ON PARLE SOUVENT DE LA BLUE TEAM COMME ÉTANT LE « PERSONNEL DE LA CYBERSÉCURITÉ », EN RAISON DE LA NATURE PLUS « HUMAINE » DE LEUR INTERVENTION, LÉGÈREMENT DÉCONNECTÉE DES PURS OUTILS TECHNIQUES. »

par le SOC, sont finalement là pour décortiquer et passer au crible d'attaques « plus terre à terre » les trésors de technologie déployés par la red team.

Compétences

Bien que leur rôle ne consiste pas à mobiliser directement les compétences techniques au cœur de l'activité de la red team, les blue teamers se doivent - en tant que challengers et testeurs des red teamers - d'être parfaitement formés sur les sujets de prédilection de leurs « collègues-concurrents ». Aussi, ils doivent avoir une bonne compréhension et une bonne approche de l'ensemble des sujets suivants :

· La sécurité des systèmes d'exploitation
· La sécurité des réseaux et protocoles
· Les couches applicatives
· L'ensemble des méthodologies d'audit, en prenant bien en compte les normes, standards et principes de gouvernance en vigueur
· Toutes les techniques relatives aux audits techniques de sécurité et aux tests d'intrusion
· Les différents types de vulnérabilités pouvant être rencontrés sur les environnements les plus courants
· Les principes de reverse engineering ou rétro-ingénierie des systèmes
· Le panorama complet des techniques d'attaques et d'intrusion les plus courants, en prenant soin de le compléter au fur et à mesure par la connaissance des techniques nouvelles et récentes
· Les mécanismes du scripting

Des notions de droit informatique seront également précieuses, sur le point précis de la sécurité des systèmes d'information et de la protection des données. Les blue teamers doivent aussi être en mesure de mener un travail de veille technologique de manière efficace, afin de connaître les dernières pratiques en vogue chez les hackers et de ne manquer aucune faille possible dans les défenses pensées par la red team.

Les compétences en gestion de projet peuvent également être utiles, notamment pour le blue teamer nommé référent d'une équipe.

Études

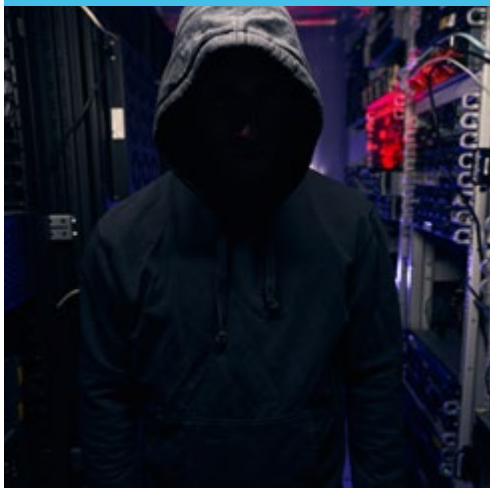
Le Bac +5 est une condition préalable pour intégrer une blue team. Le poste requiert un certain nombre de compétences techniques de haut niveau, ainsi qu'une compréhension globale des enjeux de cybersécurité.

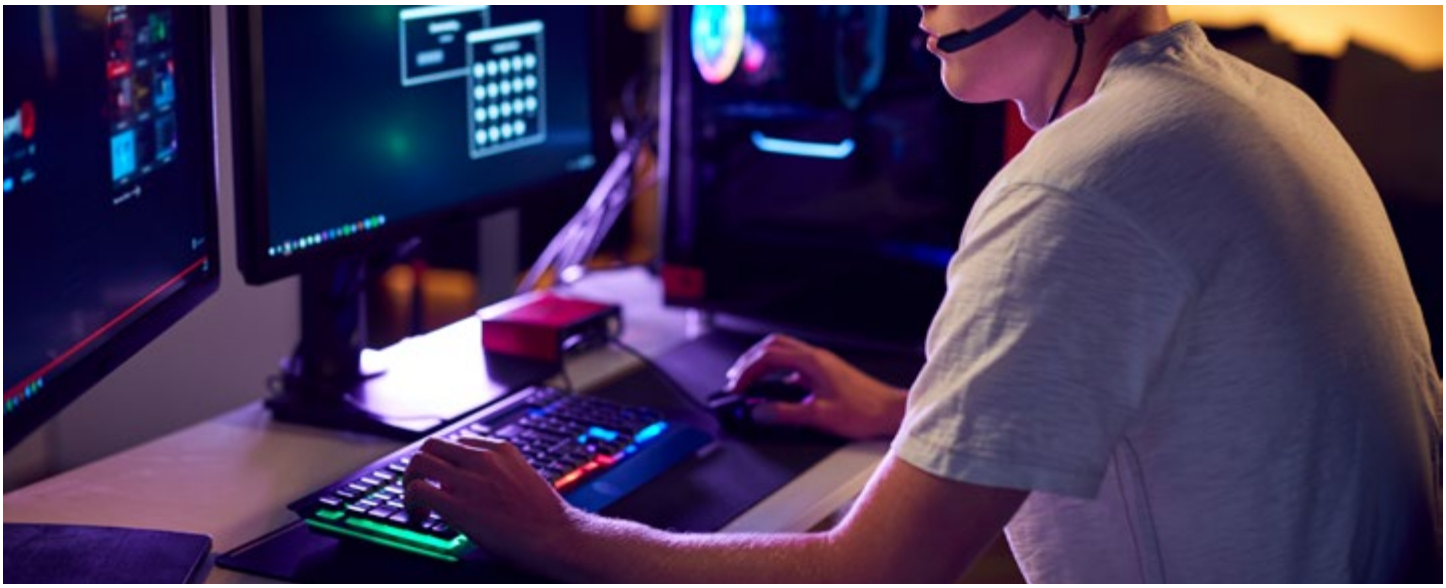
Salaire

Pour un premier poste, un blue teamer peut viser un salaire brut mensuel aux alentours de 3 050 euros. Ce salaire peut atteindre jusqu'à 3 550 euros si l'individu en question a occupé un autre poste significatif en lien avec les tests de cyberdéfense, au sein du SOC ou avec une red team, par exemple. Un Bue teamer confirmé peut espérer gagner jusqu'à 5 150 euros brut par mois environ. À nouveau, les expériences complémentaires en cybersécurité – sur des postes très techniques ou des missions plus traverses – donneront certainement lieu à un ajustement de salaire à la hausse.

QUALITÉS

Les deux mots d'ordre aux sons desquels vibre toute team sont : proactif, réactif. Un bon blue teamer doit par conséquent redoubler d'énergie et d'inventivité pour partir à l'assaut des systèmes de défense mis en place par leurs collègues de la red team. Cela demande à la fois de la rigueur et de la créativité pour mener des tests de manière efficace mais aussi inattendue. La fonction requiert une grande capacité de concentration, un bon équilibre entre initiative personnelle et goût du travail en équipe, ainsi qu'un goût prononcé pour le jeu : travailler pour la blue team revient ni plus ni moins à s'engager dans une lutte inoffensive contre la red team, pour le bien de l'organisation !





Où travailler ?

Les blue teamers ont un rôle actif à jouer partout où les red teamers se trouvent eux aussi impliqués. Le recrutement de ces spécialistes complémentaires est particulièrement fréquent dans les secteurs du consulting et de l'audit en général, de même que dans la banque, la finance et l'assurance. Les grands acteurs de l'industrie automobile et aéronautique ne sont pas en reste, de même que les entreprises spécialisées dans la haute technologie, les fournisseurs de services numériques et les services traitant des données de santé.

Parmi les entreprises fréquemment à la recherche de blue teamers, on trouve notamment :

- EY
- KPMG
- AXA
- HeadMind Partners
- SQUAD
- Airbus
- Atos
- Orange Cyberdefense
- Thales

Évolution de carrière

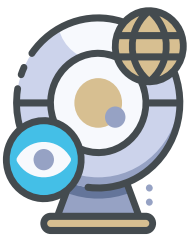
Le membre d'une blue team qui a envie de changer d'horizon peut assez facilement demander à passer du côté rouge des forces de cyberdéfense. Il sera au préalable soumis à des formations et à un accompagnement de mise à jour, pour se défaire de certains réflexes d'analyse et adapter la bonne approche. Ce changement correspond, en général, à une légère augmentation de salaire, valorisant des compétences plus techniques.

Les blue teamers peuvent aussi envisager de se reconvertir en consultants en cybersécurité. Leur travail au sein du SOC en fait des experts confirmés. Une mise à jour sur certains techniques est, une fois encore, une condition préalable à ce type d'évolution.

Un blue teamer bénéficiant de dix années au moins d'expérience ont également la légitimité suffisante pour progresser au sein du SOC : après être passé sur un poste plus général d'analyste opérateur du SOC, il est possible de briguer le poste le plus convoité, à savoir responsable du SOC.

Avantages et inconvénients

« Lorsqu'on a été formé pour être un petit as de la technique, il peut être un peu compliqué d'oublier ses réflexes et ses acquis lorsqu'on rejoint une blue team. On peut avoir envie, plus ou moins consciemment, de montrer ce que l'on sait et ce que l'on sait faire : il peut y avoir une tendance à basculer dans un rôle de red teamer, sans s'en rendre compte. À chaque membre de prendre garde à bien maintenir son cap et à ne pas déborder du rôle qui est le sien. Cela peut générer des frustrations à l'occasion, mais il faut se rappeler que chercher la faille simple n'est pas – et c'est là toute l'ironie – un exercice facile. Le rôle de blue teamer prend dès lors une dimension très ludique et très valorisante à la fois », reconnaît Alessio D. *« L'un des avantages flagrants est que passer d'une blue team à une red team est relativement aisé. Si la monotonie ou l'ennui s'installe, on peut assez facilement envisager de changer d'équipe et d'horizon, avec pas mal de perfectionnements à la clé – pour l'entreprise et sa sécurité d'une part, pour l'employé et ses compétences d'autre part. »*



Niveau d'études : Bac+5

Spé Conseillée : Scientifique

Employabilité : Très bonne

Salaire débutant : 3 050 €

Code ROME : M1802 - Code FAP : M2Z

LORSQU'IL S'AGIT DE PASSER AU CRIBLE DES SYSTÈMES ET DES ENVIRONNEMENTS COMPLEXES, DANS LE BUT DE REPÉRER LE DÉFAUT LE PLUS INFIME, VOUS ÊTES UN VÉRITABLE ŒIL DE LYNX ? VOUS ÊTES DOTÉ D'UN GRAND SENS DE L'AUTONOMIE ET D'UNE BELLE CAPACITÉ D'INITIATIVE, ET POURTANT C'EST EN ÉQUIPE QUE VOUS VOUS ÉPANOUISSEZ VRAIMENT ? VOUS SEMBLEZ ÊTRE TRÈS BIEN PARTI POUR ÊTRE UN ÉLÉMENT EN OR AU SEIN D'UNE PURPLE TEAM ! CETTE CELLULE CLÉ DES ACTIONS DE CYBERSÉCURITÉ, INDISPENSABLE POUR TOUTES LES STRUCTURES DONT LA TAILLE OU LES ACTIVITÉS SONT LOIN D'ÊTRE NÉGLIGEABLES, EST AUX COMMANDES DES AUDITS TECHNIQUES LES PLUS DÉTERMINANTS LORSQU'IL EST QUESTION DE CYBERDÉFENSE. DÉCOUVREZ AVEC NOUS CE MÉTIER AU CŒUR DE LA MACHINE DÉFENSIVE.

Missions

En tant qu'unité globale réunissant blue team et red team, la purple team réunit les missions qui leur sont propres. Ainsi, elle embrasse toutes les activités suivantes :

· Conduire des tests d'intrusion
· Examiner l'état d'évolution des malwares les plus répandus d'une part, et des nouvelles formes de logiciels malveillants d'autre part
· Évaluer les cas d'autres structures ayant subi des attaques employant des techniques encore peu connues, afin d'adapter les défenses de la structure pour laquelle opère la purple team
· Tenir un journal des menaces et des attaques les plus courantes et les plus dommageables
· Conduire des évaluations d'ingénierie sociale
· Concevoir des scénarios d'attaque mettant à mal les toutes dernières défenses mises en place dans la structure elle-même, afin d'évaluer l'efficacité de ces défenses et de les améliorer si besoin
· Proposer des rapports d'analyse complets, abordant les manipulations techniques et humaines employées pour renforcer la cyberdéfense de la structure, et résumant à la fois le travail de la red team et de la blue team

« Pour expliquer le sens qu'a la purple team, j'aime utiliser la comparaison avec le jeu vidéo en mode collaboratif : on est plusieurs sur le même terrain, et même si l'on se met des bâtons dans les roues de temps à autre, c'est un exercice tout à fait conscient puisque nous allons tous

dans le même sens », explique Solène R., référente d'une purple team pour une grande référence du conseil en haute technologie.

« La responsabilité de la purple team, c'est de faire en sorte que tous les trésors d'ingéniosité techniques et humains qui ont été mis en œuvre trouvent une vraie utilité finale : c'est tirer les meilleures conclusions de ce travail par à-coups. Transformer, du point de vue officiel, le travail de deux équipes 'fictivement" opposées en travail d'équipe à proprement parler, tout simplement ! »

Compétences

La purple team agrège l'ensemble des compétences clés de la red team et blue team. Considérés dans leur ensemble, les purple teamers peuvent donc être sollicités à intervenir sur les sujets suivants :

· La sécurité des systèmes d'exploitation
· La sécurité des réseaux et protocoles
· Les couches applicatives
· L'ensemble des méthodologies d'audit, en prenant bien en compte les normes, standards et principes de gouvernance en vigueur
· Toutes les techniques relatives aux audits techniques de sécurité et aux tests d'intrusion
· Les différents types de vulnérabilités pouvant être rencontrés sur les environnements les plus courants
· Les principes de reverse engineering ou rétro-ingénierie des systèmes
· Le panorama complet des techniques d'attaques et d'intrusion les plus courants, en prenant soin de le compléter au fur et à mesure par la connaissance des techniques nouvelles et récentes
· Les mécanismes du scripting

La purple team s'appuie aussi sur quelques notions en droit informatique, indispensables pour gérer la situation en cas d'attaque de hackers réussie.

Ces professionnels doivent par ailleurs être à l'aise avec la mission de veille technologique et la gestion de projet. Cette dernière aptitude sera notamment précieuse pour des référents

Études

Le pass d'entrée minimal pour rejoindre une purple team est un Bac +5. Les formations proposant une base technique solide, sans oublier des compétences formelles en gestion de projet, sont vivement conseillées. Ce métier suppose en effet une formation de haut niveau abordant à la fois les points de détails de la sécurité informatique et les enjeux plus globaux de la cybersécurité.

« POUR COMPRENDRE LE RÔLE ATTRIBUÉ À LA PURPLE TEAM, IL SUFFIT D'AVOIR LES IDÉES CLAIRES SUR LA PALETTE DES COULEURS ! POURQUOI ? PARCE QUE L'ÉQUIPE DITE "VIOLETTE" N'EST RIEN D'AUTRE QUE LA RÉUNION DES RED TEAM ET BLUE TEAM : LA RENCONTRE DU ROUGE ET DU BLEU, C'EST-À-DIRE DE L'APPROCHE TECHNIQUE ET DE L'APPROCHE HUMAINE DES AUDITS DE SÉCURITÉ. »

QUALITÉS

De manière presque ironique, c'est le sens du travail en équipe qui constitue la qualité première nécessaire pour opérer dans une purple team : malgré le jeu d'opposition soutenu que doivent mener certains auditeurs et spécialistes contre d'autres, c'est un double objectif de cohésion et de projection qui est recherché.
Une curiosité prononcé et un grand sens de l'initiative seront indispensables pour faire progresser l'arsenal de défense et créer l'émulation au sein des différentes parties de l'équipe. Dans le même ordre d'idée, on compte sur une grande réactivité et une vivacité d'esprit évidente pour réaliser les mises à jour nécessaires à temps.

Salaire

La fourchette de salaire est compris entre 3 050 euros brut mensuels en début de carrière et 5 450 euros brut par mois pour un profil confirmé. En règle général, ce sont les professionnels affectés à la blue team qui se voient attribuer les salaires les plus bas, avec un salaire plafonnant à 5 150 euros en fin de carrière. En raison de leur plus forte implication sur des points techniques, les red teamers, eux, peuvent espérer commencer leur carrière en touchant 3 250 euros brut par mois environ. Le salaire de fin de carrière de 5 450 euros correspond, de fait, à leur cas de figure. Il s'agit de moyennes pouvant évoluer en fonction des expériences et aptitudes techniques de chacun. Les personnes navigant régulièrement entre l'une ou l'autre équipe voient en général leur rétribution majorée, de manière à valoriser leur double approche des problèmes.

Où travailler ?

Un grand nombre de grandes entreprises décide de mettre en place une purple team : c'est une sécurité précieuse – pour ne pas dire indispensable – pour empêcher un détournement de leurs données. Aussi, les purple teamers en devenir peuvent s'intéresser de près aux domaines de la finance, de la banque et de l'assurance. Les cabinets d'audit et de consulting sont également de bons recruteurs, notamment lorsqu'ils sont spécialisés dans les sujets numériques ou la haute technologie. Les grandes références du domaine industriel ont elles aussi des offres récurrentes, notamment du côté de la construction automobile, de l'aéronautique et des hautes technologies en général.

Attention : intégrer une purple team veut souvent dire intégrer une blue team ou une red team : c'est donc en filtrant les annonces avec ces mots clés que l'on pourra repérer facilement des opportunités !

Parmi les grands recruteurs de purple teamers, on relève fréquemment les noms de :

- Atos
- Airbus
- EY
- KPMG
- AXA
- HeadMind Partners
- SQUAD
- Orange Cyberdefense
- Thales

Évolution de carrière

La voie la plus naturelle pour un membre de la purple team souhaitant évoluer est de passer à un poste différent au sein du SOC, avec lequel il collabore déjà étroitement. Au-delà d'un changement relativement neutre, pour devenir analyste opérateur du SOC, les purple teamers les plus aguerris peuvent viser un poste de responsable du SOC. Selon les profils, cette évolution peut être réalisée après 5 à 10 ans de carrière de terrain, au sein de la blue ou red team.

Avantages et inconvénients

Solène R. voit le travail au sein d'une purple team *« comme un petit exercice de schizophrénie - et il s'agit d'un exercice qui n'est pas toujours évident. »* Pour elle, *« devoir retenir ses réflexes techniques, lorsque l'on est du côté de la blue team, ou passer régulièrement de l'expert technique de la red team au stratégiste plus terre à terre de la blue team peut être légèrement déroutant. Mais c'est aussi et surtout un très bon exercice intellectuel, qui nous permet d'échapper à la sensation d'ennui et qui nous invite à nous renouveler sans cesse. Sans cela, nous deviendrons rapidement aveuglés par nos automatismes et nos tests d'intrusion ne seraient plus aussi pertinents ».* Parmi les grands avantages, Solène R. souligne un aspect extrêmement valorisant, lié aux capacités techniques de haut vol qui sont souvent mobilisées et au rôle central que joue cette équipe « violette » dans le maintien de cyberdéfenses efficaces.

« ENVISAGER LES CHOSES SOUS L'ANGLE DE LA PURPLE TEAM, C'EST CONSIDÉRER LE TRAVAIL COMPLÉMENTAIRE DES BLUE TEAMERS ET DES RED TEAMERS À LA FOIS. »

48 CHERCHEUR·EUSE EN SÉCURITÉ DES SYSTÈMES D'INFORMATION

Niveau d'études : Bac+5

Spé Conseillée : Scientifique

Employabilité : Bonne

Salaire débutant : 4 000 €

Code ROME : M1802 - Code FAP : M2Z

LA CYBERSÉCURITÉ EST DEVENUE UN ENJEU MAJEUR POUR LES ENTREPRISES, MAIS POUR AUSSI LES INDUSTRIELS QUI DÉVELOPPENT DES MACHINES CONNECTÉES. AUJOURD'HUI, TOUS LES RÉSEAUX INFORMATIQUES SONT HYPER CONNECTÉS. L'EXPLOITATION D'UNE FAILLE DE SÉCURITÉ PAR DES PIRATES PEUT ENTRAINER LA PARALYSIE D'UNE CHAINE DE PRODUCTION OU LE VOL DE DONNÉES SENSIBLES. C'EST L'OBJECTIF DE CETTE PRATIQUE CONSISTANT À PROTÉGER LES SYSTÈMES CRITIQUES ET LES INFORMATIONS SENSIBLES CONTRE LES ATTAQUES NUMÉRIQUES. ET LE SYSTÈME D'INFORMATION (SI) EST LA PIERRE ANGULAIRE DE TOUTE ACTIVITÉ.

Missions

Ses missions sont très larges. Elles varient selon ses spécialités et son employeur : une multinationale, un éditeur de logiciels, un fabricant d'automates industriels, une organisation gouvernementale comme l'ANSSI qui est l'autorité nationale en matière de sécurité et de défense des systèmes d'information en France…

Il peut assurer, superviser ou déléguer l'exécution ou la restitution des travaux scientifiques, mener des activités d'enseignement et d'encadrement d'autres chercheurs ou étudiants/stagiaires. Il peut également participer au développement de produits, de procédés ou de services innovants.

De façon générale, ses principales missions consistent à :

· Établir un plan de test pour les cibles faisant l'objet d'une évaluation de sécurité
· Découvrir des vulnérabilités ou des faiblesses dans des sites web ou des produits
· Rédiger des exploits de preuve de concept (Proof of concept-POC) pour les vulnérabilités
· Travailler avec l'équipe de développement (s'il intègre un éditeur de logiciels par exemple) pour corriger les vulnérabilités découvertes
· Analyser/enquêter sur les nouvelles attaques…
· Proposer de nouvelles approches, de nouvelles méthodes de détection et/ou de défense

« LE CHERCHEUR EN SÉCURITÉ DES SYSTÈMES D'INFORMATION DOIT SE METTRE DANS LA PEAU DES CYBERATTAQUANTS. PAR QUELLE « PORTE » POURRAIENT-ILS S'ENGOUFFRER POUR RÉCUPÉRER DES DONNÉES CRITIQUES DANS UN SYSTÈME D'INFORMATION (SI) ? QUELS LOGICIELS PRÉSENTENT PLUS DE FAILLES DE SÉCURITÉ QUE LES AUTRES ? COMMENT METTRE EN PLACE DES PARADES EFFICACES ? »

· Documenter les travaux réalisés et participer à la valorisation et au transfert des résultats obtenus
· Assurer une veille scientifique et technologique en suivant les publications de l'industrie de la sécurité, les groupes de discussion et autres sources en ligne pour connaître et comprendre les vulnérabilités de sécurité récemment découvertes et les menaces émergentes
· Anticiper les problématiques opérationnelles et les défis à venir dans son domaine, etc.

Une partie importante de son travail consiste à étudier les failles de sécurité, appelées aussi vulnérabilités. Il va donc analyser les vulnérabilités des logiciels et des services afin de déterminer leur cause profonde, leur gravité et leur impact sur la sécurité du système d'information et les données qu'il traite. Les cybercriminels ayant beaucoup d'imagination, il doit aussi identifier les variantes des vulnérabilités, développer des outils et concevoir de nouvelles approches pour automatiser la découverte et l'analyse des vulnérabilités.

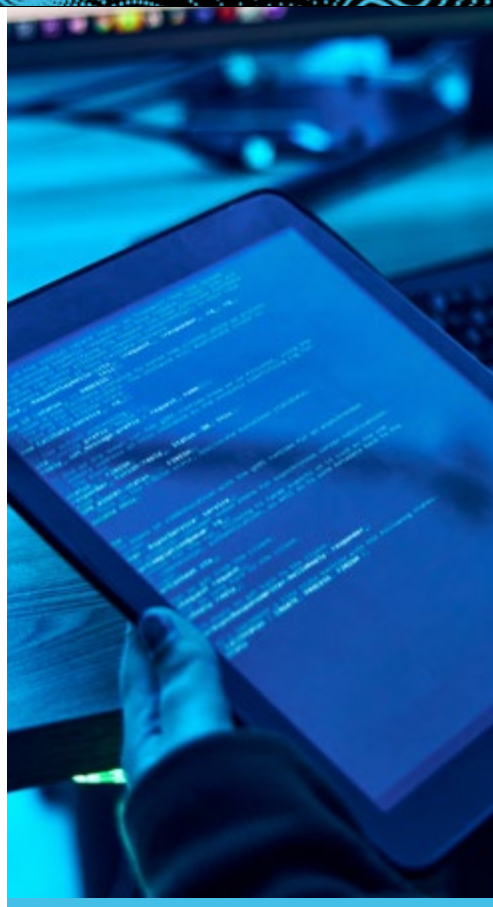
Les chercheurs en sécurité passent un temps considérable à examiner le code source et les logiciels malveillants et à étudier les rapports d'incidents pour mieux comprendre les menaces. Les logiciels malveillants peuvent représenter un défi difficile à relever. Il faut de la patience et de solides compétences analytiques pour « démonter » les logiciels malveillants, en faire l'ingénierie inverse (ou reverse engineering) pour savoir comment ils fonctionnent et concevoir des mesures d'atténuation.

Le travail d'un chercheur en sécurité n'a presque pas de limites, car la variété, la profondeur et l'ampleur des variantes de logiciels malveillants sont elles aussi sans limites. C'est la raison pour laquelle ces chercheurs en sécurité doivent avoir une stratégie pour concentrer leurs efforts sur les domaines les plus susceptibles d'apporter des avantages à leur employeur.

Pour être polyvalents et aborder la cybersécurité sur différents fronts, les chercheurs en sécurité passent beaucoup de temps sur des « machines virtuelles ». Schématiquement, il s'agit d'un ordinateur fonctionnant avec une version particulière d'un système d'exploitation (le plus connu étant Windows) installé sur un autre ordinateur. Par exemple, sur un ordinateur fonctionnant sous Windows 11, ce chercheur peut avoir plusieurs PC « installés », mais fonctionnant sous Windows 10 ou 8 ou sous une distribution Linux comme Opensuse.

Cette capacité à faire tourner différents systèmes d'exploitation (ou operating system) sur un ordinateur permet de tester des codes malveillants ou des techniques d'attaque tout en limitant les risques d'infection au PC virtuel. C'est ce qu'on appelle la virtualisation, un processus de création d'une version logicielle ou « virtuelle » d'un ordinateur, avec des quantités dédiées d'UC, de mémoires et de stockage « empruntées » à un ordinateur hôte physique, tel que votre ordinateur.

Le fait de disposer de ces différents environnements pour faire des expériences est très utile pour observer le comportement des logiciels malveillants.



QUALITÉS

Il faut être autonome et surtout motivé, car le travail de recherche peut être vite épuisant. Des aptitudes avérées à l'analyse et à la résolution de problèmes, ainsi qu'à la réflexion hors des sentiers battus sont des qualités indispensables pour devenir un excellent chercheur en sécurité.

Compétences

Maîtriser le socle scientifique et technique propre à l'informatique en général et à la cybersécurité en particulier est évidemment la première des compétences à avoir. Dans le détail, il est essentiel de bien comprendre les processus et les cycles de vie du développement logiciel et de noyaux sur Linux / Windows / iOS / Android. Il est difficile de maîtriser tous ces systèmes d'exploitation, mais en fonction des priorités de son employeur, il sera nécessaire de renforcer ses connaissances sur tel ou tel OS et sur certains langages de programmation (Java, JavaScript et/ou Python…).

Une compréhension des protocoles de réseau (TCP/IP, DNS, HTTP, etc.) est également indispensable. Une bonne expérience des tests de pénétration (ou pentest en anglais) d'applications Web et de l'analyse des attaques à l'aide d'outils (Burp Suite, Fiddler, Metasploit, etc.) est recommandée.

Études

Le minimum est un Bac +5, mais il est possible aussi d'avoir un doctorat. Dans certains cas, il est nécessaire d'obtenir une habilitation à diriger des recherches.

La voie royale est celle d'une école d'ingénieurs en cybersécurité qui propose de nombreux cours pratiques sur la sécurité informatique offensive.

Salaire

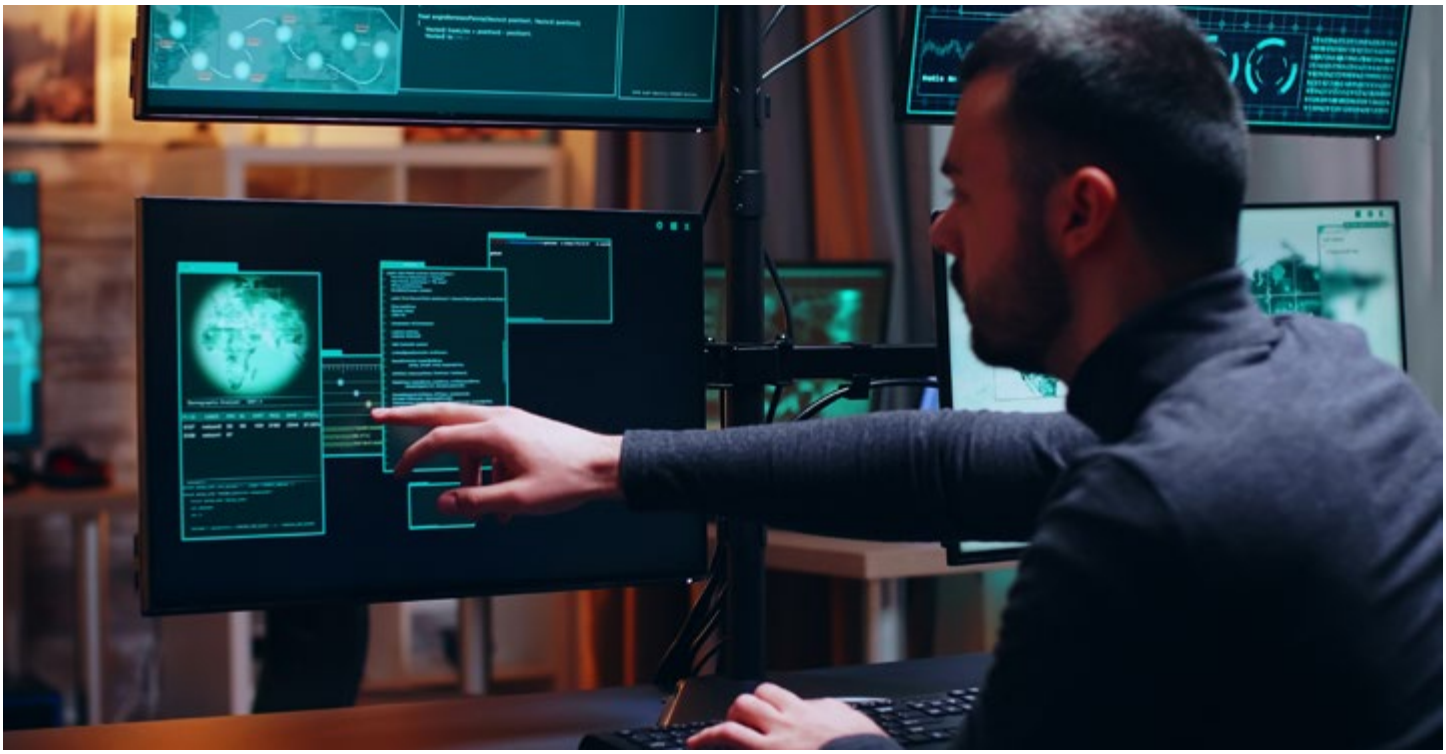
Il est très variable en fonction de ses missions et du type d'employeur. Un important éditeur de logiciels informatiques ou une grosse entreprise spécialisée dans la cybersécurité offrira des rémunérations plus élevées qu'une agence officielle. Une chercheuse débutante peut espérer les 40 000 à 48 000 euros brut par an, tandis qu'une senior peut prétendre à 120 000 euros brut par an, voire plus en fonction de ses années d'expérience et de ses spécialités.

Évolution de carrière

La chercheuse en sécurité des SI peut appartenir à une équipe de recherche et développement (R&D). Dans le domaine de la recherche publique, il peut collaborer avec une équipe de recherche dont les axes de travail ne sont pas strictement dédiés à la sécurité. Cette multidisciplinarité est souvent nécessaire pour appréhender la complexité du domaine.

Comment le devenir ?

Les chercheurs les plus connus sont régulièrement invités dans des conférences internationales dédiées au hacking. Elles leur permettent de présenter leurs derniers travaux de recherche. Mais avant d'arriver à ce statut, les débutants devront passer des années à améliorer leurs connaissances sur des points particuliers. Pour ceux et celles qui ont un esprit scientifique, c'est une voie idéale pour découvrir et expérimenter des codes malveillants et des techniques d'attaques.



Niveau d'études : Bac+5

Spé Conseillée : Scientifique

Employabilité : Bonne

Salaire débutant : 3 300 €

Code ROME : M1802 - Code FAP : M2Z

TOUS LES LOGICIELS PRÉSENTENT DES FAILLES DE SÉCURITÉ. IL EST DONC ESSENTIEL DE LES TROUVER LE PLUS RAPIDEMENT POSSIBLE AVANT QUE DES CYBERMALVEILLANTS NE PROFITENT D'UNE BRÈCHE POUR RÉCUPÉRER DES DONNÉES. CETTE COURSE DE VITESSE AUX BUGS ATTIRE DE PLUS EN PLUS DE « CHASSEURS DE PRIMES », CAR LES ENTREPRISES ET DES PLATEFORMES ONT MIS EN PLACE DES BUGS BOUNTY AUX RÉCOMPENSES ATTRACTIVES. SI AUCUN DIPLÔME N'EST REQUIS, IL EST INDISPENSABLE D'ÊTRE RIGOUREUX ET COMPÉTENT.

Missions

Il a deux tâches principales :

· Trouver des bogues et des failles de sécurité
· Signaler ces bogues et ces failles de sécurité de manière responsable.

Lorsqu'un pirate découvre une faille dans un système, il signale sa découverte par courrier électronique. Un responsable du programme de bug bounty examine toutes les découvertes signalées et décide de récompenser ou non la personne responsable

Une fois la décision prise, le responsable du programme de primes aux bugs envoie un chèque au chercheur et des instructions sur la manière de réclamer la récompense. Les chasseurs de bug bounty qui réussissent doivent également suivre des directives strictes lorsqu'ils signalent des failles. Ils doivent notamment préserver la confidentialité des informations personnelles, n'utiliser qu'un seul ordinateur à la fois et ne jamais divulguer de données sensibles sans autorisation.

Dans le cadre des programmes de bug bounty, les chercheurs en sécurité et les hackers sont invités à examiner en toute légalité diverses applications, plateformes et services dans un cadre donné. Si une vulnérabilité est découverte et que son impact entre dans le cadre du programme, les chercheurs doivent soumettre un rapport de bogue par les canaux appropriés. Une fois que l'entreprise aura vérifié la menace et son impact, les chercheurs seront payés dans les délais impartis.

Dans le cadre des programmes de primes aux bugs, chaque projet spécifie les actifs que l'entreprise souhaite examiner, les liens pertinents et les instructions de partage pour se connecter, le cas échéant. Plus importants encore, les programmes de primes de bogues indiqueront clairement les zones du produit qui ne doivent pas faire l'objet d'une enquête, et la mener sur ces actifs est illégale.

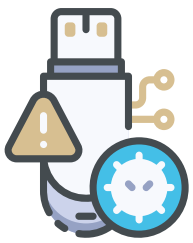
Les entreprises indiquent également la fourchette des paiements pour les bogues valides et, le cas échéant, les paiements moyens pour les primes précédentes. Elles peuvent également inclure d'autres récompenses, comme la reconnaissance, pour les experts qui cherchent à construire leur réputation.

Les petites et moyennes entreprises n'ont pas les moyens de mettre en place leur propre programme de bug bounty. Elles se tournent donc vers des plates-formes qui se chargeront du recrutement, de la vérification et de la gestion des chercheurs ainsi que de l'analyse des bogues découverts et de la gestion des paiements.

Des entreprises de plus grande taille préfèrent mettre en œuvre de tels programmes en continu, de sorte que chaque fois qu'un chercheur trouve un bug, il est payé s'il s'agit d'une faille qui mérite d'être rémunérée. D'autres programmes sont mis en œuvre pour des périodes limitées et, dans ce délai, les chercheurs disposent d'une marge de manœuvre pour explorer les failles.

Compétences

Les bugs bounty hunter connaissent les principes fondamentaux de la cybersécurité, mais ils doivent surtout acquérir des connaissances approfondies et se perfectionner dans de nombreux domaines tels que le réseau, le codage, la sécurité, le cloud et la façon dont tout fonctionne ensemble.



Mais ces compétences ne sont pas suffisantes ! Cela peut surprendre, mais de solides compétences en communication sont indispensables, car l'objectif de ce type de programme est de permettre à une entreprise de comprenne le risque et d'être capable de le résoudre.

Études

Le niveau Bac +2 est le minimum requis.

La meilleure école est celle de la vie ! Avoir un esprit d'attaquant et être méthodique valent toutes les écoles. Mais suivre un cursus d'ingénieur en cybersécurité permet d'acquérir de solides expériences et une méthodologie.

Salaire

Ne rêvez pas ! Être chasseur de bogues n'est pas un moyen de s'enrichir rapidement. La plupart des hackers gagnent moins de 20 000 dollars par an, mais au moins sept d'entre eux ont gagné plus d'un million de dollars et un hacker éthique roumain du nom de Cosmin Lordache, ou @inhibitor181, a gagné plus de 2 millions de dollars grâce à HackerOne.

Comment le devenir ?

C'est à la fois, une activité passionnante, car vous passerez des jours à décortiquer une application à la recherche d'une vulnérabilité très critique qui vous fera connaître de la communauté des hackers. Cette découverte vous permettra aussi de remporter une prime élevée. Mais il y a aussi le revers de la médaille. Passer tout son temps sur un logiciel peut devenir frustrant à la longue. Mais si cette perspective ne vous décourage pas, foncez ! De nombreuses entreprises et plateformes ont mis en place des programmes de bug bounty. Et n'oubliez pas cette citation du patron de Twitter, Elon Musk : *« J'ai commencé SpaceX avec l'espoir d'un échec »*.

QUALITÉS

Vous devez avoir l'esprit d'un hacker, ce qui signifie être curieux de savoir comment la technologie fonctionne, pourquoi le bug existe et comment l'exploiter. Ensuite, apprenez-en le plus possible. De cette façon, vous ne vous contenterez pas d'exploiter les bugs, mais vous développerez également des méthodologies sur la façon de les rechercher. D'autres qualités permettent de faire la différence et d'être plus efficace :
Soyez patient : si vous n'aimez pas rester assis toute la journée, la chasse aux bugs n'est probablement pas faite pour vous. En revanche, si vous aimez passer des heures et des heures à essayer de trouver des vulnérabilités dans divers sites, applications ou logiciels, cette activité vous conviendra parfaitement. La patience est l'une des choses les plus difficiles à surmonter, car vous ne serez pas payé tant que vous n'aurez pas trouvé de bug… Même les hackers talentueux peuvent chasser pendant des jours, voire des semaines, sans trouver un seul bug. Imaginez à quel point cela peut être frustrant ! N'oubliez pas de tout documenter : une fois que vous avez identifié une faille, faites des captures d'écran du site web affecté ainsi que son URL ou de l'application. Vous pouvez également enregistrer des séquences vidéo ou des enregistrements audio de l'attaque elle-même. Plus vous recueillerez de preuves, plus vous aurez de chances d'être payé.

Gardez une trace de vos progrès
Comme indiqué précédemment, de nombreuses entreprises offrent des primes pour certains types de bogues. Veillez donc à consigner tous les exploits que vous découvrez. Ainsi, vous ne manquerez rien d'important. C'est en forgeant qu'on devient forgeron : même si vous deviez déjà savoir coder, la pratique des défis de codage contribue à améliorer vos connaissances en matière de bug bounty. De plus, cela vous permet de vous entraîner à identifier les failles des applications.

SECURITY AWARENESS OFFICER

Niveau d'études : Bac+5

Spé Conseillée : Scientifique

Employabilité : Bonne

Salaire débutant : 4 100 €

Code ROME : M1802 - Code FAP : M2Z

LA MULTIPLICATION DES CYBERATTAQUES OBLIGE LES ENTREPRISES À RENFORCER LEUR NIVEAU DE SÉCURITÉ. PENDANT DE NOMBREUSES ANNÉES, LA TECHNOLOGIE EST APPARUE COMME LA PRINCIPALE PARADE. MAIS CE N'EST PAS UNE SOLUTION MIRACLE, CAR LA MAJORITÉ DES ATTAQUES MALVEILLANTES EXPLOITENT TOUJOURS LE MÊME FILON : LA MÉCONNAISSANCE DES SALARIÉS EN MATIÈRE DE PIRATAGE. C'EST LA RAISON POUR LAQUELLE, DE PLUS EN PLUS D'ENTREPRISES METTENT EN PLACE DES PROGRAMMES DE SENSIBILISATION DE TOUS LES COLLABORATEURS. UN SECURITY AWARENESS OFFICER (QUE L'ON PEUT TRADUIRE PAR RESPONSABLE DE LA SENSIBILISATION À LA SÉCURITÉ) JOUE DONC UN RÔLE MAJEUR, CAR ELLE EST RESPONSABLE DE L'ÉDITION ET DE LA MISE EN PLACE DU PROGRAMME DE SENSIBILISATION ET D'ÉDUCATION À LA CYBERSÉCURITÉ.

Missions

En collaboration avec d'autres membres du département informatique, le security awareness officer gère un large éventail d'activités. Il doit structurer et maintenir son programme à long terme, car il ne s'agit pas seulement d'un changement de comportement, mais de culture.

Ses différentes missions sont les suivantes :

· S'assurer que le programme de sensibilisation à la sécurité répond à toutes les réglementations, normes et exigences de conformité du secteur d'activité de l'entreprise

· Établir et garantir que le programme de sensibilisation à la sécurité communique les politiques et exigences en matière de sécurité afin que les collaborateurs les connaissent, les comprennent et puissent les suivre

· Identifier les principaux risques humains pour l'entreprise et les comportements qu'il convient de changer pour atténuer ces risques

· Développer et maintenir un programme de sensibilisation à la sécurité qui modifie efficacement ces comportements, afin que les salariés agissent de manière sécurisée, réduisant ainsi les risques les plus importants pour l'organisation

· Veiller à ce que des informations régulières soient transmises aux employés pour les tenir au courant des risques de sécurité, des tendances en matière d'attaques et des meilleures pratiques, afin qu'ils prennent conscience de leurs responsabilités

et agissent de manière plus sûre sur les sujets cyber, tant à la maison qu'au travail
· Définir un kit d'accueil pour les employés/contractants en matière de cybersécurité afin de faciliter leur intégration et de les aider à se mettre à niveau dans les plus brefs délais
· Structurer et tenir à jour les documents relatifs à la sécurité, en mettant l'accent sur les politiques et les enregistrements, afin de faciliter l'audit du département de cybersécurité par les parties prenantes concernées (internes ou externes)

Compétences

Pour travailler dans une entreprise, le security awareness officer doit posséder certaines connaissances afin d'exercer correctement ses activités :

· Connaissance de base de la manière dont les processus commerciaux sont soutenus par les contrôles informatiques et de sécurité
· Bonnes compétences en matière de connaissances générales sur la cybersécurité, y compris les risques, les techniques d'attaque et les principales mesures d'atténuation, afin de garantir un GO approprié entre l'expert technique et les employés
· Bonne connaissance de l'exigence du système de gestion de la sécurité de l'information (ISO2700x)

Ce professionnel doit avoir de l'expérience dans la gestion de projet, la capacité de planifier, gérer et maintenir un programme, qui dans certains cas peut avoir un plus grand niveau de complexité, à travers l'organisation.

En outre, ce professionnel doit comprendre les concepts de cyberrisques et les différents éléments qui constituent un risque. Il doit connaître les différents concepts et la terminologie associés à la sécurité de l'information.

Dès lors, il doit posséder ces différentes compétences :

· Maîtrise des outils et plateformes spécifiques à la formation en SSi
· Connaissance du système d'information et des principes d'architecture
· Connaissance des technologies de sécurité et des outils associés
· Gestion des risques, politique de cybersécurité et SMSi (en anglais : Information security management system, ou ISMS)
· Maîtrise des fondamentaux dans les principaux domaines de la SSi
· Veille technologique cybersécurité et étude des tendances

Études

En plus d'un Bac +5, disposée d'une ou de plusieurs certifications de sécurité CISSP, ISO 2700x Lead implementer, C-RISC ou encore CISM est un plus.

Quel bac ?

Bac +5 en système d'Information

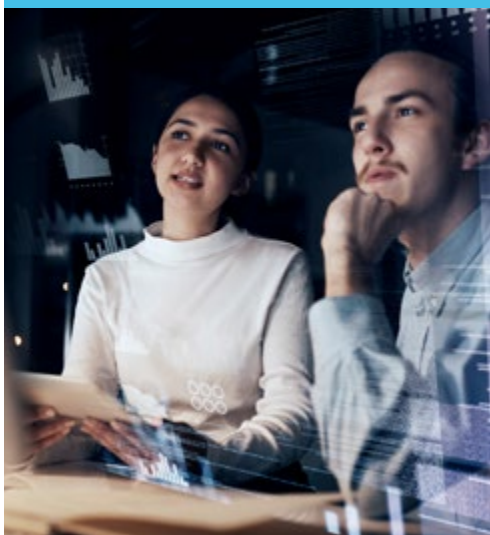
Quelle école ?

Une école d'ingénieur spécialisée en cybersécurité est indispensable.

QUALITÉS

Si la cybersécurité est technique par nature, les responsables de la sensibilisation à la sécurité doivent exceller dans la compréhension et la collaboration avec les autres. Les courriels d'hameçonnage (ou phishing) incitant continuellement les utilisateurs à effectuer diverses actions, l'élément humain de la cybercriminalité est de plus en plus important. Il incombe au security awareness officer de veiller à ce que l'organisation ne s'appuie pas uniquement sur la technologie pour combattre les pirates. Il doit donc être capable de modifier son programme de formation en cours de route en fonction de l'évolution des menaces et de la réglementation. Il est donc impératif de posséder de solides compétences en communication et en service à la clientèle. Il est également capital de répondre efficacement aux attentes des diverses parties prenantes internes.

« LE SECURITY AWARENESS OFFICER EST RESPONSABLE DU PROGRAMME DE SENSIBILISATION ET D'ÉDUCATION À LA SÉCURITÉ DANS LES GRANDES ENTREPRISES. SON TRAVAIL CONSISTE À RÉDUIRE LES RISQUES POUR SON ORGANISATION EN S'ASSURANT QUE TOUS LES EMPLOYÉS, LE PERSONNEL ET LES CONTRACTANTS CONNAISSENT, COMPRENNENT ET SUIVENT SES EXIGENCES EN MATIÈRE DE SÉCURITÉ ET SE COMPORTENT DE MANIÈRE SÉCURISÉE. »



« LE TRAVAIL D'UN SECURITY AWARENESS OFFICER CONSISTE À RÉDUIRE LES RISQUES POUR SON ENTREPRISE EN VEILLANT À CE QUE TOUS LES EMPLOYÉS, LE PERSONNEL ET LES CONTRACTANTS CONNAISSENT, COMPRENNENT ET RESPECTENT LES EXIGENCES EN MATIÈRE DE SÉCURITÉ ET SE COMPORTENT DE MANIÈRE SÛRE. L'OBJECTIF EST QUE LES EMPLOYÉS ADOPTENT LES MÊMES COMPORTEMENTS SÉCURITAIRES, QUEL QUE SOIT L'ENDROIT OÙ ILS SE TROUVENT OU LES APPAREILS QU'ILS UTILISENT. »

Salaire

Il varie entre 50 000 euros brut par an et 90 000 euros brut par an selon l'expérience et la taille de l'entreprise.

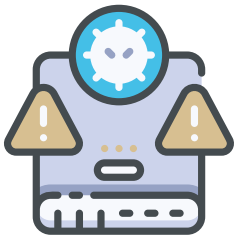
Évolution de carrière

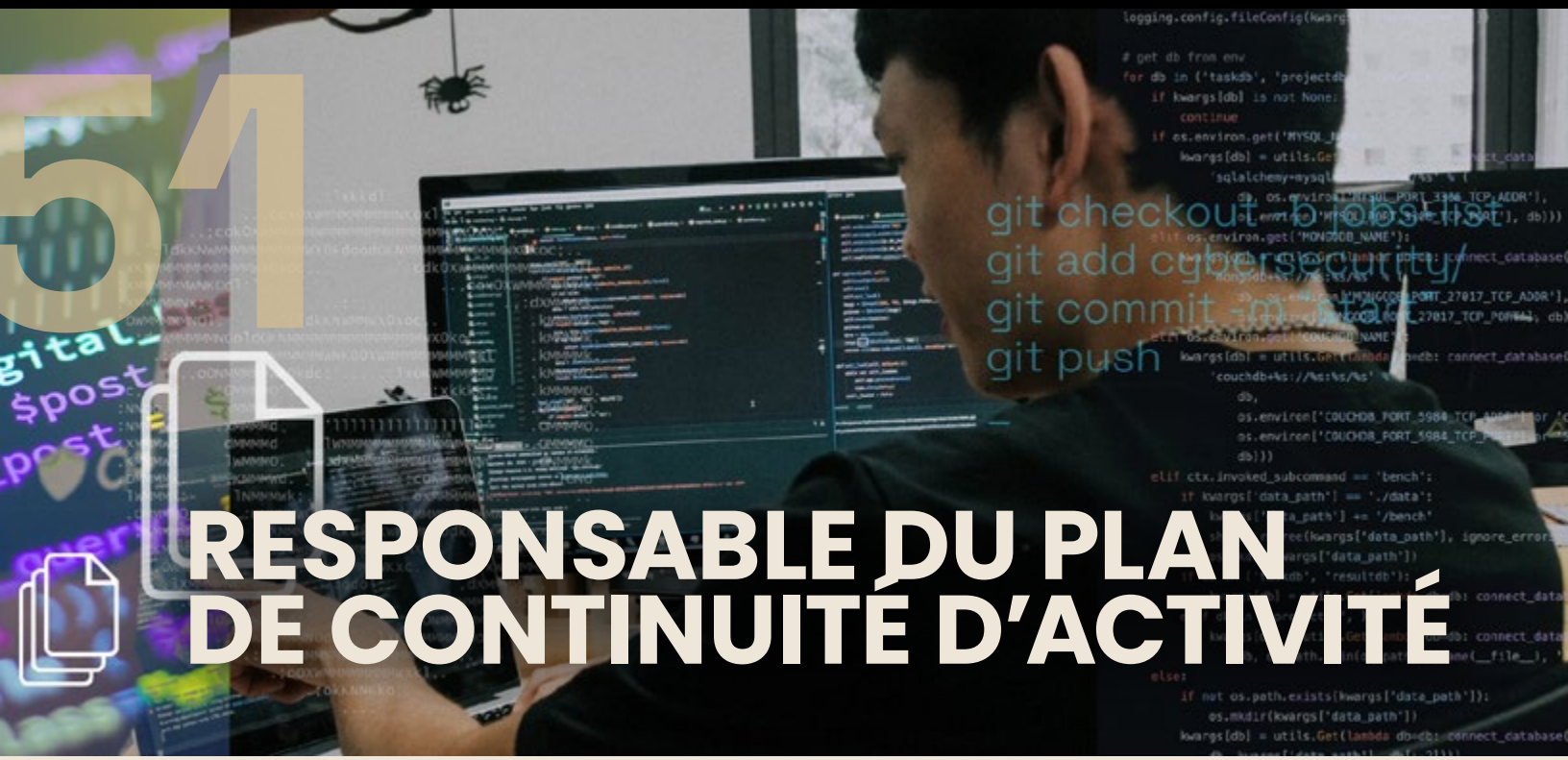
De par ses compétences, un security awareness officer peut évoluer dans diverses directions. Il peut devenir un DPO (data protection officer) pour veiller à la mise en conformité de son entreprise avec le RGPD (règlement général sur la protection des données» – en anglais «general data protection regulation» ou GDPR). Il peut aussi évoluer pour devenir un DSI (directeur des systèmes informatiques), voire un RSSI (responsable sécurité des systèmes d'information).

Comment le devenir ?

La sensibilisation à la sécurité est l'un des domaines les plus passionnants. Non seulement vous pouvez avoir le plus grand impact sur la sécurité globale d'une entreprise, mais il est encore relativement nouveau. Vous pouvez contribuer à développer son avenir.

Mais il est important de savoir qu'une solide expérience en matière de sécurité ne suffira pas à vous faire réussir. Vous devez vous diversifier et acquérir de nouvelles compétences, notamment en matière de communication et de collaboration.





51 RESPONSABLE DU PLAN DE CONTINUITÉ D'ACTIVITÉ

Niveau d'études : Bac+5

Spé Conseillée : Eco. et Soc. ou Scien.

Employabilité : Bonne

Salaire débutant : 3 500 €

Code ROME : M1402 - Code FAP : L5Z

VOUS AIMEZ NAVIGUER ENTRE DES RESPONSABILITÉS DE DIFFÉRENTES NATURES, TANTÔT DU CÔTÉ DU PILOTAGE DE PROJET, TANTÔT DU CÔTÉ DU CONSEIL STRATÉGIQUE ? VOUS APPRÉCIEZ TOUT AUTANT DE FAIRE LE LIEN ENTRE DES CHAMPS DE COMPÉTENCES DIFFÉRENTS – MAIS COMPLÉMENTAIRES – AU SEIN D'UNE GRANDE STRUCTURE ? VOUS DISPOSEZ D'ORES ET DÉJÀ DE BONNES BASES POUR ABORDER UN POSTE DE RESPONSABLE DU PLAN DE CONTINUITÉ D'ACTIVITÉ AVEC SÉRÉNITÉ ET ENTHOUSIASME. SI VOUS AIMEZ RESSENTIR DIRECTEMENT LE POIDS DES RESPONSABILITÉS, CE MÉTIER EST FAIT POUR VOUS : EN CAS D'INCIDENT CYBER, C'EST VOUS QUI SEREZ LE PILIER À QUI IL REVIENT DE MAINTENIR LA STRUCTURE DEBOUT – EN MAINTENANT SES ACTIVITÉS ET SES AFFAIRES SUR LA BONNE TRAJECTOIRE. VOYONS PLUS EN DÉTAILS COMMENT SE STRUCTURE CE MÉTIER D'IMPORTANCE CRUCIALE À L'ÈRE DES HACKERS ET DES ATTAQUES INFORMATIQUES.

Missions

La première tâche du responsable PCA consiste à dialoguer avec tous les départements impactés par l'attaque informatique, de manière directe ou indirecte, afin d'identifier les risques avérés ou potentiels, avant de proposer des solutions concrètes visant à maîtriser ou, du moins, minimiser ces risques. C'est à lui que revient la mission délicate d'aider tous les responsables et toutes les équipes impactées de près ou de loin à gérer et mieux vivre les périodes de crise.

Cela suppose un autre travail de dialogue préalable, avec ces mêmes départements et leurs responsables, afin de comprendre leurs processus de fonctionnement, l'organisation de leurs forces de travail et l'architecture globale de leurs systèmes techniques. En période de calme – c'est-à-dire en dehors des crises et incidents, c'est là le travail principal du responsable PCA : continuer à affiner sa connaissance des entités qui l'entourent et composent l'entreprise, et mettre à jour, si besoin, ses connaissances à leur sujet, suite à des mises à jour techniques, un changement structurel ou une recomposition notamment.

Plus particulièrement, ce professionnel doit communiquer de manière ininterrompue avec les fonctions commerciales critiques afin de bien évaluer les dommages financiers et de penser aux actions de récupération.

Comme son titre l'indique de manière très claire, le RPCA est tenu de mettre au point – plus qu'un document – une véritable politique qui prend le nom de plan de continuité d'activité. Il lui revient donc

« À LA LISIÈRE DE LA GESTION DU RISQUE, DU PILOTAGE DES ORGANISATIONS, DU CONSEIL ET DE L'AUDIT, C'EST LUI QUI EST CHARGÉ D'ASSURER LA POURSUITE DE LA PRODUCTION, DES TRANSACTIONS, DE LA RELATION CLIENT ET DE LA RELATION CONSOMMATEUR, ET DE TOUTE AUTRE ACTIVITÉ CONSTITUANT LA RAISON D'ÊTRE DE L'ENTREPRISE, EN CAS D'ATTAQUE INFORMATIQUE. »

de définir les grandes lignes d'action qui permettront de ne pas mettre l'entreprise en situation de freinage ou à l'arrêt total.

Sa fonction est intimement liée à la notion de cyber-résilience. Il s'agit de prendre en compte des scénarios :

Qui ne correspondent pas à la situation idéale souhaitée par l'entreprise, dans ses meilleures projections de croissance ;

Mais qui prennent en compte la réalité de l'attaque et définissent une nouvelle « situation idéale », prenant en compte l'incident majeur qui est survenu. Celle-ci est pensée pour être temporaire, avant une remise en état de tous les systèmes et un dépassement des conséquences néfastes de l'attaque.

C'est toute la filière cybersécurité de l'entreprise qui est appelée à informer le RPCA sur les risques de continuité pouvant être causés par une attaque informatique. En amont, avant même qu'un incident ne survienne, le responsable du plan de continuité valide avec les experts cyber les mesures à mettre en œuvre en cas de crise. Celles-ci constituent un premier filet de sécurité, permettant de réagir sans délai sur tous les critères dits de disponibilité et d'intégrité, en cas d'incident. Chaque mesure doit être soumise à des tests : c'est le RPCA qui doit en assurer l'organisation et le suivi, en visant une amélioration continue des résultats obtenus.

Ces mesures seront ajustées et affinées au cas par cas, selon la nature et l'étendue de chaque incident.

Compétences

Le responsable du plan de continuité d'activité doit être opérationnel sur un certain nombre de points liés à la gestion de projet et à la gestion de crise. Il doit disposer de tous les éléments de compréhension relatifs à la structure et à son activité afin de :

· Mettre en place des plans de continuité d'activité et, si nécessaire, de reprise prévoyant la restauration des actifs critiques touchés par l'attaque (un système d'information ou un centre de données, très souvent)
· Déterminer le risque potentiel et l'impact réel sur les fonctions commerciales les plus importantes
· Définir le temps de récupération acceptable en cas d'incident et les ressources à mobiliser pour maintenir la structure en état de fonctionnement
· Réaliser des tests sur les stratégies de continuité proposées
· Élaborer des plans d'urgence pour assurer des prises de décision rapides et un relais efficace des informations qui y ont trait auprès de tous les départements concernés
· Analyser les conséquences potentielles d'une fermeture d'un service ou d'un autre en cas d'incident
· Définir les services les moins critiques, qui pourront être mis en pause plus facilement pour gérer la restauration de l'état initial

QUALITÉS

Le responsable du plan de continuité d'activité doit faire preuve d'un sens de l'organisation et de la communication imparables, qui lui serviront notamment pour :
· Définir des arbres d'appel afin de garantir un relais rapide et efficace des informations en cas de crise
· S'adapter à divers types de publics dans ses communications orales et écrites, notamment dans ses rapports d'analyse
· Avoir une appétence claire pour les questions logistiques
Il doit également posséder un certain goût pour les questions techniques : c'est à lui que revient en effet le rôle de suggérer des améliorations dans les outils de communication utilisés, dans un souci permanent de rapidité.
Les qualités pédagogiques sont aussi de mise, dans la mesure où le RPCA est susceptible d'accompagner les différents métiers dans la conception de plans de continuité d'activité spécifiques.
La rigueur, la capacité à l'adaptation et la créativité sont enfin d'autres qualités évidentes pour réussir à ce poste, de même qu'une aptitude confirmée à la prise de décision.

Le responsable PCA a besoin de compétences analytiques solides, qui devront lui permettre de proposer des scénarios de rétablissement rapide des opérations à partir de différents cas de perturbation.

Outre ce travail en amont, qui relève de la prévision et de la précaution, le RPCA doit être particulièrement actif pour :

· Faire le point sur l'efficacité du plan de continuité après retour à un niveau d'activité normal
· Identifier les points d'amélioration possible pour réduire le temps d'interruption des activités en cas de nouvel incident
· Affiner les méthodes de veille et d'alerte relatives à la détection en amont des risques de répercussion des attaques cyber
· Rédiger des rapports faisant état de l'ensemble des conclusions et proposant des pistes d'amélioration. Il sera par ailleurs bienvenu de définir des objectifs relatifs au maintien d'un certain niveau d'activité en cas de crise

Études

Pour accéder à un emploi de responsable de plan de continuité d'activité, un Bac +5 est le minimum requis. Les postes sont généralement confiés à des professionnels justifiant de quelques années d'expérience dans une ou plusieurs branches « métier » au sein d'une entreprise. C'est là la garantie d'une bonne compréhension des enjeux structurels et organisationnels.

Salaire

Pour un profil débutant, on calcule un salaire d'entrée moyen de 3 500 euros brut mensuels environ. Le niveau peut être ajusté en fonction de l'expérience passée du responsable PCA : plus le nombre de branches « métiers » au sein desquelles il a pu exercer ses fonctions est important, plus sa connaissance théorique de la structure d'entreprise est affinée, plus il peut négocier à la hausse. La négociation sera d'autant plus aisée si le RPCA a passé plusieurs années au sein de l'entreprise auprès de laquelle il postule, puisqu'il en connaît non seulement les rouages, mais aussi les équipes. Les contacts sont alors déjà établis et on peut espérer une réactivité optimale en cas d'incident.

Un responsable du plan de continuité d'activité confirmé peut viser un salaire avoisinant les 5 500 euros brut mensuels. Une fois de plus, sa longévité dans l'entreprise et la variété de ses expériences seront des arguments forts pour obtenir un salaire légèrement supérieur.

Où travailler ?

« Qui dit plan de continuité d'activité, dit très souvent entreprise bien installée ou grand groupe. Sur cette base, tous les secteurs d'activité sont susceptibles de s'attacher les services d'un responsable PCA réactif et rassembleur », analyse François-Stéphane H., actuellement en poste auprès d'un grand nom du commerce en ligne. *« Du secteur du luxe à celui de la banque, en passant par les assurances, les acteurs de la tech ou la grande distribution, il y a des besoins partout et les horizons d'emploi sont larges. »*

Parmi les entreprises en recherche de responsables PCA, avec de belles fiches de poste, on repère :

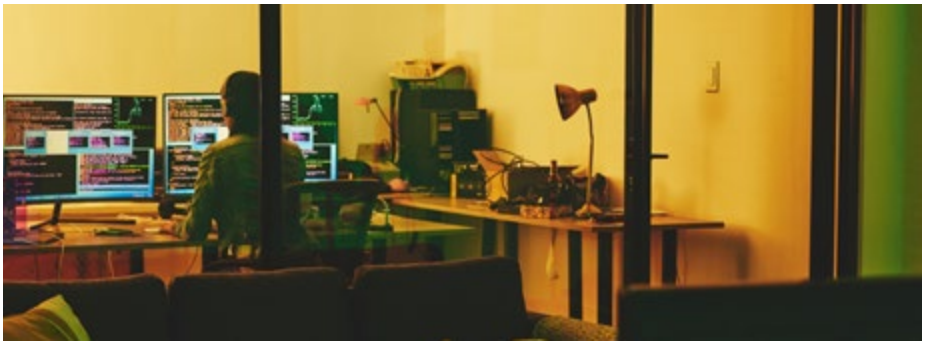
· Le Groupe Crédit Agricole, AXA Banque, Dogfinance et le groupe BPCE du côté banque et investissement
· Adsearch
· Air France

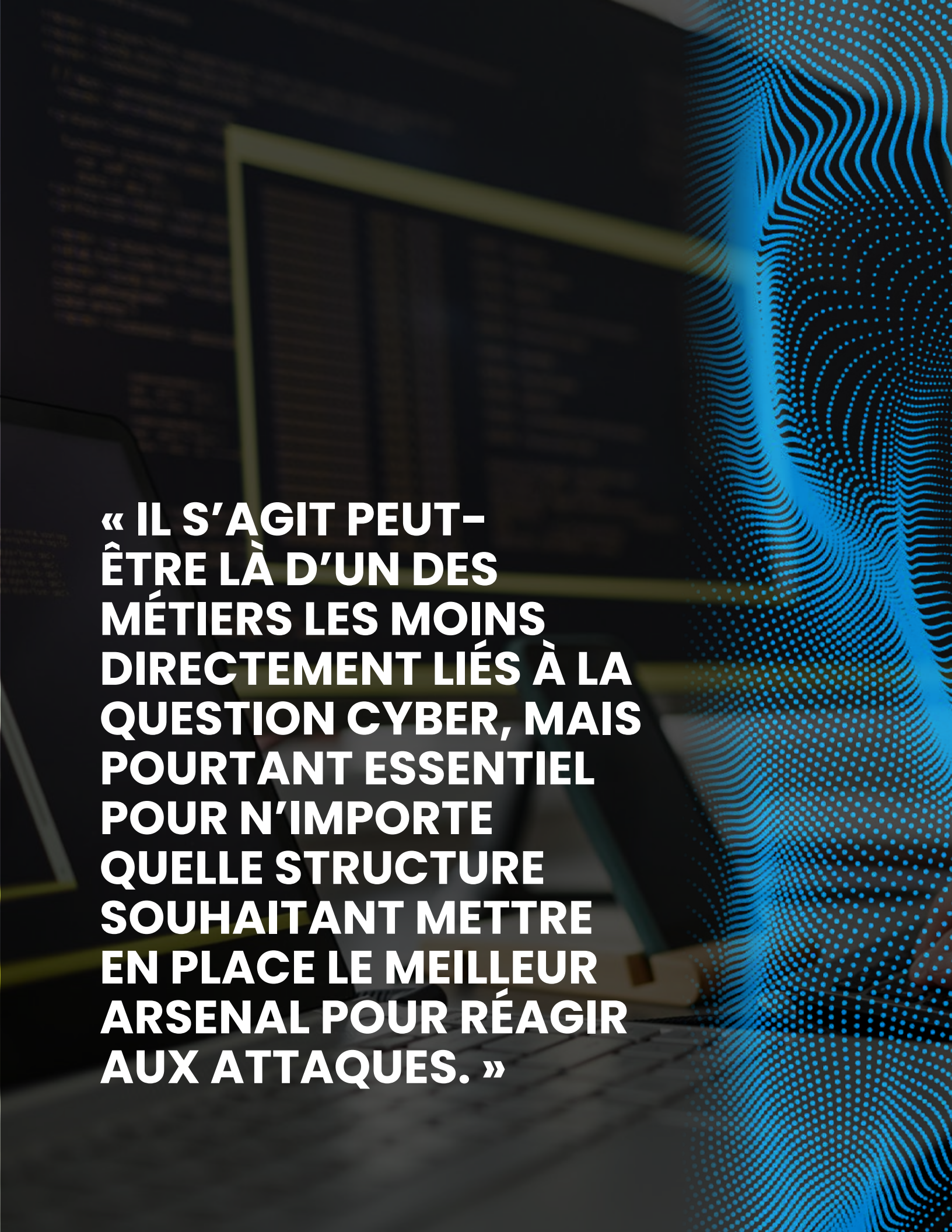
Évolution de carrière

« S'il a bien travaillé son approche des questions purement techniques, un responsable de PCA peut envisager d'évoluer, sans trop de difficultés, vers des fonctions de consultant en cybersécurité ou, pourquoi pas, de gestionnaire de crise de cybersécurité. Il devra certainement faire ses preuves, mais cette part de défi doit être une motivation supplémentaire. C'est une piste d'évolution que j'envisage pour moi-même. Et, pour y être bien préparé, je suis des formations plus techniques, afin de trouver mes appuis sur le terrain informatique. Une source de beaucoup d'épanouissement ! », confie François-Stéphane H.

Avantages et inconvénients

De l'avis de François-Stéphane H., *« être attentif au moindre détail, sans interruption, cela peut être très énergivore et provoquer, à terme, une certaine lassitude. Il faut donc s'assurer d'avoir la passion du travail bien fait chevillée au corps ! »* Parmi les avantages évidents du poste, selon ce professionnel qui exerce les fonctions de RPCA depuis 6 ans, il y a une certaine place laissée à l'improvisation : *« Il y a une part de créativité – logistique, humaine, technique un peu aussi – qui existe réellement, au cœur du poste. Les crises inattendues ne génèrent pas uniquement de la tension, c'est aussi un coup de boost très agréable sur ce type de poste. Le goût du défi doit être là. Pour moi, c'est une motivation réelle. »*





« IL S’AGIT PEUT-ÊTRE LÀ D’UN DES MÉTIERS LES MOINS DIRECTEMENT LIÉS À LA QUESTION CYBER, MAIS POURTANT ESSENTIEL POUR N’IMPORTE QUELLE STRUCTURE SOUHAITANT METTRE EN PLACE LE MEILLEUR ARSENAL POUR RÉAGIR AUX ATTAQUES. »

52

EXPERT·E EN CYBERSÉCURITÉ

Niveau d'études : Bac+5

Spé Conseillée : Scientifique

Employabilité : Bonne

Salaire débutant : 3 300 €

Code ROME : M1802 - Code FAP : M2Z

DANS UN MONDE HYPER CONNECTÉ OÙ TOUS LES RÉSEAUX ET ÉQUIPEMENTS INFORMATIQUES ET INDUSTRIELS ÉCHANGENT EN PERMANENCE DES DONNÉES, LA CYBERSÉCURITÉ EST DEVENUE UN ENJEU MAJEUR POUR TOUTES LES ENTREPRISES. LA MULTIPLICATION DES ATTAQUES, DONT CERTAINES SONT TRÈS SOPHISTIQUÉES, NÉCESSITE DE FAIRE APPEL À DES EXPERTS EN CYBERSÉCURITÉ. CES PROFILS SONT TRÈS RECHERCHÉS PAR TOUS LES SECTEURS. UN MÉTIER D'AVENIR.

Missions

Avec l'avancée de la technologie, de nouvelles menaces de sécurité peuvent apparaître à tout moment. L'expert en cybersécurité doit donc rester vigilant et se tenir au courant des dernières tactiques des pirates informatiques.

Ses principales missions sont les suivantes :

· Surveiller l'infrastructure IT pour identifier et bloquer des activités inhabituelles ou suspectes afin éviter que les données sensibles ne soient compromises

· Protéger les systèmes d'information de son entreprise en mettant en œuvre des processus de sécurité et en particulier de gestion des correctifs

· Effectuer des audits réguliers pour s'assurer que les techniques de sécurité sont conformes à l'état de l'art

· Travailler en étroite collaboration avec la direction et l'équipe chargée de l'informatique pour mettre en place des plans de continuité et de reprise d'activité (PCA et PRA)

· Sensibiliser les autres services à l'importance de la cybersécurité

· Assurer une veille technologique et règlementaire…

Les spécialistes de la cybersécurité jouent un rôle clé dans la sécurisation des systèmes d'information (SI). En surveillant, détectant, enquêtant, analysant et répondant aux événements de sécurité, ils protègent les réseaux informatiques et les postes de travail contre les cybermenaces.

L'objectif premier des experts en cybersécurité est de protéger les données et l'infrastructure informatique d'une entreprise. Cette responsabilité repose sur un large éventail de tâches et de compétences. Ils mettent en place des audits des systèmes d'exploitation (Windows, Linux, MacOs…), des serveurs web et des bases de données, ainsi que des évaluations de la vulnérabilité.

Compétences

Outre les compétences générales de base comme la communication, le leadership, le travail d'équipe et la résolution de problèmes, voici les compétences techniques requises :

1. Mise en réseau et administration de systèmes

Cela peut en étonner plus d'un, mais cette compétence s'avère indispensable. La mise en réseau étant le fondement de l'internet, il est en effet essentiel d'en avoir une connaissance approfondie si vous souhaitez faire carrière dans la cybersécurité.

Cette maîtrise consiste à comprendre comment les données sont envoyées, transportées et reçues entre les dispositifs connectés qui constituent un réseau. Vous devez donc connaître les différents modèles OSI (Open Systems Interconnexion ou Interconnexion de Systèmes Ouverts en Français) et TCP (Transmission Control Protocol, appelé «modèle Internet») des protocoles de routage. Un protocole est un ensemble de règles qui définissent comment différents systèmes communiquent entre eux.

2. Connaissance des systèmes d'exploitation

Vous devez avoir une connaissance approfondie des systèmes d'exploitation tels que Windows, Linux et Mac OS pour travailler dans le domaine de la cybersécurité. En tant que spécialiste de la cybersécurité, vous devrez être à l'aise avec n'importe quel système d'exploitation.

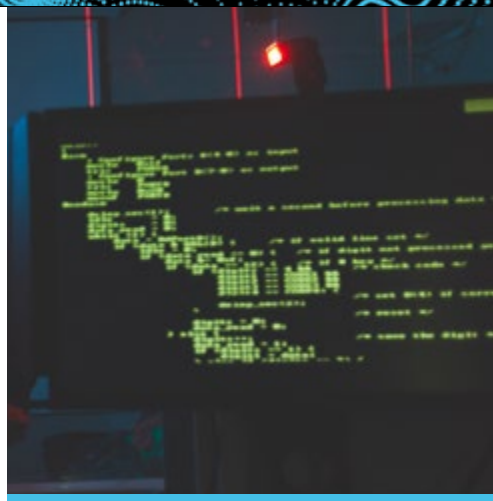
3. Contrôle de la sécurité des réseaux

Le contrôle de la sécurité des réseaux fait référence aux diverses méthodes utilisées pour améliorer, identifier et assurer la confidentialité de la sécurité des infrastructures IT. Il s'agit d'une autre compétence fondamentale que tout expert en cybersécurité devrait posséder. Il est en effet difficile de prétendre protéger efficacement un réseau si on ne sait pas comment fonctionnent les routeurs, les pare-feux et les autres dispositifs.

En tant que spécialiste de la cybersécurité, vous devez notamment être capable de configurer un pare-feu pour filtrer et empêcher le trafic non autorisé de pénétrer sur le réseau. En outre, vous devez connaître les réseaux privés virtuels, l'accès à distance, les systèmes de détection des intrusions et les systèmes de prévention des intrusions.

4. Codage

Tous les professionnels de la cybersécurité n'ont pas besoin ou ne possèdent pas de compétences en codage. Mais, le fait de ne pas savoir coder pourrait limiter vos possibilités de carrière. La connaissance de quelques langages de programmation vous permettra de repérer la stratégie d'une attaque et de mettre en place une défense adaptée.



QUALITÉS

La cybersécurité étant un domaine très technique qui évolue très rapidement, il est indispensable d'être bien organisé, passionné par l'informatique en général et la protection des données/réseaux en particulier, de pouvoir travailler en équipe afin de partager ses compétences auprès des autres services et de sa direction (pour qu'elle comprenne les enjeux de la cybersécurité, l'un des principaux étant la résilience de l'entreprise) et… d'être bilingue (notamment pour la veille technologique).

« IL EXISTE ACTUELLEMENT UNE TRÈS FORTE DEMANDE D'EXPERTS EN CYBERSÉCURITÉ DANS DIVERS SECTEURS. IL EST DONC POSSIBLE DE TRAVAILLER POUR UN INDUSTRIEL, UN CABINET SPÉCIALISÉ DANS LA SÉCURITÉ INFORMATIQUE, UNE ENTREPRISE PRIVÉE, VOIRE UNE ADMINISTRATION. LES OFFRES D'EMPLOI NE MANQUENT PAS ! »

5. La sécurité dans le cloud

En quelques années, toutes les entreprises ont migré une partie plus ou moins significative de leurs workloads dans le cloud. Dès lors, ces organisations ont besoin d'experts en cybersécurité spécialisés dans la sécurité du cloud. Les entreprises recherchent des personnes ayant une expertise en sécurité qui s'applique aux plates-formes de cloud public et hybride comme Amazon Web Services ou Microsoft Azure.

Cela inclut la mise en œuvre de politiques et de protections technologiques pour sauvegarder les dispositifs et les systèmes basés sur le cloud. Comme la sécurité du développement d'applications, la sécurité du cloud comprend également le développement de systèmes sécurisés dès le départ.

6. Intelligence artificielle (IA)

L'intelligence artificielle (IA) commence à être de plus en plus utilisée en cybersécurité même si toutes les solutions commercialisées sont loin d'être réellement efficaces… Mais certaines applications d'IA possèdent des capacités de détection très efficaces et évidemment beaucoup plus rapides que l'analyse humaine.

Études

Un diplôme en informatique permet d'acquérir des connaissances de base en technologie de l'information (TI), notamment la compréhension des protocoles TCP/IP qui sont au cœur de tous les réseaux.

Une certification complémentaire peut aider les professionnels à trouver un emploi dans le domaine de la cybersécurité. Ce secteur évoluant rapidement.il est important de se former en permanence aux nouvelles technologies et menaces.

Quelle école ?

La voie royale est celle d'une école d'ingénieurs en cybersécurité qui propose de nombreux cours pratiques sur la sécurité informatique. Mais il est important de compléter ce cursus par des formations spécialisées et des stages afin de mieux appréhender ce métier.

Quel bac ?

Bac +5 en Système d'Information.

Salaire

Un expert en cybersécurité Junior (de 0 à 2 ans) peut prétendre à un salaire compris entre 40 000 euros et 50 000 euros par an. Un spécialiste Confirmé (de 2 à 5 ans) touchera entre 45 000 euros et 70 000 euros. Enfin, un Senior (de 5 à 15 ans) peut prétendre à une rémunération comprise entre 70 000 euros et plus de 90 000 euros.

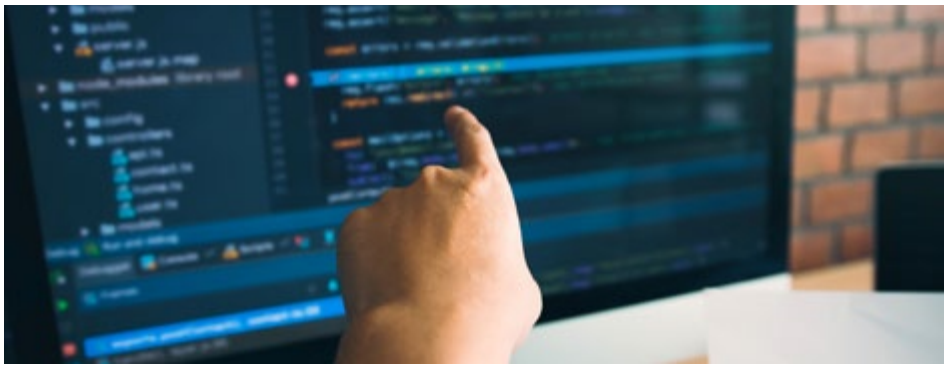
Évolution de carrière

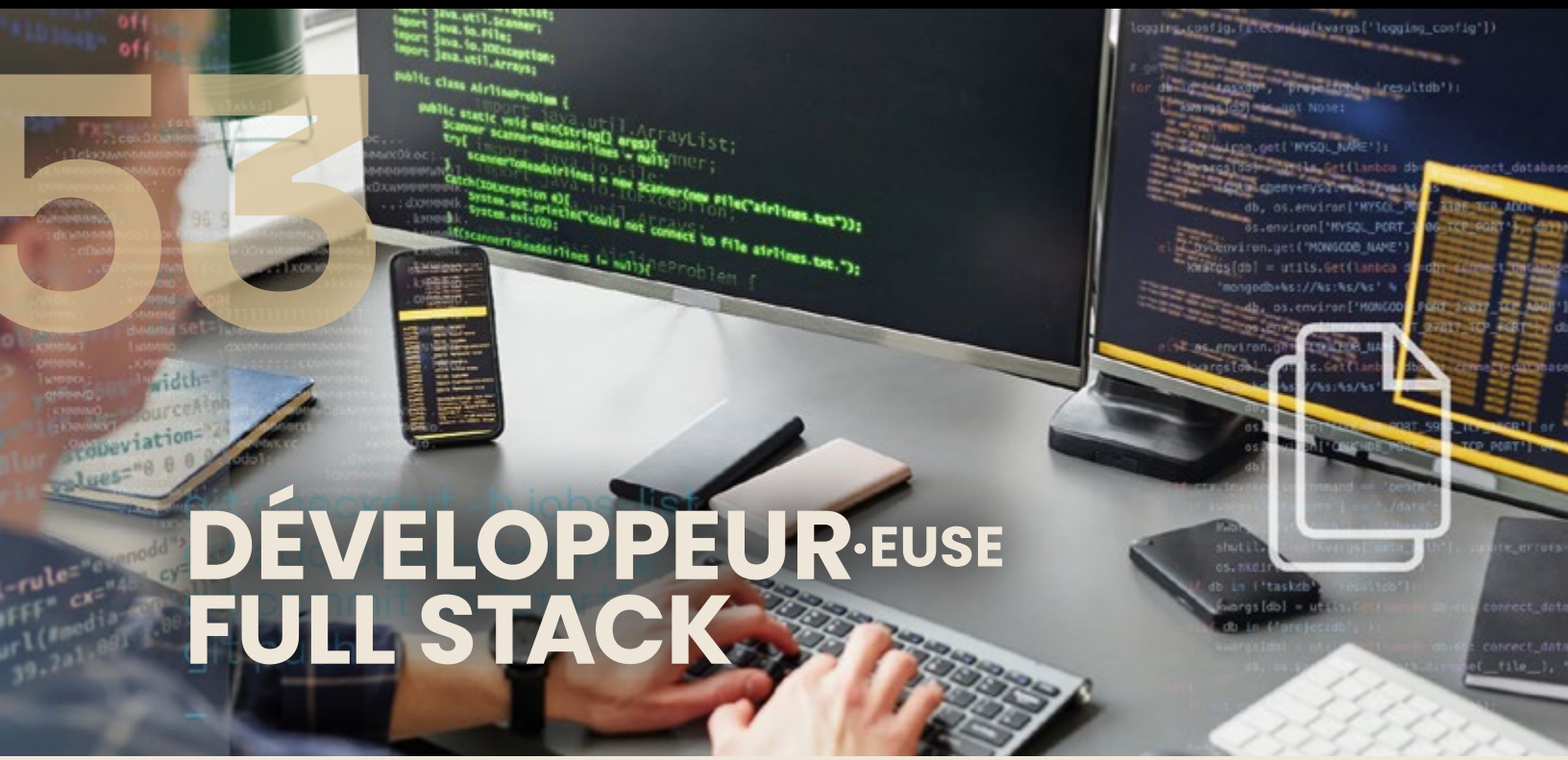
De nombreux experts en cybersécurité finissent par se mettre à leur compte ou par travailler en tant que consultants. Toutefois, il est également possible de s'orienter vers un poste de Délégué à la protection des données (data protection officer). Dans ce cas, un expert en cybersécurité pourra mettre à profit ses fortes compétences techniques et organisationnelles pour renforcer la protection des données à caractère personnelle (en référence au Règlement général sur la protection des données-RGPD).

Autre piste d'évolution : devenir Responsable de la sécurité et des systèmes d'information (RSSI) ou Responsable de la gouvernance sécurité.

Comment le devenir ?

C'est un métier d'avenir car de nombreuses entreprises embauchent ces spécialistes. Il est possible de travailler au sein d'une entreprise ou dans une ESN. Les rémunérations les plus élevées se trouvent notamment dans le secteur financier. Mais il faut suivre un parcours très sélectif. Un diplôme d'ingénieur est indispensable, mais il faut aussi le compléter par des certifications. Les plus connues sont le CISA et le CISM de l'ISACA (Association pour l'Audit et le Contrôle des Systèmes d'Information). Enfin, le cloud étant généralisé, il peut être appréciable de décrocher le certified cloud security professional, une certification pour renforcer les compétences en sécurité des hébergements en ligne (datacenter) et des accès distants.





DÉVELOPPEUR·EUSE FULL STACK

Niveau d'études : Bac+3 à Bac+5

Spé Conseillée : Scientifique

Employabilité : Bonne

Salaire débutant : 2 500 €

Code ROME : M1802 - Code FAP : M2Z

CE PROFESSIONNEL EST RESPONSABLE DE LA CONCEPTION ET DU DÉVELOPPEMENT DE SITES WEB ET DE PLATEFORMES. IL TRAVAILLE AVEC LES ÉQUIPES DE CONCEPTION POUR S'ASSURER QUE LES INTERACTIONS DES UTILISATEURS SUR LES PAGES WEB SONT INTUITIVES ET ATTRAYANTES. IL FOURNIT ÉGALEMENT DES FONCTIONNALITÉS BACK-END QUI PEUVENT FONCTIONNER DE MANIÈRE FLUIDE À PARTIR DE N'IMPORTE QUEL APPAREIL OU TYPE DE NAVIGATEUR COURAMMENT UTILISÉ AUJOURD'HUI.

Missions

Quelle que soit leur mission, les développeurs full stack commencent par réfléchir à des plateformes aux côtés d'une équipe de conception graphique, examinant souvent des prototypes avant de les transformer en produits codés.

Ensuite, ces programmeurs polyvalents créent des bases de données et des serveurs fonctionnels pour prendre en charge le contenu destiné aux clients, en évaluant toujours la réactivité d'une application pour les utilisateurs finaux et en résolvant les problèmes si nécessaire.

Ses responsabilités quotidiennes comprennent notamment de :

· Travailler avec CSS, HTML et JavaScript, ainsi qu'avec les préprocesseurs CSS, pour créer des plates-formes orientées client
· Gérer des bases de données et des serveurs, et concevoir l'architecture côté client et côté serveur
· Coder des fonctionnalités dans plusieurs langues et sur plusieurs plates-formes
· Créer des paramètres de sécurité et de protection des données
· Tester les logiciels pour garantir leur réactivité et leur efficacité
· Communiquer avec les développeurs spécialisés et l'équipe de conception graphique afin de fournir le meilleur produit possible
· Se tenir au courant des technologies émergentes susceptibles de répondre aux besoins de l'entreprise
· Prototyper des produits minimalement viables pour les communiquer aux

parties prenantes de l'entreprise
· Rédiger de la documentation technique et des API efficaces

Compétences

Si les exigences du rôle d'un développeur «full stack» dépendent de son secteur d'activité et de son poste, tous doivent posséder les mêmes compétences de base en matière de développement front-end et front-back.

Il est donc nécessaire de maîtriser en particulier :

· HTML
· CSS
· JavaScript
· SQL/NoSQL
· Python

Egalement les frameworks JavaScript tels qu'Angular JS, React et Amber est par ailleurs indispensable. Même chose avec la technologie des bases de données telles que MySQL, Oracle et MongoDB.

Études

Comme pour la majorité des métiers du développement informatique, plusieurs formations sont envisageables : formations en ligne, formations courtes en présentiel (1, 3, 6 mois), MOOC… Mais il est néanmoins recommandé d'obtenir un Bac +2 ou +3 (BTS, DUT, Licence). Après le Bac, vous pouvez faire un BTS SIO – SISR ou un DUT Informatique.

Quelle école ?

Un IUT ou école d'ingénieur.

Quel bac ?

Tout baccalauréat peut mener à ce métier, même s'il faut une affinité pour le numérique et les mathématiques.

Salaire

Comme tout métier, le salaire du développeur web full stack évolue en fonction de son expérience, de ses différents projets, mais également de la zone géographique dans laquelle il se trouve. Il perçoit une rémunération souvent un peu plus élevée que celle d'une développeuse front-end ou back-end. Le salaire varie entre 23 000 euros brut par an et 48 000 euros brut par an pour un profil expérimenté.

Ce métier sollicitant de plus en plus l'intérêt des recruteurs (détrônant les développeurs backend), il est possible de négocier son salaire si votre profil correspond au besoin de l'agence web et de ses clients ou pour une grosse entreprise.

Évolution de carrière

Etant donné ses compétences et sa polyvalence, un développeur full stack peut gérer des équipes d'une agence web. Il peut devenir Lead développeur, chef de projet informatique, product manager, directeur de nouvelles technologies ou CTO…

Comment le devenir ?

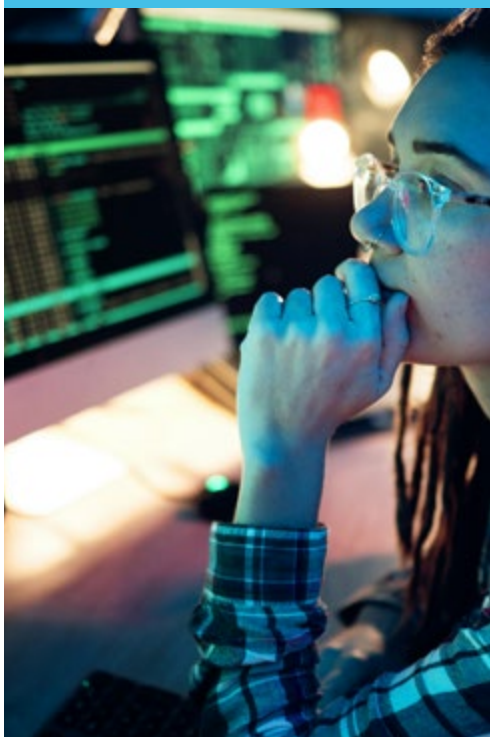
Le métier de développeur full-stack est synonyme de polyvalence. Il inclut les activités d'une développeuse front-end et d'un développeur back-end. D'où son appellation de «full-stack» : développeur à tout faire.

C'est la raison pour laquelle on trouve souvent ce genre de description dans les offres d'emploi : «Il faut être à l'aise avec les langages de codage front-end et front-back, les cadres de développement et les bibliothèques tierces. Vous devez également avoir l'esprit d'équipe et un don pour la conception visuelle et l'utilité».

Si cette description vous intéresse fortement, foncez, mais il faudra connaitre sous le bout des doigts tous les rouages du développement web. Un métier d'avenir, passionnant, mais aussi exigeant.

QUALITÉS

Bien que très autonome, un développeur full stack doit savoir travailler en équipe. En fonction de la taille de l'entreprise et de l'équipe, il collabore généralement avec les interlocuteurs suivants :
· Lead developer, développeur front-end ou développeur back-end
· Chef de projet ou product owner
· Webdesigner
· Rédacteur ou intégrateur web
· Référenceur SEO
· DevOps



54

DÉVELOPPEUR·EUSE WEB

Niveau d'études : Bac+3 à Bac+5

Spé Conseillée : Scientifique

Employabilité : Bonne

Salaire débutant : 2 000 €

Code ROME : M1802 - Code FAP : M2Z

CHARGÉS DE PROGRAMMER DE NOMBREUSES APPLICATIONS WEB, CES PROFESSIONNELS AIDENT LES ENTREPRISES À CRÉER DES SITES ATTRACTIFS ET COMPLETS POUR ATTIRER DE NOMBREUX VISITEURS. ILS PEUVENT TRAVAILLER POUR DES AGENCES DIGITALES OU ÊTRE INDÉPENDANTS ET OFFRIR LEURS SERVICES À DES ENTREPRISES ET À DES PROFESSIONS LIBÉRALES.

Missions

Comme nous venons de le voir précédemment, les tâches sont diverses. Si l'on entre dans le détail du développement d'un site, différentes étapes doivent être suivies :

1. Élaborer un plan

La première chose à faire avant de développer un site Web est d'établir un plan. Les objectifs les plus courants sont les suivants : « permettre aux utilisateurs d'acheter nos produits sur notre site » et « informer les utilisateurs sur nos produits et services ».

2. Créer un plan du site

Une fois que vous avez défini des objectifs généraux, vous pouvez commencer à planifier la mise en page de votre site. La meilleure façon de procéder est de créer un plan du site, dans lequel vous planifiez simplement les différentes sections et pages qui composeront votre site (à ne pas confondre avec un plan de site XML).

3. Acheter un nom de domaine

L'étape suivante consiste à enregistrer un nom de domaine. Votre nom de domaine est l'URL de votre site. Pour un site Web d'entreprise, la meilleure approche consiste à utiliser simplement le nom de votre entreprise comme nom de domaine.

4. Construiser un backend

Dès que vous connaissez la mise en page de votre site Web, vous pouvez commencer à coder.

5. Construiser un front-end

Après avoir construit le back-end de votre site, la prochaine étape naturelle est de passer au front-end. Il s'agit de configurer

« IL S'AGIT D'UN PROFESSIONNEL QUI SE SPÉCIALISE DANS LE DÉVELOPPEMENT DE SITES ET D'APPLICATIONS WEB. IL CONTRÔLE PRESQUE TOUS LES ASPECTS "EN COULISSE" D'UN SITE WEB, Y COMPRIS SON CODE, SES LIENS SORTANTS ET SON CONTENU, AFIN DE GARANTIR UNE EXPÉRIENCE UTILISATEUR DE QUALITÉ QUI SATISFAIT LES CONSOMMATEURS. LES PERSONNES PASSIONNÉES PAR LA TECHNOLOGIE ET AIMANT LE CODAGE DEVRAIENT DONC APPRÉCIER CE MÉTIER. »

la partie de votre site que les utilisateurs verront lorsqu'ils le visiteront.

6. Lancer un site web

Pas de précipitations, commencez à effectuer quelques tests pour vérifier que tout fonctionne correctement. Mais une fois que vous êtes sûr que tout est en ordre, vous pouvez le rendre public.

Un développeur web peut travailler pour une entreprise ou une agence, ou en tant que freelance pour différents clients professionnels. Un développeur qui s'occupe d'un client local ou basé sur les services doit souvent mettre à jour régulièrement le contenu du site web pour refléter les nouvelles réductions accordées aux clients, les heures d'ouverture et d'autres détails.

En revanche, elle qui s'occupe de plusieurs clients met généralement à jour les sites web moins fréquemment et est libre de procéder à des modifications à plus grande échelle, de créer de nouvelles pages et d'améliorer la sécurité.

Ses responsabilités varieront donc en fonction de votre situation de travail, mais les responsabilités quotidiennes peuvent généralement inclure :

· La conception d'interfaces utilisateur et de menus de navigation
· La communication avec les concepteurs pour mieux comprendre la mise en page préférée du site Web avant de commencer le codage
· Le test des nouveaux éléments du site sur différents moteurs de recherche et appareils
· La migration des éléments du site Web vers des sites réels lorsque les tests sont concluants
· La résolution de tout problème lié au contenu destiné au client ou à la compatibilité du back-end
· La mise à jour des thèmes, des plugins et de la sécurité du site Web afin de refléter les meilleures pratiques actuelles en la matière
· L'optimisation de l'expérience utilisateur
· Etc.

Compétences

Les compétences spécialisées dépendent souvent du type de développeur web que vous souhaitez devenir. Par exemple, les langages frontaux comme HTML et CSS sont nécessaires si vous voulez être un développeur front-end. Pour le back-end, vous devrez connaître des langages comme C++, SQL, Ruby et Python.

Il est surtout très important de se tenir au courant des tendances en étudiant, en assistant à des conférences et en participant à des ateliers pour découvrir ce qui est tendance sur le marché et comment cela peut aider à construire un meilleur site Web.

QUALITÉS

Il est important de maitriser les principaux langages de programmation et de technologies, tels que HTML, CSS, JavaScript et PHP, pour construire les composants fonctionnels d'un site Web ou d'une application. En plus des compétences techniques, il est indispensable de comprendre les principes de l'expérience utilisateur (UX-acronyme de l'anglais « User eXperience »), afin de s'assurer que les sites web que vous créez sont faciles à utiliser et que les internautes trouvent rapidement l'information qu'ils recherchent.

Les compétences supplémentaires, en particulier pour les développeurs front-end, comprennent la conception visuelle, la conception graphique et l'expérience utilisateur. Ces compétences contribuent principalement à déterminer l'apparence d'un site web et la manière dont les utilisateurs interagissent avec lui.

Le codage : Les langages de programmation courants comprennent HTML, PHP, les feuilles de style en cascade et JavaScript pour la conception frontale. Envisagez d'apprendre Python, Java ou Ruby si vous voulez faire du développement back-end.

Le « responsive design » : Les internautes utilisent une variété d'appareils pour consulter les sites Web. Les développeurs doivent être capables de créer des sites qui sont aussi beaux sur les smartphones et les tablettes que sur les écrans d'ordinateur.

Référencement technique : De nombreux facteurs de la conception de sites Web peuvent affecter le classement du site dans les moteurs de recherche. Comprendre comment les moteurs de recherche classent les sites est utile dans le travail d'une développeuse. Sans oublier un critère déterminant : plus une page Web se charge rapidement, meilleure est l'expérience de l'utilisateur !

Conception visuelle : La compréhension des principes de base de la conception, comme l'utilisation des espaces blancs, le choix des polices de caractères et l'intégration d'images, peut améliorer vos possibilités de commercialisation.

Études

Contrairement à une idée reçue, les profils littéraires comme technologiques peuvent très bien devenir des développeurs web. Après le Bac, vous pouvez vous orienter soit vers un BTS Services informatiques aux organisations (option B solutions logicielles et applications métiers) soit vers un BTS Systèmes numériques (option A informatique et réseaux).

Ces programmes sont conçus pour vous aider à acquérir les compétences spécifiques en matière de programmation, de codage et de script dont vous aurez besoin pour réussir dans cette carrière.

Si vous souhaitez aller plus loin, vous pourrez viser la licence avec un Bac + 3 ou un Master Pro avec un Bac +5. Le plus important reste votre détermination.

Mais il est possible d'être développeur web sans suivre un cursus classique, car c'est un métier où les compétences sont plus recherchées que le diplôme. Il existe de nombreuses formations courtes ou longues qu'il convient de choisir sans précipitation…

Quelle école ?

Plusieurs écoles forment à ce métier. Les plus connues sont SUPINFO, EPITECH et Ecole 42.

Mais n'oubliez pas qu'une combinaison d'expérience pratique, de réseautage professionnel et peut-être même un portfolio de travail prêt à être présenté à des employeurs potentiels sont aussi importants que les diplômes.

Quel bac ?

Dans l'absolu, un Bac scientifique est un « plus », mais décrocher un Bac technologique ne vous empêchera pas de devenir développeur web.

Salaire

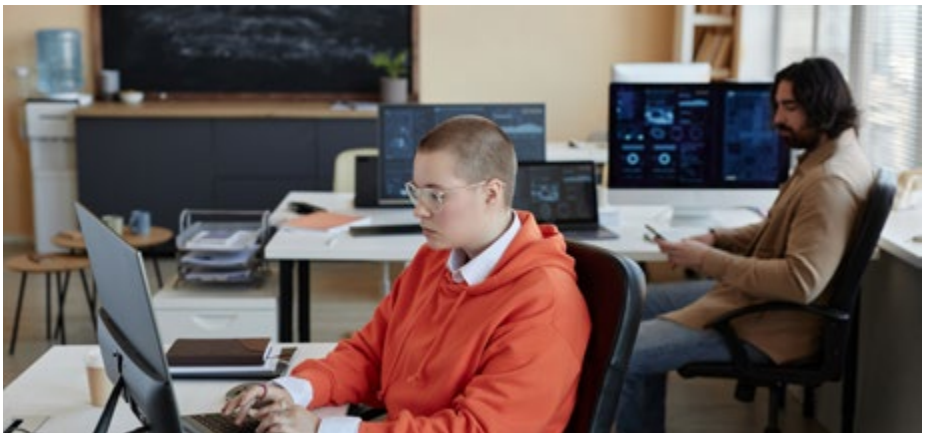
Une jeune développeuse peut prétendre à un salaire de 30 000 euros brut à l'année. Avec plus d'expérience, la rémunération peut atteindre les 50 000 euros par an. En tant que freelance, le taux journalier moyen (TJM) peut atteindre les 300 euros la journée.

Évolution de carrière

De nombreux développeurs web commencent leur carrière avec un seul objectif, généralement être front ou back-end. Ils peuvent ensuite devenir des développeurs complets ou explorer des carrières dans des domaines connexes, notamment la gestion de projet, la programmation informatique ou la conception graphique.

Comment le devenir ?

Le métier de développeuse web est très demandé. De nombreux postes sont proposés. Mais il nécessite souvent des certifications dans plusieurs langages de programmation ainsi que des années d'études supérieures. Toute personne souhaitant devenir développeur web devra combiner une compréhension approfondie de la programmation avec une patience pour le code complexe afin de développer des sites web répondant précisément aux demandes des clients.



THREAT HUNTER

Niveau d'études :	Bac+5
Spé Conseillée :	Scientifique
Employabilité :	Bonne
Salaire débutant :	4 100 €

Code ROME : M1802 - Code FAP : M2Z

LE RÔLE DE CET EXPERT DEVIENT DE PLUS EN PLUS IMPORTANT. LES ENTREPRISES ET LES DIFFÉRENTS ÉDITEURS DE SOLUTIONS DE CYBERSÉCURITÉ S'EFFORCENT DE RESTER À L'AFFÛT DES DERNIÈRES MENACES ET DE METTRE EN ŒUVRE UNE RÉPONSE RAPIDE POUR ATTÉNUER LES DOMMAGES POTENTIELS.

Missions

Ce spécialiste n'a pas pour mission de s'attaquer aux incidents qui se sont déjà produits. Il recherche les cybermenaces qui se cachent dans le « bruit » avant que l'attaque ne se produise.

Il peut être chargé des tâches suivantes :

· Rechercher les cybermenaces et les risques qui se cachent dans les données avant que les attaques ne se produisent
· Recueillir le plus d'informations possible sur le comportement, les objectifs et les méthodes des menaces
· Organiser et analyser les données collectées pour déterminer les tendances dans l'environnement de sécurité de l'organisation

Faire des prévisions pour l'avenir et éliminer les vulnérabilités actuelles.

Anticiper et innover. Ce sont les deux maîtres-mots de la fonction de threat hunter. Ce spécialiste doit en effet adopter une approche proactive pour détecter les menaces de cybersécurité. Il s'appuie principalement sur la méthode scientifique pour tester et valider ses hypothèses.

Le threat hunter enquête, identifie et rend compte des menaces et des modèles qui ne sont pas identifiés par des outils automatisés. Il peut identifier des modèles de comportements adverses et élaborer des profils de menaces à partir de sources publiques de renseignements et d'informations d'origine privée.

Cet expert rend compte de ses conclusions et peut recommander des investigations supplémentaires pour

répondre et remédier aux menaces de sécurité vérifiées. Par contre, il n'intervient pas en cas d'incident. La remédiation n'est pas de sa responsabilité, bien qu'il puisse collaborer avec des équipes de réponse aux incidents.

Compétences

Ce sont des professionnels hautement qualifiés qui possèdent une grande expérience et une connaissance approfondie des outils du métier, tels que les journaux de pare-feu, les journaux de fenêtres, les techniques d'attaque, les systèmes de détection d'intrusion et la gestion des incidents et événements de sécurité (SIEM).

Ils possèdent en particulier une très forte connaissance des environnements informatiques (Windows et Linux/Unix), des vecteurs d'attaque des logiciels malveillants (ou malwares) et des acteurs de la menace. Ils savent quels outils, techniques et procédures rechercher dans un environnement.

Étant donné leur mission, ils doivent avoir une expérience pratique de la criminalistique, de l'analyse des données, de l'analyse du renseignement, de la sécurité des réseaux (maîtrise des différents protocoles, tels que la pile TCP/IP) et des terminaux (ou endpoints).

Outre l'expérience pratique, ils doivent également avoir une connaissance approfondie des méthodes actuelles et passées des logiciels malveillants, des méthodologies d'attaque et des TTP (tactiques, techniques, procédures), de l'ingénierie inverse. Les TTP sont des modèles spécifiques de techniques et d'activités associés à certains cyberadversaires. Des compétences en codage et en langages informatiques sont indispensables pour analyser les journaux, automatiser des tâches et effectuer des analyses de données complexes. Il doit être en effet capable de repérer les schémas inhabituels sur le réseau et de confirmer s'il s'agit d'un faux positif ou d'un logiciel malveillant avancé (attaques de type «Zero-day») qui tente de communiquer avec une partie externe.

Études

Quelle école ?

Il est recommandé d'intégrer une école d'ingénieur en cybersécurité et ensuite de suivre des formations pour obtenir certaines certifications très demandées.

Quel bac ?

Il est recommandé d'avoir Bac +5. Un baccalauréat en technologie de l'information, en informatique ou dans une discipline connexe, permet à ces chasseurs de se familiariser avec les technologies, les théories et les pratiques de base dans ce domaine. Mais il convient ensuite et de suivre es formations très spécialisées.

Salaire

Il varie en fonction de l'entreprise ou du prestataire. Un hunter peut prétendre à une rémunération se situant autour de 50 000 euros brut par an. Quant à un expert senior, son salaire peut atteindre les 150 000 euros brut par an.

Évolution de carrière

Actuellement, il existe une énorme pénurie de talents dans le domaine de la cybersécurité. Les chasseurs de cybermenaces sont des analystes de niveau 3, et trouver des professionnels qualifiés pour ce rôle est un défi. La première évolution possible est donc d'envisager de rejoindre un important MSP ou une grosse entreprise spécialisée dans la cybersécurité. Étant donné ses compétences très pointues, un hunter peut ensuite devenir un chasseur de prime (bug bounty hunter), voire un analyste en réponse à incident.

QUALITÉS

Toutes les compétences ne suffisent pas à devenir un excellent threat hunter. La préparation de rapports de sécurité et de différents documents techniques est une partie essentielle de leur travail. Il doit donc posséder d'excellentes compétences en matière de rédaction technique et de rédaction de rapports. Enfin, il doit posséder quelques compétences non techniques : gestion du stress, analyse, en recherche et résolution de problèmes.

Un certain niveau de raisonnement déductif est également vital, car il doit être capable de formuler des hypothèses raisonnables (par exemple, comment une menace pourrait-elle échapper à un IDS ou « Intrusion Detection Systems » ?) et exfiltrer des données spécifiques) et de travailler à rebours pour rechercher des traces d'une éventuelle intrusion en cours. Il peut utiliser les données collectées avec un outil SIEM (Security Information and Event Management) pour créer des graphiques personnalisés, basés sur son hypothèse, qui l'aideront à reconnaître plus facilement les modèles.

56 MEDIA EXPLOITATION ANALYST

Niveau d'études : Bac+5

Spé Conseillée : Scientifique

Employabilité : Bonne

Salaire débutant : 3 300 €

Code ROME : M1802 - Code FAP : M2Z

TOUT LE MONDE CONNAIT LA SÉRIE LES EXPERTS. DE FINS LIMIERS SONT CAPABLES DE TROUVER LES MOINDRES PREUVES EN DÉCORTIQUANT UN VÉHICULE OU UN APPAREIL. UN MEDIA EXPLOITATION ANALYST PROCÈDE DE LA MÊME FAÇON EN ANALYSANT TOUT TYPE DE SUPPORT : DISQUES DURS D'ORDINATEURS, CLÉS USB, TÉLÉPHONES PORTABLES... SON OBJECTIF : TROUVER DES PREUVES DANS LE CADRE D'UNE ENQUÊTE.

Missions

Elles sont à la fois variées et très précises. Prenons le cas d'une analyse dans le cadre d'une enquête judiciaire. Ses missions sont les suivantes :

· Copier le disque dur du système faisant l'objet de l'enquête : cette étape consiste à faire une copie des fichiers et des dossiers présents sur le disque dur. Cette «image disque» est créée sur un autre support

· Vérification des données copiées : après avoir copié les données du disque dur du système faisant l'objet de l'enquête sur un autre disque dur, ces spécialistes s'assurent que les données copiées sont exactement les mêmes que les originales. Ils doivent vérifier qu'elles ne sont pas altérées d'aucune façon

· Récupération des fichiers supprimés : Les fichiers supprimés par l'utilisateur sur l'ordinateur peuvent être récupérés par ces experts, car dans la majorité des cas les données ne sont pas supprimées définitivement

· Trouver des données dans l'espace libre : le système d'exploitation considère l'espace libre du disque dur comme un espace disponible pour stocker les nouveaux fichiers et dossiers, mais les fichiers temporaires et les fichiers supprimés depuis des années sont stockés ici jusqu'à ce que de nouvelles données soient écrites dans l'espace libre. Les experts recherchent dans cet espace libre pour recréer ces fichiers

De façon plus globale et en dehors d'une affaire judiciaire, les media exploitation analyst peuvent aussi effectuer une analyse des «logs» (journaux), des preuves et d'autres informations (code anormal, données volatiles…) afin de déterminer les meilleures méthodes pour identifier le ou les auteurs d'une intrusion dans un réseau.

Ils cherchent aussi à confirmer ce que l'on sait d'une intrusion et découvrir de nouvelles informations, si possible, après avoir identifié l'intrusion (nécessité d'identifier les techniques dites d'obfuscation) par une analyse dynamique. Cela passe notamment par une analyse de la signature des fichiers.

Sa principale responsabilité est de savoir interpréter et analyser les données de manière continue et de s'assurer qu'aucune d'entre elles n'a été compromise ou modifiée de quelque manière que ce soit. Il doit en effet préserver l'intégrité des preuves conformément aux procédures opérationnelles standard ou aux normes nationales.

Compétences

Ces professionnels doivent avoir une connaissance approfondie des systèmes informatiques et des réseaux, et donc les principaux langages de programmation (Python et C++), les scripts et l'automatisation.

Ils doivent partager une connaissance approfondie de la technologie d'intrusion et des tests de pénétration (appelés «pentest» en anglais) pour pirater les systèmes potentiels des cybercriminels afin d'en reprendre le contrôle et de s'assurer qu'aucun fichier n'a été altéré ou modifié.

Pour une connaissance plus approfondie, OWASP Threats Fundamentals est un excellent moyen d'acquérir une connaissance complète des clauses qui doivent être déterminées et prises en compte dans ce type d'analyse.

Dans le détail, leurs compétences doivent leur permettre de maîtriser le démontage et le remontage d'appareils électroniques tels que des ordinateurs et des périphériques associés. Ils doivent maîtriser l'architecture des disques durs et des types de connexion, mais aussi celle des smartphones qui sont de plus en plus utilisés pour échanger des données sensibles. De façon générale, ce qu'on appelle le renseignement SIGINT (Signals intelligence).

Enfin, les méthodes actuelles d'ingénierie inverse (ou rétro-ingénierie) pour mieux comprendre les techniques modernes utilisées par les attaquants pour exploiter et pénétrer les systèmes vulnérables est un « plus ».

Études

Il est recommandé de suivre un Mastère spécialisé expert forensic et cybersécurité après avoir un diplôme professionnel Bac +5 ou de de M1 avec 3 ans d'expérience.

Quelle école ?

École d'ingénieurs.

Quel bac ?

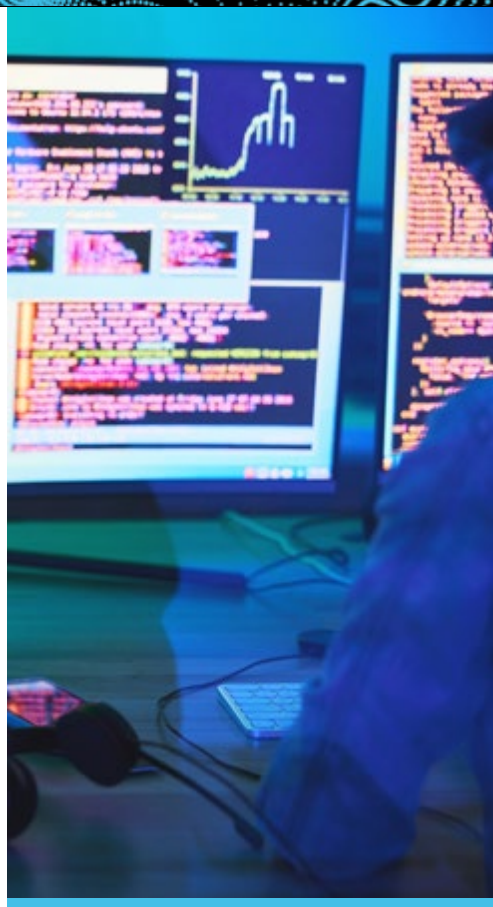
Au lycée, il est recommandé de suivre un cursus basé sur les mathématiques et le numérique.

Salaire

Il peut varier entre 40 0000 euros brut par an pour un technicien débutant pour approcher les 200 000 euros brut par an pour des experts seniors.

Évolution de carrière

Compte tenu de ses compétences, un media exploitation analyst peut évoluer vers d'autres postes comme chercheur en cybersécurité ou bug bounty hunter.



QUALITÉS

La patience et un fort intérêt pour des enquêtes minutieuses sont indispensables. Comprendre les processus et le fonctionnement des différents systèmes d'exploitation, du matériel informatique, des appareils mobiles et des réseaux implique de passer des heures et des heures le nez dans l'unité centrale d'un ordinateur !

57

DÉVELOPPEUR·EUSE FRONT-END

Niveau d'études : Bac+3 à Bac+5

Spé Conseillée : Scientifique

Employabilité : Bonne

Salaire débutant : 2 000 €

Code ROME : M1802 - Code FAP : M2Z

LE RÔLE DE CE PROFESSIONNEL CONSISTE À IMPLÉMENTER DES ÉLÉMENTS VISUELS ET INTERACTIFS AFIN DE RENDRE ATTRACTIF ET PRATIQUE UN SITE INTERNET. IL EST DONC CHARGÉ DE CONCEVOIR LA MISE EN PAGE. OUTRE LES TECHNIQUES ET MÉTHODES DE DÉVELOPPEMENT CLASSIQUES, LE DÉVELOPPEMENT FRONT-END COMPREND ÉGALEMENT LA CRÉATION D'APPLICATIONS MOBILES.

Missions

Il existe deux rôles principaux dans le développement front-end : les développeurs d'interface front-end et les ingénieurs front-end. Bien qu'ils puissent sembler similaires, plusieurs distinctions existent entre les deux.

Les développeurs d'interface front-end (ou concepteurs front-end) prennent des dessins et autres images statiques et les traduisent en pages Web. C'est une tâche importante, car les pages web doivent correspondre aux dessins et s'assurer qu'elles fonctionnent sur différentes tailles d'écran, et en particulier les smartphones (voir ci-dessous la partie compétences sur le responsive design).

Les ingénieurs front-end se concentrent moins sur la conception. Ils s'attachent davantage à rendre le site web fonctionnel et évolutif. Certains ingénieurs front-end font également du travail de conception.

Cette distinction étant faite, les missions de ces développeuses peuvent être regroupées en trois grandes catégories :

· Être responsable de l'écriture d'un code propre et accessible en suivant une approche d'amélioration progressive
· Créer un code ouvert par défaut et facile à réutiliser par d'autres personnes
· Concevoir des logiciels qui répondent aux besoins des utilisateurs et créent des interactions et des relations significatives avec eux

Contrairement au développeur back end (en charge de construire la structure), le développeur front end est en charge de la partie « visible » d'un site internet, autrement dit de son design.

Le développeur front-end est donc en charge :

· Du design et de l'ergonomie du site
· De la compatibilité du site sur les différents supports (responsive design) et navigateurs
· De l'accessibilité des pages (normes W3C)

Ses responsabilités consistent à concevoir, construire et améliorer les logiciels de sites web qui répondent aux besoins des utilisateurs. Son principal défi consiste donc à veiller à ce que les visiteurs du site web puissent interagir facilement avec les pages et le contenu. Pour ce faire, il combine le design, la technologie et la programmation afin de coder l'apparence d'un site web et de s'occuper du débogage.

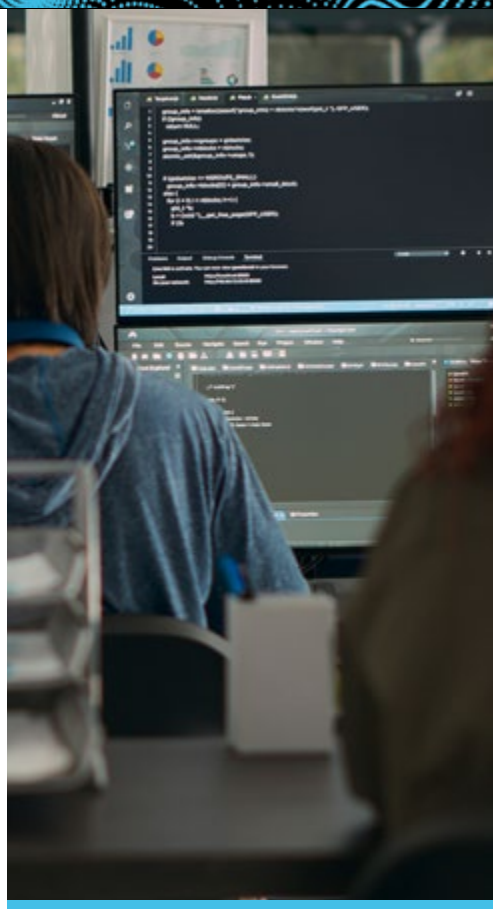
Compétences

Voici quelques-unes des compétences les plus importantes que vous devrez posséder en tant que développeur front-end :

· HTML, CSS et JavaScript : ces trois langages sont essentiels pour quiconque souhaite travailler dans le développement frontal. HTML, CSS et JavaScript travaillent ensemble pour déterminer l'apparence et la fonctionnalité de la page
· Frameworks : ce sont des outils nécessaires pour que JavaScript et CSS fonctionnent comme vous le souhaitez. Il est essentiel de bien les comprendre pour créer des structures de page
· Outils et logiciels pour développeurs : un logiciel tel que le contrôle de version, qui permet de suivre et de contrôler les modifications apportées à votre code source, est essentiel pour vous permettre d'effectuer des changements sans avoir à recommencer. La compréhension de l'utilisation de nombreux outils de développement de logiciels différents est une composante essentielle d'une carrière réussie
· Préprocesseurs CSS : la plupart des développeurs front-end utilisent des préprocesseurs CSS pour ajouter des fonctionnalités au codage CSS, le rendant plus évolutif et plus facile à utiliser. Avant de publier le code sur votre site web, les préprocesseurs CSS le transforment en un code CSS bien formaté qui fonctionne sur une variété de navigateurs, les plus demandés étant LESS et SASS
· Utilisation des API et des services RESTful : un développeur frontal interagit également avec les API et les services RESTful et les utilisera. REST (Representational State Transfer) est une architecture légère qui simplifie les communications réseau, tandis que les API et les services RESTful suivent cette architecture
· Création, maintenance et conception mobile : avec l'augmentation du nombre de personnes utilisant des appareils mobiles pour se connecter à l'internet, il est devenu essentiel que les sites web soient adaptés aux mobiles. C'est pourquoi la plupart des développeurs frontaux créent désormais des designs réactifs ou des designs mobiles pour leurs sites web

Le responsive design modifie la mise en page d'un site web en fonction de l'appareil et de la taille de l'écran, ce qui nécessite parfois de modifier le contenu et les fonctionnalités en fonction de ces facteurs.

Développement sur plusieurs navigateurs : Si votre développement web n'est pas fonctionnel sur l'ensemble des navigateurs disponibles aujourd'hui, vous passez à côté d'une catégorie entière d'utilisateurs potentiels. Si les navigateurs sont assez homogènes, leurs différences peuvent être importantes, notamment en termes d'interprétation du codage. Un développeur web frontal doit comprendre ces différences et les intégrer dans son code.



QUALITÉS

Ces professionnels ont un rôle majeur dans le succès d'un site web. L'une de leurs principales qualités est donc d'être capables de créer des designs attractifs et efficaces. Ils doivent également capables d'analyser les performances côté client d'une page web pour mieux comprendre « l'expérience utilisateur ». Enfin, ils doivent être familiarisés avec les dernières pratiques de référencement (SEO).

Études

Ce métier est accessible dès le niveau Bac +2. Mais la forte concurrence sur le marché de l'emploi et la complexité toujours plus grande des langages web poussent les candidats à augmenter leur niveau de qualifications. Après le Bac, vous pouvez suivre un :

· DUT Informatique
· BTS SN (systèmes numériques)
· BTS SIO (services informatiques aux organisations)

Et si vous voulez faire un Bac+3, vous pouvez suivre une :

· Licence Informatique
· Licence pro Développeur web et multimédia
· Licence pro Métiers du design, parcours : activités et techniques de communication
· Licence pro Métiers de l'informatique : applications web, parcours : développeur full stack

Quelle école ?

Vous pouvez suivre une école d'ingénieurs ou vous orienter vers un IUT.

Quel bac ?

Un baccalauréat général peut convenir, mais il est essentiel d'aimer un peu les mathématiques et les langages informatiques. Le plus important reste la motivation !

Salaire

Le salaire du développeur front-end oscille entre 2 000 euros et 2 500 euros mensuels pour un premier poste, selon le niveau de diplôme du candidat. Par la suite, il augmente sensiblement pour atteindre 4 000 euros par mois environ pour les profils expérimentés.

Mais la rémunération de ces développeurs est moins élevée que celle des développeurs back-end. Ces derniers travaillent sur l'administration d'un site web ou d'une application. Ils s'assurent que tout fonctionne bien et sont en charge du côté serveur des choses, comme les bases de données, le flux de données client-serveur, la logique du serveur, et plus encore.

Leurs exigences professionnelles et leurs responsabilités étant plus complexes que celles d'une développeuse front-end. Il est logique que leur salaire soit plus élevé.

Évolution de carrière

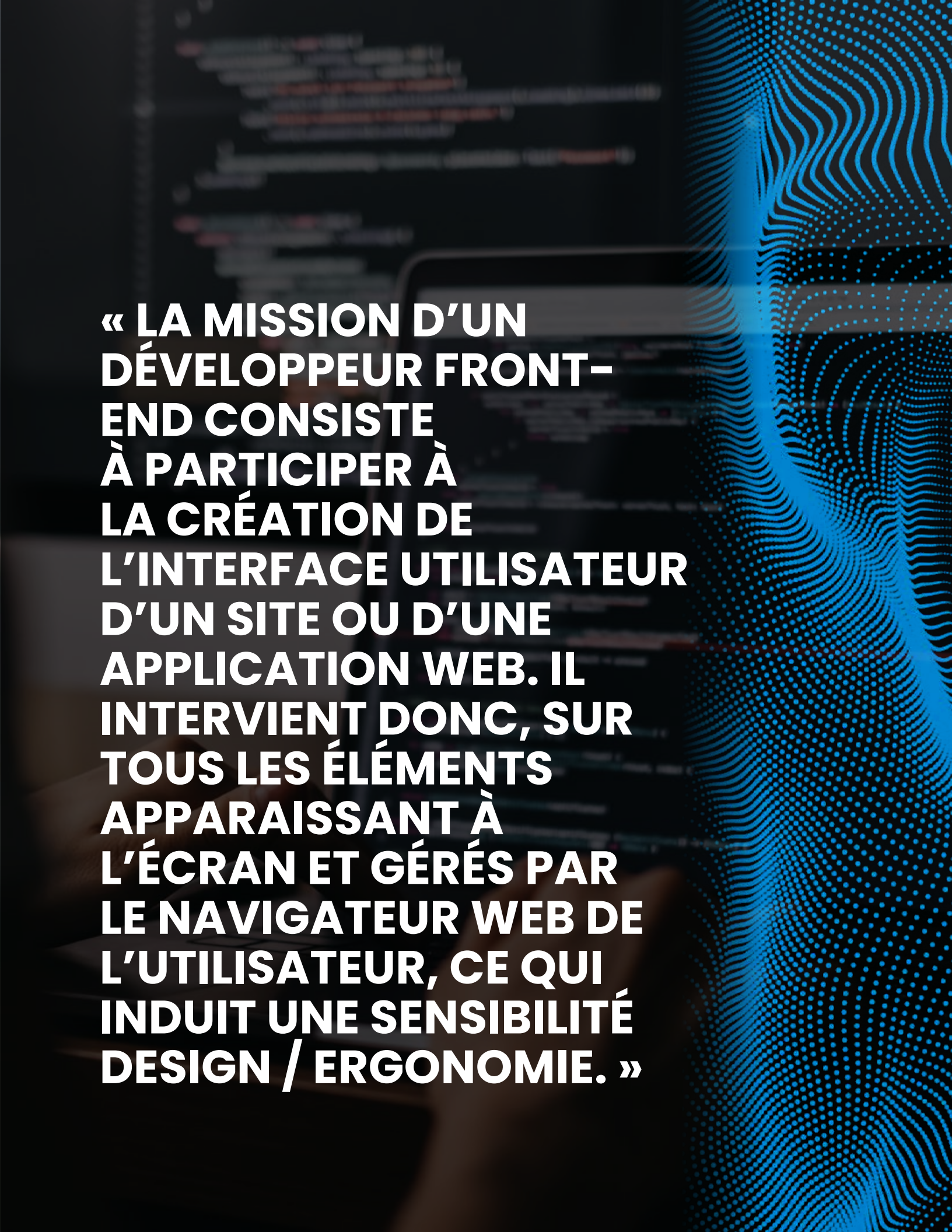
Un développeur front-end peut gagner en responsabilités, notamment managériales en devenant chef d'équipe ou chef de projet.

En validant des formations complémentaires, le développeur front-end peut aussi élargir son champ de compétences : back end, langages informatiques spécifiques…

Comment le devenir ?

Le développement front-end se concentre sur l'interface publique d'un site web ou d'une application – la partie que les utilisateurs voient et avec laquelle ils interagissent. Ce travail impliquant plusieurs autres personnes (notamment des designers, des artistes et des professionnels du marketing), il est essentiel d'être à l'aise avec la communication et le travail en équipe.

« LE RÔLE DE CE PROFESSIONNEL CONSISTE À IMPLÉMENTER DES ÉLÉMENTS VISUELS ET INTERACTIFS AFIN DE RENDRE ATTRACTIF ET PRATIQUE UN SITE INTERNET. IL EST DONC CHARGÉ DE CONCEVOIR LA MISE EN PAGE. OUTRE LES TECHNIQUES ET MÉTHODES DE DÉVELOPPEMENT CLASSIQUES, LE DÉVELOPPEMENT FRONT-END COMPREND ÉGALEMENT LA CRÉATION D'APPLICATIONS MOBILES. »



« LA MISSION D'UN DÉVELOPPEUR FRONT-END CONSISTE À PARTICIPER À LA CRÉATION DE L'INTERFACE UTILISATEUR D'UN SITE OU D'UNE APPLICATION WEB. IL INTERVIENT DONC, SUR TOUS LES ÉLÉMENTS APPARAISSANT À L'ÉCRAN ET GÉRÉS PAR LE NAVIGATEUR WEB DE L'UTILISATEUR, CE QUI INDUIT UNE SENSIBILITÉ DESIGN / ERGONOMIE. »

58

DÉVELOPPEUR·EUSE BACK-END

Niveau d'études : Bac+3 à Bac+5

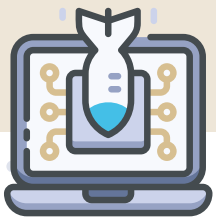
Spé Conseillée : Scientifique

Employabilité : Bonne

Salaire débutant : 2 000 €

Code ROME : M1802 - Code FAP : M2Z

UN DÉVELOPPEUR BACK-END EST RESPONSABLE DE L'ÉCRITURE DES CODES BACK-END DE TOUT SITE WEB ET DE LA MANIÈRE DONT IL VA COMMUNIQUER LORSQUE L'UTILISATEUR DÉCLENCHE UNE ACTION PARTICULIÈRE.



Missions

Les rôles les plus courants en matière de développement back-end sont les suivants :

· Développeur web back-end : le travail le plus courant des développeurs back-end consiste à construire le back-end d'un site web. Ils sont responsables de la création et de la maintenance de la base de données, du serveur et de la logique commerciale d'un site Web.
· Développeurs full-stack : les développeurs full-stack ont une connaissance pratique à la fois du front-end et du back-end d'une pile technologique. Sur les petits projets, ils peuvent être le seul développeur à créer un produit minimum viable. Sur des projets plus importants, ils sont des chefs d'équipe qui aident à l'intégration entre le front-end et le back-end d'une application.
· Développeurs Java : des sites Web aux applications de bureau, les développeurs back-end spécialisés en Java sont très demandés dans le secteur des applications d'entreprise.
· Développeurs de logiciels : selon la description du poste, il peut s'agir d'un autre poste de développeur Java ou de l'un des autres langages énumérés ci-dessus. Les rôles de développeur de logiciels font généralement référence à des applications autres que des sites Web, telles que des applications de bureau.

Dans le détail, voici ce que font de nombreux développeurs back-end au quotidien :

· Construire et maintenir des sites web : La principale responsabilité d'un développeur back-end est d'utiliser divers outils, frameworks et langages pour déterminer la meilleure façon de développer des prototypes intuitifs et conviviaux et de les transformer en sites web. Cela nécessite une compréhension de la fonctionnalité et de la compatibilité multiplateforme
· Rédiger un code de haute qualité : pour produire des applications web durables, les développeurs doivent écrire un code propre et facilement maintenable.
· Effectuer des tests d'assurance qualité : créer et superviser des calendriers de tests pour optimiser l'interface et l'expérience utilisateur, en garantissant un affichage optimal sur divers navigateurs et appareils
· Évaluer l'efficacité et la rapidité : une fois qu'un site Web est opérationnel, et pendant les mises à jour et les modifications, les développeurs doivent évaluer ses performances et son évolutivité, en ajustant le code si nécessaire
· Dépanner et déboguer : être capable de dépanner les problèmes et de les résoudre, tout en les communiquant aux chefs de projet, aux parties prenantes et aux équipes d'assurance qualité
· Former et soutenir : maintenir les flux de travail avec les équipes du client pour assurer un soutien continu, tout en dirigeant la formation et le mentorat des développeurs juniors.

Compétences

Les développeurs back-end doivent posséder une expertise technique, un esprit d'analyse et d'excellentes capacités de collaboration. En tant que développeur web back-end, vous devez être capable de travailler de manière autonome pour concevoir l'infrastructure web.

Langages de programmation : tout développeur back-end doit bien connaître les langages de programmation back-end tels que Python, Java et PHP. Ceux-ci font fonctionner le site web lorsqu'ils sont utilisés aux côtés de bases de données, de frameworks et de serveurs. Python est l'un des langages de programmation les plus populaires, car il est compatible avec l'intelligence artificielle (IA) et l'apprentissage automatique, et permet d'écrire un code clair et logique. Une connaissance de base des langages frontaux HTML, CSS et JavaScript est un atout.

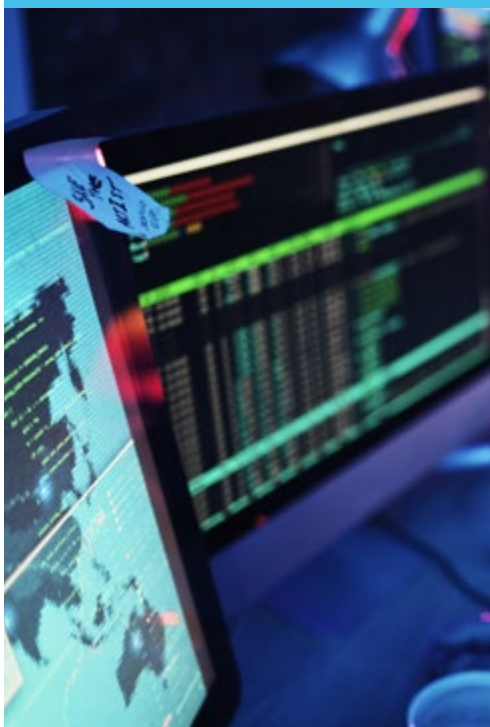
Frameworks : ce sont les bibliothèques de langages de programmation back-end qui aident à construire la configuration du serveur. Ils ont tendance à être liés aux langages de programmation, donc si vous êtes familier avec Python, vous connaîtrez également Flask, Django, ou un autre framework basé sur Python, et ainsi de suite.

Bases de données et serveurs : vous devrez comprendre comment empiler et récupérer les données des bases de données, car la programmation back-end contrôle l'accès à ces informations, y compris le stockage et la récupération. MongoDB et MySQL sont des programmes de base de données populaires.

« LE DÉVELOPPEMENT BACK-END CONSISTE À TRAVAILLER SUR LE LOGICIEL CÔTÉ SERVEUR, QUI SE CONCENTRE SUR TOUT CE QUE VOUS NE POUVEZ PAS VOIR SUR UN SITE WEB. LES DÉVELOPPEUSES BACK-END S'ASSURENT QUE LE SITE WEB FONCTIONNE CORRECTEMENT, EN SE CONCENTRANT SUR LES BASES DE DONNÉES, LA LOGIQUE BACK-END, L'INTERFACE DE PROGRAMMATION D'APPLICATIONS (API), L'ARCHITECTURE ET LES SERVEURS. ILS UTILISENT LE CODE QUI AIDE LES NAVIGATEURS À COMMUNIQUER AVEC LES BASES DE DONNÉES, À STOCKER, COMPRENDRE ET SUPPRIMER LES DONNÉES. »

QUALITÉS

Étant donné leurs différentes missions et responsabilités, ces développeuses back-end doivent être familiarisés avec de nombreux types d'outils et de cadres, y compris des langages tels que Python, Java et Ruby. Ils doivent en effet s'assurer que le back-end fonctionne rapidement et répond aux demandes des utilisateurs du front-end. Mais il est également indispensable d'avoir de la rigueur et être méthodique pour exercer ce métier. De l'autonomie, mais également le goût du travail en équipe, sont nécessaires. Ce qui implique le sens des responsabilités et un relationnel important. Enfin, ces professionnels doivent être créatifs, force de proposition et diplomates pour formuler à leur client leurs idées ou leurs objections.



La base de données stocke et organise les données du client afin qu'elles puissent être facilement organisées et récupérées, tout comme vous pourriez utiliser le stockage en nuage pour vos photos. Cette base de données fonctionne ensuite sur un serveur qui fournit des données sur demande.

Interface de programme d'application (API) : une API est une série de définitions et de règles pour le développement de logiciels d'application. En plus des sites web de navigateur Internet, les entreprises veulent souvent une application mobile pour iOS ou Android. La connaissance de langages de création d'applications tels que JavaScript élargira vos possibilités d'emploi.

Accessibilité et sécurité : vous devez acquérir des connaissances sur les protocoles de réseau et la sécurité du web. Savoir comment sécuriser les bases de données et les serveurs sera essentiel à votre réussite en tant que développeur back-end.

Études

Apprendre le développement back-end vous permet de vous familiariser avec plusieurs langages de programmation, ce qui peut donner un grand coup de pouce à votre carrière. Si vous avez une compréhension de base du fonctionnement de la logique, cela peut s'avérer très bénéfique.

Si ce n'est pas le cas, vous pouvez toujours vous inscrire à un cours de base de langage informatique pour vous familiariser avec les bases. Cela permet de s'assurer que vous ne manquerez de rien à aucun moment une fois que vous vous serez engagé sur la voie de l'apprentissage du développement back-end.

Dès lors, il est recommandé de suivre une école spécialisée en informatique ou une école d'ingénieurs et de suivre ensuite des formations précises et répondant aux besoins des entreprises.

Quelle école ?

Un IUT ou école d'ingénieur.

Quel bac ?

Tout baccalauréat peut mener à ce métier, même s'il faut une affinité pour le numérique et les mathématiques.

Salaire

Un développeur back-end débutant ayant de 1 à 3 ans d'expérience professionnelle perçoit un salaire d'environ 37 120 euros brut par an. Un développeur back-end en milieu de carrière (avec une expérience de 4 à 9 ans) perçoit un salaire moyen de 41 660 euros, tandis qu'un développeur back-end senior avec une expérience de 10 à 20 ans touche un salaire moyen de 55 470 euros. En fin de carrière, un développeur back-end avec plus de 20 ans d'expérience peut toucher un salaire de 58 920 euros.

Évolution de carrière

Étant donné ses compétences et sa polyvalence, une développeuse full stack peut gérer des équipes d'une agence web.

Comment le devenir ?

Un développeur back-end est responsable de l'écriture des codes back-end et de la communication lorsque l'utilisateur déclenche une action particulière. Aujourd'hui, ils sont devenus l'épine dorsale du développement web et sont très demandés par un grand nombre d'entreprises.

CHIEF INFORMATION SECURITY OFFICER (CISO)

Niveau d'études : Bac+5

Spé Conseillée : Scientifique

Employabilité : Très bonne

Salaire débutant : 5 850 €

Code ROME : M1802 - Code FAP : M2Z

VOUS AVEZ À LA FOIS UN SENS INNÉ DE L'ORGANISATION ET UNE CAPACITÉ À ENDOSSER DES RESPONSABILITÉS STRATÉGIQUES ? VOTRE SENS DE LA PRÉVISION STRATÉGIQUE N'A D'ÉGALE QUE VOTRE SANG FROID, MÊME DANS LES SITUATIONS DE CRISE ? VOUS POURRIEZ DONC BIEN ÊTRE LE CHIEF INFORMATION SECURITY OFFICER (CISO) QUE RECHERCHENT DE NOMBREUSES ENTREPRISES POUR CHAPEAUTER LEURS EFFORTS DE CYBERSÉCURITÉ. LE RÔLE DU CISO EST DESTINÉ À DEVENIR DE PLUS CRUCIAL – ET DE PLUS EN PLUS COMPLEXE – AU SEIN DES STRUCTURES EN TOUS GENRES. IL EST DONC PLUS QUE BIENVENU DE FAIRE LE POINT SUR LES TENANTS ET LES ABOUTISSANTS DE CE MÉTIER QUI STRUCTURE TOUTE LA FONCTION DE CYBERSÉCURITÉ AU SEIN DES ENTREPRISES.

Missions

De manière globale, le chief information security officer est tenu de piloter la démarche de cybersécurité en prenant en compte tous les impératifs de prévention, de protection, de détection, de résilience et de correction ayant trait aux systèmes d'information. C'est en partie à lui que revient la tâche de proposer des outils concrets et des processus précis, mais aussi de s'assurer de leur juste compréhension et de leur bonne application par les équipes. Son obsession au quotidien : la sécurité des données.

À ce titre, le CISO assure à la fois un rôle de conseil, d'assistance, d'information, de formation et de mise en alerte, tout particulièrement auprès des directions et des directeurs métiers. Son rôle de préconisation et de supervision sera plus ou moins important en fonction de la taille de l'entreprise au sein de laquelle il opère.

De manière plus détaillée, au jour le jour, le chief information security officer devra assurer un très grand nombre de tâches, selon quatre grands objectifs.

Identifier

Il s'agira en premier lieu :

· De décliner les axes et les objectifs stratégiques cyber pour son périmètre et obtenir la validation de la ou des directions compétentes
· D'identifier les enjeux et les risques de sécurité majeurs sur un périmètre donné
· De décliner et maintenir la politique de sécurité des SI en collaboration avec les parties prenantes

« LE CHIEF INFORMATION SECURITY OFFICER (CISO) DÉFINIT ET ÉTAYE LA POLITIQUE DE SÉCURITÉ DE L'INFORMATION DE SA STRUCTURE. IL EST GARANT DE LA MISE EN ŒUVRE DE CETTE STRATÉGIE ET EN ASSURE ÉGALEMENT LE SUIVI PRÉCIS. »

· De définir un plan d'actions annuel ou pluriannuel sur son périmètre
· De proposer une politique d'investissement concernant les objectifs de sécurité
· D'assurer une veille sur les évolutions réglementaires et techniques de son domaine
· D'assurer les relations avec les acteurs de son secteur d'activité autour de la cybersécurité

Protéger

Sur ce deuxième volet, il s'agira notamment :

· D'organiser les structures de pilotage des plans d'actions de sécurité au sein des entités concernées
· De définir les mesures organisationnelles et techniques à mettre en œuvre pour atteindre les objectifs de sécurité
· De fournir un catalogue de services pour la mise en application de la politique cyber
· De déployer une culture SSI à destination des utilisateurs et décideurs
· D'assurer la promotion des chartes de sécurité informatique
· De conduire des audits périodiques pour évaluer le niveau de sécurité de différents périmètres
· De vérifier la bonne application par les tiers et sous-traitants des règles de sécurité s'appliquant au système informatique de l'entreprise
· D'aider à répondre aux questions des clients éventuels sur les points de cybersécurité, notamment lors d'appels d'offre

Détecter

Ici, l'objectif est :

· De prendre les mesures techniques et/ou organisationnelles permettant la surveillance des événements de sécurité
· D'appréhender les incidents de sécurité et les possibilités de réaction face aux attaques
· D'assurer la mise en place d'un SOC (security operation center)

Répondre

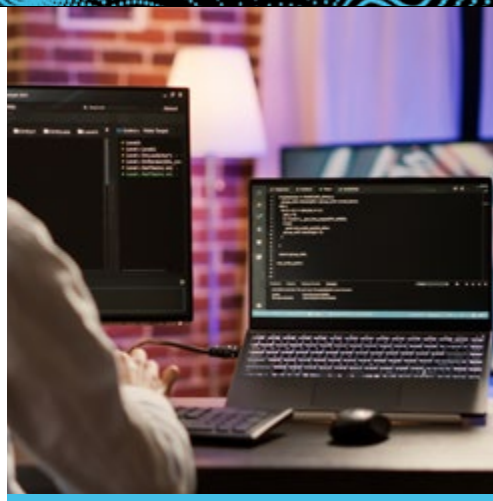
Le CISO doit aussi :

· Veiller à ce que le dispositif de gestion de crise de sécurité soit bien opérationnel
· Contribuer au pilotage de la gestion des incidents et des crises de sécurité, en s'appuyant si besoin sur le CSIRT (Ccomputer security incident response team)
· Préparer et déployer un plan de continuité informatique, dans le cadre du plan de continuité des activités (PCA)
· Préparer et déployer, si besoin, un plan de reprise informatique, dans le cadre du plan de reprise des activités (PRA)
· Proposer une stratégie de cyber-résilience

Rendre compte

Enfin, le CISO doit être prêt à :

· Livrer des rapports réguliers à sa hiérarchie concernant le degré de couverture des risques de sécurité SI
· Représenter l'organisation dans les relations avec les autorités de régulation



QUALITÉS

Arun V. perçoit la fonction de CISO comme une mission très complète : « *Le chief information security officer doit avoir deux grandes qualités, plus complémentaires que contradictoires : il doit à la fois faire preuve d'autorité pour imposer sa vision, parce que c'est comme ça que l'on embarque tout le monde sur une stratégie de sécurité efficace, et il doit être dans le même temps, en continu, un artiste du dialogue. Il doit, à 80 % du temps, se mettre au même niveau que chaque expert technique de la chaîne cyber pour percevoir les adaptations nécessaires dans l'arsenal de défense, vérifier que ses propositions sont bien appliquées ou pressentir les défis à venir.* »
Aussi, le chief information security officer doit principalement faire preuve :
· D'une rigueur à toute épreuve, aussi bien dans l'analyse des éléments techniques que dans la transmission de ses directives et des grandes lignes de sa stratégie
· D'une aisance de contact et d'une grande facilité d'approche pour obtenir rapidement les informations dont il a besoin auprès de ses équipes et communiquer efficacement ses analyses
· D'une aptitude avérée au management et à la gestion d'une grande équipe.

Compétences

On peut identifier deux types de compétences fondamentales qui forment la base du métier de CISO.

Tout d'abord, toute une série de compétences cœur de métier sont à prendre en compte. Un bon CISO doit faire preuve :

· D'une bonne connaissance des métiers et des enjeux propres à son entreprise
· D'une capacité à élaborer des stratégies pointues et cohérentes, et cependant compréhensibles par le plus grand nombre ; à ce titre, ce sont ses compétences pédagogiques qui seront également évaluées ;
· D'une compréhension approfondie des problématiques de cybersécurité et d'une compréhension technique suffisante des types de menace existants
· De même, d'une compréhension technique satisfaisante des outils de réponse aux cyberattaques
· D'une bonne maîtrise des principes d'architecture réseau et de la construction des systèmes d'information
· D'une familiarité avec les principaux domaines des systèmes d'information
· D'une aptitude à la gestion des risques cyber et des situations de crise
· De bases juridiques en matière de droit informatique, avec une spécialisation en sécurité des systèmes d'information et en protection des données
· De connaissances solides en matière de gouvernance, de normes et de standards propres à la cybersécurité, comme les normes ISO 2700X ou les normes sectorielles de type PCI-DSS)

En parallèle, le chief information security officer doit faire preuves de compétences comportementales, centrées essentiellement sur la capacité de convaincre et le sens de l'intérêt général.

Études

La détention d'un Bac +5 est un prérequis minimum pour se positionner sur un emploi de chief information security officer. Les formations alliant bases techniques et aptitude à la gestion de projet seront largement valorisées dans les processus de recrutement. Les cursus intégrant les compétences managériales seront par ailleurs un plus non négligeable.

Salaire

En moyenne, un chief information security officer peut prétendre à un salaire de 5 850 euros mensuels brut dès sa première prise de poste. La maîtrise de certains aspects techniques spécifiques, notamment des langages informatiques clés pour la compréhension de l'environnement cyber de la structure, peut justifier une révision de ce salaire à la hausse. C'est le nombre d'années d'expérience qui permettra de grimper sur l'échelle de salaires, jusqu'à atteindre un plafond aujourd'hui situé à un peu plus de 16 000 euros mensuels brut en France.

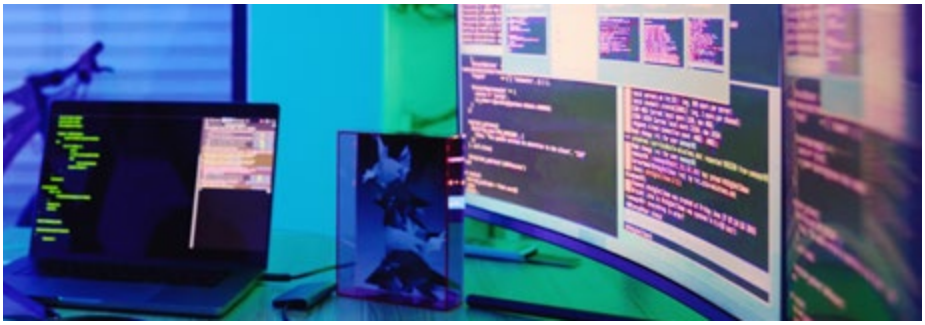
Où travailler ?

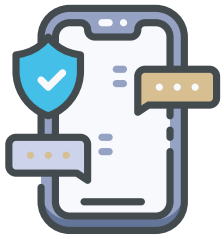
Sans grande surprise, en raison de leur contribution stratégique, les professionnels préparés aux fonctions de chief information security officer peuvent viser des horizons professionnels larges. Ils sont devenus essentiels au sein des grands groupes, dès lors que ces derniers se frottent à la réalité des données. Les CISO trouveront de nombreuses opportunités auprès des acteurs du secteur bancaire notamment, auprès des assureurs en tous genres (des assureurs cyber aux assureurs santé, en passant par toute la panoplie des assurances existantes). Les grands groupes industriels, qu'ils officient dans le secteur automobile, de l'aérospatiale ou de la vente d'appareils électroniques, par exemple, sont tout aussi en demande.

Il faut aussi penser à tous les acteurs du e-commerce, aux start-ups lançant des applications et aux GAFAM développant de nouveaux services. Les opportunités sont larges et toutes les pistes doivent être explorées.

Parmi les entreprises en recherche active de CISO, au cours de la période récente, on trouve notamment :

· Le Groupe Crédit Agricole, AXA Banque, Dogfinance et le groupe BPCE du côté banque et investissement
· Adsearch
· Air France
· Thales
· Atos
· Airbus
· EY
· KPMG
· AXA
· HeadMind Partners
· SQUAD
· Orange Cyberdefense





« C'EST AU CISO QU'INCOMBE LA RESPONSABILITÉ DE COMMUNIQUER SUR LES NORMES DE SÉCURITÉ CYBER AUPRÈS DE TOUS LES COLLABORATEURS. POUR LES AIDER À S'EMPARER DE CES SUJETS ET À INTÉGRER LES POINTS DE VIGILANCE, IL ACCOMPAGNE LA MISE EN ŒUVRE D'OUTILS COMME DES CHARTES NUMÉRIQUES OU DES GUIDELINES DE SÉCURITÉ. CETTE TRANSMISSION ET CETTE SENSIBILISATION PASSENT AUSSI PAR UN CERTAIN NOMBRE D'ACTIONS DE COMMUNICATION DONT IL A LA CHARGE. »

Évolution de carrière

Le CISO en besoin de changement peut tout d'abord envisager de changer de périmètre d'action au sein de son entreprise. De CISO en charge du périmètre industriel, par exemple, il sera possible de passer sans encombre au poste de CISO pour le périmètre commercial.

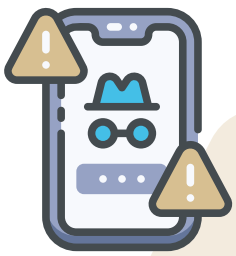
Pour un changement de poste plus radical, l'évolution naturelle consiste à viser un poste de directeur de la cybersécurité. Au sein des grandes entreprises et de certaines administrations, le CISO et le directeur cybersécurité partage d'ailleurs déjà certaines tâches et sont amenés à travailler en étroite collaboration.

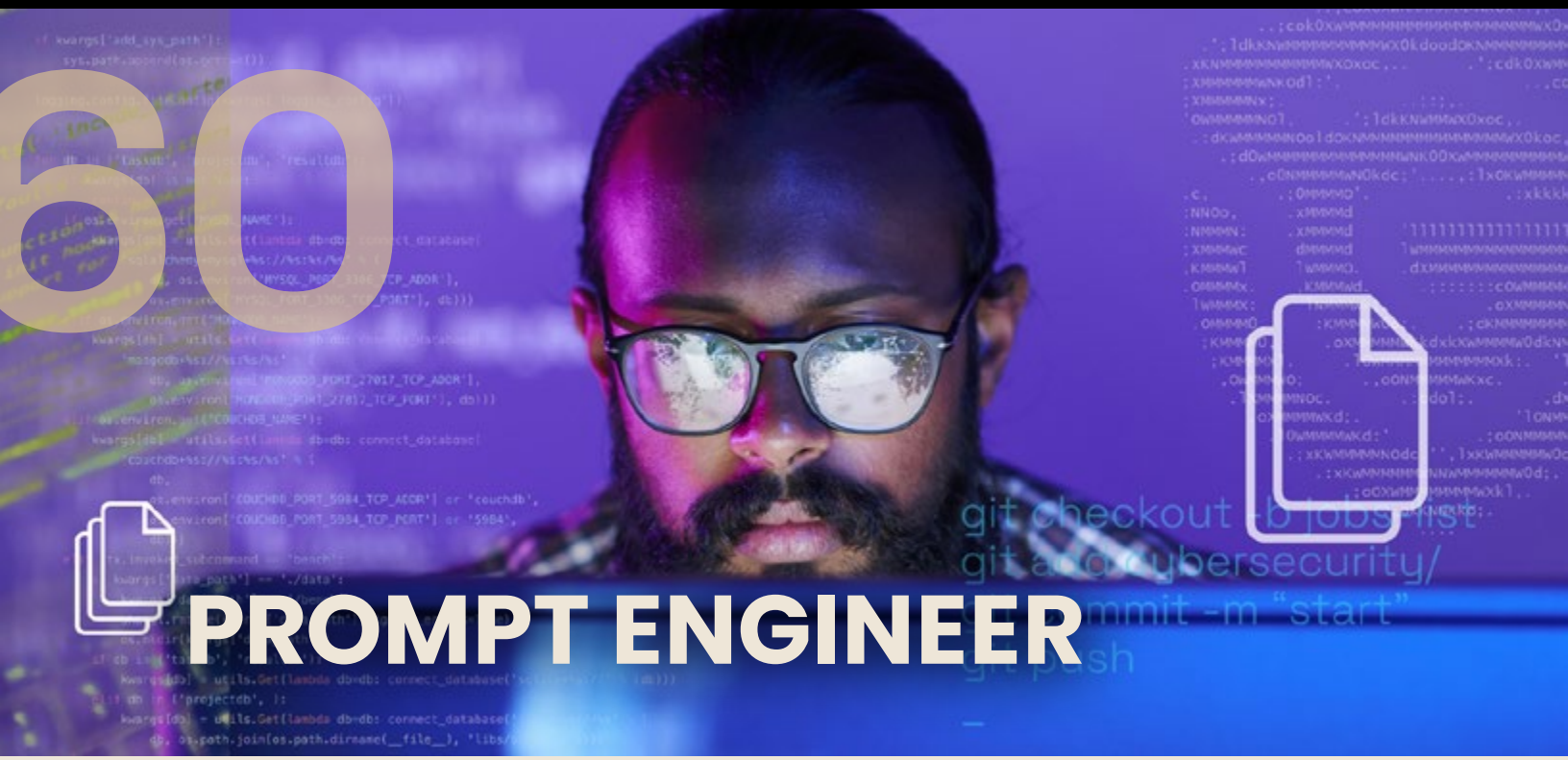
Freelance

Il est tout à fait envisageable de proposer ses talents de chief information security officer sous statut indépendant ou en rejoignant un cabinet externe d'experts en cybersécurité. Il faudra, avant de sauter ce pas, pouvoir justifier de plusieurs années en tant que CISO au sein d'une ou, de préférence, plusieurs structures. Pour un freelance, le tarif journalier moyen oscille entre 700 euros brut environ et 1 300 euros.

Avantages et inconvénients

Pour Arun V., le principal inconvénient de la fonction de CISO peut aussi être perçu comme une motivation : *« Il existe un certain niveau de stress facilement compréhensible, du fait de l'importance stratégique du poste. Le CISO porte une responsabilité majeure dans la mise en place de l'arsenal de cyberdéfense. Sa mission suppose un degré de concentration intellectuelle et d'organisation particulièrement élevés et il doit, malgré les situations délicates, rester un parfait diplomate dans son contact avec les équipes, pour ne pas bloquer les processus. L'avantage qui en découle, c''est un sentiment fort d'utilité et de valorisation pour celui ou celle qui a la chance de piloter les projets cyber à ce niveau ».*





Niveau d'études : Bac+5

Spé Conseillée : Scientifique

Employabilité : Très bonne

Salaire débutant : 5 850 €

Code ROME : M1802 - Code FAP : M2Z

AVEC LA MONTÉE EN PUISSANCE DE L'INTELLIGENCE ARTIFICIELLE, DE NOUVEAUX MÉTIERS SONT APPELÉS À ÊTRE CRÉÉS. LOIN DE CE QUE L'ON POURRAIT PENSER, LA MACHINE NE DEVRAIT PAS COMPLÈTEMENT REMPLACER L'HUMAIN : ELLE DEMANDE À ÊTRE ACCOMPAGNÉE. C'EST DANS CE CONTEXTE QUE LE MÉTIER DE PROMPT ENGINEER SE TROUVE TOUT À COUP MIS EN LUMIÈRE. À L'HEURE DE CHATGPT, CETTE FONCTION ENCORE PEU CONNUE PREND UNE IMPORTANCE TOUTE PARTICULIÈRE. L'OCCASION EST IDÉALE POUR EN FAIRE LE TOUR ET PASSER EN REVUE SES DÉFIS ET SES PROMESSES. FOCUS SUR UN MÉTIER D'AVENIR.

Missions

Au jour le jour, le prompt engineer pose des questions : c'est le cœur de sa mission. *« Le GAFAM pour lequel je travaille à cette heure a besoin d'avancer sur certains projets fortement liés à l'intelligence artificielle. Parfois, ce sont nos partenaires qui ont besoin que je travaille l'IA – que la questionne, en réalité – pour obtenir des éléments de réponse qui vont être décisifs pour certains projets. L'idée, c'est de faire mieux, plus moderne, plus rapide, plus intelligent, en tirant le meilleur parti de l'IA ».*

Mais le prompt engineer a-t-il pour seule mission de faire décoller de « grands projets », des projets novateurs ? *« Non, absolument pas ! L'IA a d'abord et avant tout un intérêt pour les tâches et fonctions du quotidien : en la poussant dans le bon sens, on pourra coder plus vite qu'un développeur bien formé. On pourra gérer plus vite un dossier de subvention, savoir quels partenaires potentiels contacter sans se faire devancer par nos concurrents… On va pouvoir rédiger plus vite certains documents purement formels, des mails aussi bien sûr. Il y a des dizaines et des dizaines de tâches que l'IA peut nous aider à optimiser et automatiser dans leur traitement, et le rôle des personnes comme moi est de s'assurer que les choses vont dans le bon sens. »*

La raison d'être du prompt engineer est de *« faciliter tous les processus possibles au sein de l'entreprise, du plus basique au plus complexe, au service d'un maximum de métiers »*, selon Olivier P. *« Ça, c'est pour son travail à petite échelle. Il a aussi une visée plus grande : il est un des*

maîtres d'œuvre de la modernisation de l'entreprise. C'est lui qui peut la propulser loin dans le monde du futur, pour dire les choses de manière littéraire ».

Compétences

Les principales compétences pour réussir au poste d'ingénieurs spécialiste des requêtes se découpent en un volet technique et un volet comportemental.

Parmi les compétences techniques, on retiendra notamment :

· La maîtrise de la plus large palette de langages informatiques possibles, à adapter selon les besoins et pratiques de l'entreprise
· Une compréhension fine des principaux modèles d'intelligence artificielle
· Une maîtrise des grandes notions d'algorithmie
· Une parfaite aisance sur tous les mécanismes de Développement

Sur un plan plus général, le prompt engineer doit faire preuve d'une grande créativité, afin d'aborder la complexité de l'IA de manière efficiente, et une grande appétence pour la résolution de problèmes complexes.

Études

La fonction de prompt engineer est accessible à partir d'un Bac +5. La validation d'une spécialisation en intelligence artificielle est un pré-requis indispensable pour la majorité des recruteurs. Souvent, des développeurs aguerris passent par une formation spécialisée pouvant aller d'une trentaine à une cinquantaine d'heures pour présenter le niveau de compétence nécessaire.

Soulignons qu'une expérience solide en développement est l'une des voies les plus naturelles pour avoir une légitimité auprès des entreprises.

Salaire

Le salaire moyen d'un prompt engineer qui fait ses armes est estimé à 3 100 euros brut mensuels environ. Les ajustements à la hausse se feront sur la base de ses expériences passées et de la concordance entre ses spécialisations et les besoins de l'entreprise qui l'embauche. Les professionnels les plus expérimentés peuvent espérer toucher jusqu'à 6 800 euros brut par mois en moyenne.

Où travailler ?

La demande de prompt engineers commence à devenir important dans un certain nombre de secteurs liés aux services de santé, à la banque et à l'assurance et à l'industrie automobile notamment. Les entreprises très actives sur le plan informatique, les GAFAM et les experts en cybersécurité se penchent aussi largement sur ces professionnels qui peuvent représenter un très grand atout.

De manière générale, ce sont toutes les structures qui sont engagées dans des processus modernes qui peuvent avoir intérêt à s'attacher les services de ces spécialistes de l'IA.

Récemment, on a pu repérer des offres intéressantes auprès d'acteurs très divers, notamment :

· De grandes références du jeu vidéo, comme Ubisoft, SQUAD ou Gameloft
· Des représentants de la sphère bancaire, comme BNP Paribas, le groupe La Poste ou Natixis
· De grandes références de l'aérospatiale et de l'équipement de pointe, comme Thales
· Des représentants de l'industrie automobile, comme le groupe Renault
· Des cabinets de conseil spécialisés en stratégie numérique et optimisation des systèmes informatiques, comme Eraneos en Suisse ou AI Builders

QUALITÉS

Le prompt engineer se conçoit d'abord et avant tout comme un professionnel disposant d'une très grande capacité d'écoute et d'une hauteur de vue, pour collecter les commentaires de tous les métiers et comprendre – parfois mieux que les professionnels interrogés – leurs besoins réels.
Il doit avoir un côté visionnaire pour « trouver des solutions aux questions que ses collègues ne se sont pas encore posées ».
Au-delà de l'aptitude au dialogue, ce spécialiste de l'IA doit aussi faire preuve d'une grande capacité d'analyse et de synthèse, pour rendre la transmission d'informations aux machines liées à l'IA aussi efficace que possible. Son sens de l'organisation et son esprit structuré doivent être des évidences. La curiosité et le goût pour la recherche sur le temps longs sont d'autres qualités indispensables : l'IA se présente comme une galaxie encore complexe qu'il doit avoir envie d'explorer pour en tirer le meilleur parti possible.

Évolution de carrière

« Il est difficile – et presque un peu dommage – de parler d'évolution de carrière pour un métier tout juste en création. On peut néanmoins dire que les ingénieurs spécialistes de la requête ont de belles années devant eux : leur métier pourra évoluer avec les perfectionnements et les élargissements de l'intelligence artificielle. Plus l'IA deviendra puissante et perfectionnée, plus leur mission devra être consolidée – et on peut imaginer l'apparition de nouveaux métiers pour lesquels les prompt engineers seront particulièrement bien préparés », explique Olivier P.

En raison de leurs bases solides en langages informatiques, en IA et, dans de nombreux cas, en codage, un prompt engineer n'aura aucune difficulté à reprendre des fonctions plus généralistes de développeur. Il pourra aussi proposer ses services en tant que conseiller en cyberstratégie ou en analyste cyber, selon ses spécialités. Les options d'évolution dépendront largement, dans le cas présent, des expériences concrètes de chaque professionnel.

Avantages et inconvénients

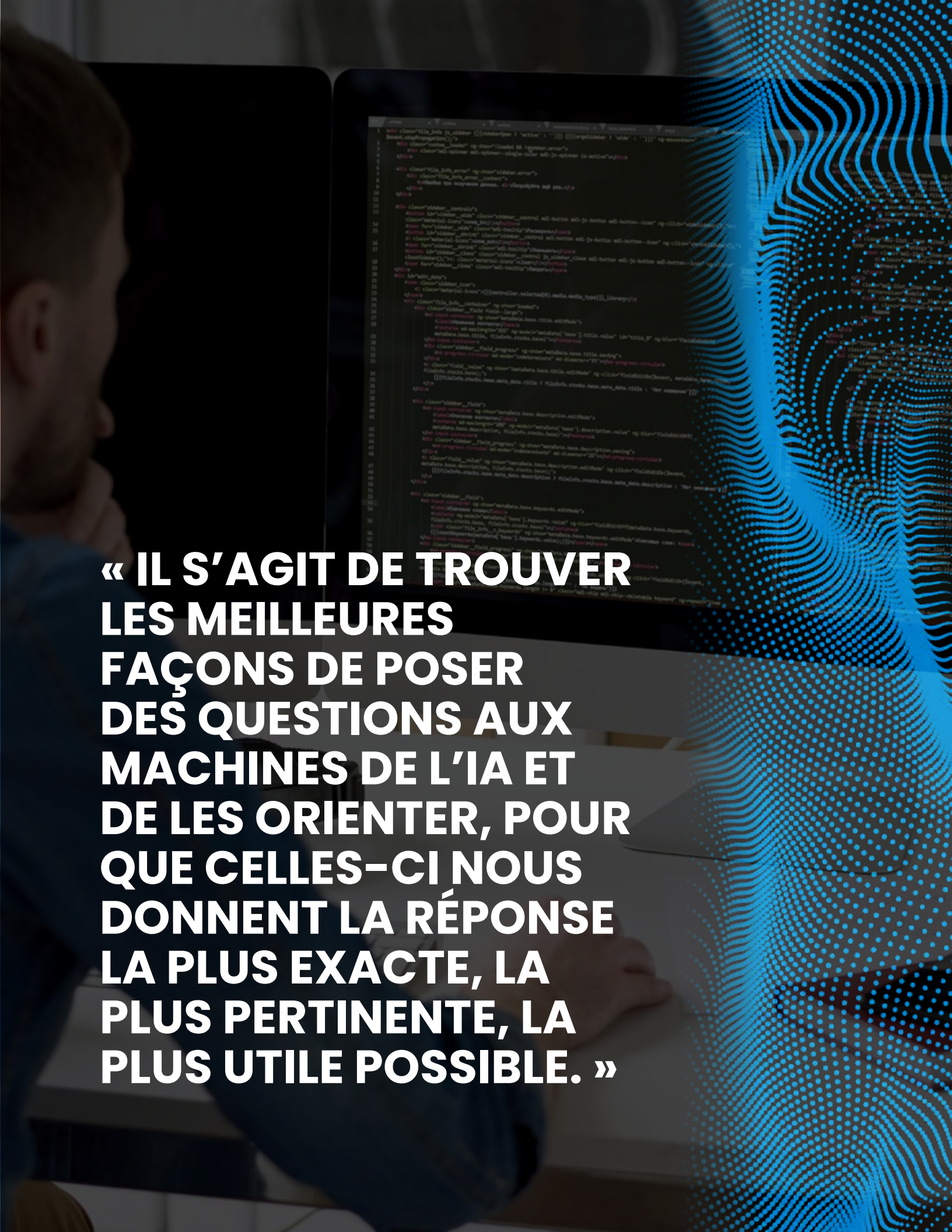
« J'ai du mal à envisager les choses autrement qu'avec beaucoup d'enthousiasme, je l'avoue – et je pense ne pas avoir tort de voir les choses sous cet angle », confie Olivier P. *« Nous sommes sur un métier nouveau, de plain-pied dans la modernité : on parle d'un métier qui surfe sur une grande technologie du futur. Cela veut dire qu'il va y avoir de la demande de la part des entreprises, des perspectives passionnantes de formation pour les nouveaux arrivants sur le marché de l'emploi informatique et cyber, et peut-être aussi de belles opportunités de salaire. Et puis il y a cette idée d'un terrain encore largement inconnu, de pistes à explorer : les prompt engineers devraient être au centre du jeu et devraient ne pas s'ennuyer pendant quelques dizaines d'années ! ».*

Parmi les inconvénients de ce métier en construction, Olivier P. identifie un niveau de responsabilité qui n'apparaît pas forcément au premier coup d'œil, mais qui est bien réel : *« Lorsqu'on veut mettre l'IA au service de nombreux métiers, il faut être sûr qu'on leur fournit des processus bien pensés. Si le prompt engineer oriente mal les choses et qu'il ne se rend pas compte immédiatement que l'IA fournit une réponse biaisée, parce qu'il ne connaît pas assez bien le métier auquel il apporte une réponse, alors nous sommes face à de possibles problèmes en chaîne dans l'entreprise. Et la responsabilité première, ce n'est pas la machine qui va la porter : c'est l'humain, l'ingénieur. Plus qu'un haut niveau de stress, c'est un degré de vigilance et d'attention élevé qui apparaît ».*

L'AVIS DU PROFESSIONNEL

« Je suis un ingénieur des requêtes, littéralement. Et ici, il s'agit des requêtes qui peuvent être faites à la grande reine du moment : l'intelligence artificielle. »

Olivier P.
Prompt Engineer



« IL S'AGIT DE TROUVER LES MEILLEURES FAÇONS DE POSER DES QUESTIONS AUX MACHINES DE L'IA ET DE LES ORIENTER, POUR QUE CELLES-CI NOUS DONNENT LA RÉPONSE LA PLUS EXACTE, LA PLUS PERTINENTE, LA PLUS UTILE POSSIBLE. »

64

ARCHITECTE RÉSEAU

Niveau d'études : Bac+5

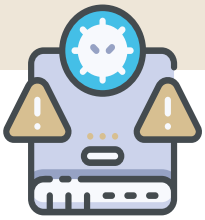
Spé Conseillée : Scientifique

Employabilité : Très bonne

Salaire débutant : 2 850 €

Code ROME : M1802 - Code FAP : M2Z

ON RELIE SOUVENT LES ENJEUX DE CYBERSÉCURITÉ À DES MÉTIERS COMPLEXES – DU MOINS NOUVEAUX, ET DONC COMPLIQUÉS À APPRÉHENDER. IL NE FAUT CEPENDANT PAS OUBLIER QUE CE SONT TOUTES LES PROFESSIONS DE LA CHAÎNE INFORMATIQUE QUI SONT IMPLIQUÉS DANS LA CONSTRUCTION D'UNE CYBERDÉFENSE EFFICACE. CETTE DERNIÈRE PASSE NON SEULEMENT PAR LA MISE EN PLACE D'UN CERTAIN NOMBRE D'OUTILS, MAIS AUSSI D'UNE CULTURE DE LA SÉCURITÉ. LES ARCHITECTES RÉSEAU FONT PARTIE DE CES MÉTIERS ESSENTIELS À LA MISE EN PLACE DE LA BONNE INFRASTRUCTURE INFORMATIQUE – CELLE SUR LAQUELLE REPOSERA TOUTE L'ACTIVITÉ DE L'ENTREPRISE. IL EST IMPORTANT DE RAPPELER POURQUOI CE POSTE RESTE CRUCIAL À L'HEURE ACTUELLE, QUELS EN SONT LES ENJEUX ET QUELLES SONT LES QUALITÉS NÉCESSAIRES POUR L'EXERCER.



Missions

L'architecte réseau peut être amené à réaliser des tâches très variées. On compte notamment sur lui pour :

· Mettre en place les réseaux LAN, WiFi ou VPN, par exemple, en fonction des besoins concrets de l'entreprise
· Associer à ses réseaux les outils nécessaires au bon fonctionnement du business : messagerie, site internet, intranet, lignes téléphoniques, ...
· Identifier les besoins et en chiffrer le déploiement en fonction des contraintes techniques comme le débit ; à ce titre, il pourra être amené à choisir différents protocoles de communication
· Négocier les contrats de fourniture avec les prestataires
· Procéder à des audits de sécurité, de fiabilité et de rapidité sur les réseaux de télécommunications
· Prendre part aux tests sur le matériel informatique
· Proposer des solutions pratiques en cas de surcharge des systèmes
· Résoudre en partie les bugs et prendre le lead sur les actions correctives
· Rédiger la documentation technique relative aux réseaux
· Assurer une veille technologique
· Avancer des plans d'évolution du réseau en fonction des innovations technologiques à venir et des types de cyberattaques identifiés

Les responsabilités de l'architecte réseau peuvent être découpées en trois grands volets.

Il lui revient tout d'abord d'analyser le réseau existant. Les premières questions qu'il doit se poser concernent l'utilité du réseau : à quoi va-t-il servir et qui va l'utiliser ? Il lui faut bien comprendre comment circule l'information dans l'entreprise et comment elle pourrait mieux circuler. Pour cela, l'architecte réseau doit faire le bilan des besoins techniques exprimés par les différentes équipes métier. C'est sur lui que l'on compte également pour penser la connexion entre les différents points du système informatique ou pour la création d'un réseau intranet ou d'une messagerie électronique, par exemple. Compte tenu des nouveaux enjeux cyber, on attend de sa part qu'il intègre dès le départ de son travail un souci des points de cybersécurité.

Sur la base des besoins qu'il a identifiés, l'architecte a la charge de sélectionner et tester différents types d'architecture. C'est lui qui détermine la configuration du réseau (en boucle ou en étoile) et les fonctionnalités générales, en prenant bien en compte les contraintes de débit. « *L'un de ses objectifs est de réussir à intégrer de nouvelles technologies et de nouveaux appareils plus modernes à la base existante, afin de perfectionner le réseau et d'augmenter sa protection* », explique Yann L.

L'architecte réseau assume aussi un rôle d'aide et de conseil auprès des agents techniques. Dans certaines configurations, il endosse même le rôle de chef d'équipe. Il lui incombe de fixer les plannings et les budgets en fonction de toutes les contraintes existantes, qu'elles soient financières, techniques ou réglementaires.

Enfin, il supervise les relations avec les fournisseurs et négocie les contrats au meilleur coût. Il peut également être amené à rédiger des appels d'offres et à en assure le suivi.

Compétences

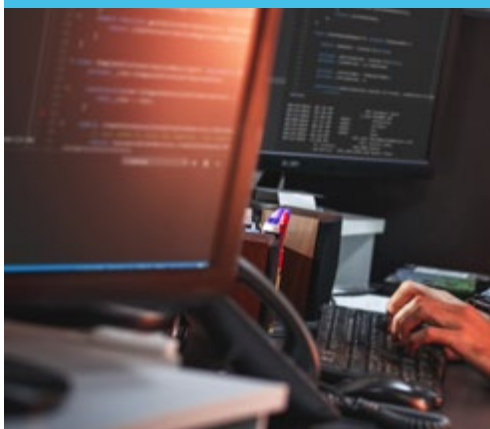
Pour bien aborder ses fonctions, l'architecte réseau doit notamment avoir :

· Une très bonne connaissance des outils liés aux réseaux routeurs et aux commutateurs (Cisco, Juniper, Arista, par exemple) et aux pare-feu (Fortinet, Palo Alto, Checkpoint…)
· Une excellente maîtrise des réseaux LAN, MAN, WAN, Wifi et Data center
· Une excellente maîtrise des protocoles et normes réseau (protocole routés, protocoles de niveau 2, routage statique et dynamique, protocoles sécurisés, AAA…)
· Une bonne connaissance des principaux éditeurs ou environnements existants
· Une bonne connaissance des technologies software-defined
· Une grande familiarité avec les notions de sécurité informatique (pare-feu, authentification, protocoles sécurisés…)
· Des notions de programmation, notamment pour l'automatisation (Python, Ansible)
· La maîtrise des certifications recommandées

La capacité à utiliser des outils de virtualisation comme Vmware ESXI ou Citrix/XenServer est un grand plus.

QUALITÉS

L'architecte réseau doit faire preuve de très bonnes capacités de dialogue et de communication. *« Ces qualités sont indispensables dans un métier où l'on peut être confronté à un grand nombre de projets et de clients. Il faut savoir les écouter pour bien recueillir les besoins. Mais la capacité de communication, c'est aussi bien savoir se faire comprendre lorsque l'on formule ses interrogations ou qu'on présente sa solution »,* explique Yann L. La force de conviction est une autre qualité souvent citée : dans la moitié des cas traités, l'architecte réseau doit en effet se prêter à un exercice d'explication et faire accepter ses choix. L'esprit de synthèse est un autre atout indispensable. *« C'est ce qui permettra à cet architecte pas comme les autres de bien appréhender l'organisation du réseau de manière globale et de prendre le recul nécessaire pour le façonner comme il se doit. Dans cet exercice, il doit aussi faire preuve d'une certaine créativité, qui ne remet cependant pas en cause le sens de la rigueur et de la méthode ! »,* selon Yann L.



L'AVIS DU PROFESSIONNEL

« Avec le grand phénomène de dématérialisation, on a de plus en plus tendance à parler d'architecte cloud plutôt que d'architecte réseau. Quel que soit le nom retenu, opérer les bons choix et assurer une bonne structuration sur le cloud est devenu une tâche à part entière de l'architecte réseau, dont la mission se modernise. »

Yann L.
Architecte réseau

Études

Le Bac +5 est le minimum requis pour les architectes réseau. La plupart des professionnels de cette branche ont validé un diplôme d'ingénieur en informatique, en choisissant une option « Réseaux et télécommunications ».

Priorité aux profils expérimentés

Il faut noter que les recruteurs ont tendance à recruter assez peu de jeunes diplômés à des postes d'architecte réseau. La bonne tenue de la structure du réseau étant une base primordiale pour le bon fonctionnement de la structure, on préfère retenir, en règle générale, des profils expérimentés.

Pour faire la différence et retenir l'attention, il peut être intéressant de dépasser le Bac +5 pour ajouter des spécialisations supplémentaires. *« Sur le CV des candidats, il n'est pas rare de voir apparaître Bac +6, avec un Master spécialisé en systèmes de communication et réseaux, par exemple »,* précise Yann L.

Salaire

Un architecte réseau débutant peut espérer un salaire minimum de 2 850 euros mensuels brut en moyenne. Souvent, ce salaire d'entrée est cependant légèrement supérieur : il oscille entre 3 000 et 3 200 euros brut, dès lors que la structure qui emploie n'est pas une toute petite entreprise. En fin de carrière, il est rare de voir ces professionnels se situer sous la barre des 4 650 euros mensuels brut. Les chiffres peuvent néanmoins grimper pour atteindre environ 5 850 euros brut environ.

Où travailler ?

Historiquement, les entreprises de services du numérique (ESN) et toutes les structures liées à l'univers des télécoms sont les premiers employeurs d'architectes réseau. Mais il ne faut pas oublier que les grands acteurs de l'industrie ont eux aussi des besoins importants sur ce point, tout comme les entreprises du secteur des services au sens large. Les administrations, elles aussi, postent régulièrement des offres d'emploi. On peut dire, de manière très générale, que les architectes réseau peuvent réussir à proposer leurs services auprès de toute structure ayant des besoins en informatique et en sécurité importants.

Parmi les structures régulièrement à la recherche d'architectes réseau, on a pu voir se démarquer, au cours des derniers mois :

- SPIE, leader européen des services multi-techniques dans les domaines de l'énergie et de la communication
- Stellantis, spécialiste de l'automobile
- Airbus
- Le groupe audiovisuel Banijay
- Le ministère de la Défense et le ministère de l'Intérieur
- Facebook France

Les cabinets de conseil en recrutement de cadres, experts et managers Michael Page et AdSearch mènent eux aussi des recherches très actives autour de ce métier.

Évolution de carrière

En accumulant de l'expérience, l'architecte réseau peut se rapprocher de fonctions plus importantes, dans la ligne de ses compétences. Selon l'entreprise dans laquelle il évolue et ses besoins, il peut ainsi devenir responsable des réseaux. À un niveau plus élevé et plus élargi, il peut devenir directeur des systèmes d'information ou responsable de la sécurité des systèmes d'information.

« Je vois de nombreux architectes réseau évoluer vers un poste plus englobant de directeur technique. C'est l'occasion de s'occuper de sujets davantage transverses. Les bons architectes réseau sont aussi souvent repositionnés sur des missions ayant trait au cloud – avec des enjeux de sécurité forts », confie Yann L.

Avantages et inconvénients

Pour Yann L., les aspects valorisants du métier et les tensions qui lui sont inhérentes sont assez évidents. *« Si le réseau ne tient pas debout, si les bases ne sont pas bien posées, rien n'est possible pour l'entreprise – pour aucune des équipes. Il y a donc une responsabilité beaucoup plus grande que ce que l'on pourrait imaginer pour l'architecte réseau. Et qui dit responsabilité, dit deux sentiments, deux dimensions : la responsabilité, c'est le fait d'être valorisé dans ce que l'ont fait, mais c'est aussi une pression en toile de fond, en permanence. Si quelque chose ne va pas, vous êtes le premier à devoir réagir – et dans ces cas de crise et d'urgence, il faut faire preuve d'une belle résistance au stress, d'un esprit méthodique indéfectible et d'une réactivité pleine. »*

62 ADMINISTRATEUR·RICE RÉSEAU

Niveau d'études : Bac+3

Spé Conseillée : Scientifique

Employabilité : Très bonne

Salaire débutant : 2 650 €

Code ROME : M1802 - Code FAP : M2Z

LA CROISSANCE EXPONENTIELLE DES CYBERATTAQUES ET LEUR PERFECTIONNEMENT PERMANENT NE CONDUIT PAS UNIQUEMENT À LA CRÉATION DE NOUVEAUX MÉTIERS AXÉS SUR L'EXPERTISE EN CYBERSÉCURITÉ. C'EST L'ENSEMBLE DES MÉTIERS DE LA PYRAMIDE INFORMATIQUE QUI SONT APPELÉS À SE RÉINVENTER, EN AJOUTANT DE NOUVELLES COMPOSANTES À LEURS MISSIONS D'ORIGINE. LA FONCTION D'ADMINISTRATEUR RÉSEAU EN FAIT PAS EXCEPTION ET RÉPOND À CE SCHÉMA. QUELS AJUSTEMENTS SONT OBSERVÉS, POUR COLLER AU PLUS PRÈS DES EXIGENCES DE CYBERDÉFENSE ? ET COMMENT, AU JOUR LE JOUR, CETTE FONCTION INFORMATIQUE CLÉ MET-ELLE TOUTE UNE ENTREPRISE SUR LES BONS RAILS ?

Missions

Les tâches principales que doit prendre en charge l'administrateur réseau sont les suivantes :

· Assurer le câblage physique du réseau et son bon routage
· Garantir la bonne circulation des informations immatérielles

On retient deux autres missions ayant pris une importance primordiale dans un contexte de multiplication des cyberattaques :

· Assurer la sécurité du réseau
· Gérer les différents comptes utilisateurs et droits d'accès – un sujet directement lié à celui de la cybersécurité

Un travail de prévention et de vigilance de premier plan

La mise en place des comptes utilisateurs et des droits d'accès peut sembler relever des « tâches basiques » du travail informatique. Il n'en est rien. L'administrateur réseau a une responsabilité essentielle sur ce terrain. Il faut rappeler que, sur la période 2019-2021, le piratage de compte était la deuxième attaque cyber la plus courante, selon diverses études menées par les agences de cybersurveillance comme l'ANSSI (l'Agence nationale de la sécurité des systèmes d'information) ou par Cybermalveillance.gouv.fr.

Dans le cas d'un piratage de compte, les hackers se concentrent sur le fait de cracker le mot de passe d'un compte

de messagerie, d'un accès à un compte bancaire ou du compte administrateur du site d'une entreprise.

L'architecte réseau veille cependant aussi à empêcher les cas d'appropriation de compte. Dans ce cas de figure, les attaquants accèdent au compte utilisateur d'un individu en se faisant passer pour un contact proche, un collègue ou un client, dans la plupart des cas. En général, la récupération des informations se fait par e-mail ou par le biais d'applications basées sur un proxy, proposant la vérification de l'identité en un clic. Pour maximiser la portée de l'opération, le cyberattaquant tentera, à l'aide de bots, de trouver la correspondance entre les données utilisateur obtenues et différents sites web : services bancaires, plateformes de vente en ligne. On parle aussi d'« usurpation d'identité cyber ».

Compétences

Pour bien aborder ses fonctions, l'administrateur réseau doit avoir, sans surprise, de très bonnes compétences en informatique. Ses connaissances doivent être tout aussi solides en matière :

· De réseaux, pour bien gérer tous les points relatifs au câblage, aux protocoles de routage, à la cybersécurité et à la gestion des droits d'accès
· De systèmes d'exploitation, puisque c'est en passant par ces derniers que les utilisateurs finaux accéderont au(x) réseau(x)

« Il faut aussi de bonnes prédispositions pour la gestion de projet », précise Sylvia R., architecte réseau. *« Sans oublier une bonne dose de curiosité, parce qu'il faut assurer la veille des évolutions technologiques en cours, en parfaite autonomie, et aussi surveiller les normes de sécurité informatique à respecter. C'est de cette manière que l'on sera capable d'apporter les meilleures solutions possibles à son entreprise ».*

Études

Le Bac +3 est le minimum requis pour les administrateurs réseau. Les entreprises ont cependant de plus en plus tendance à recruter des Bac +5 avec une forte spécialisation en Sécurité des réseaux. Ce changement d'approche n'est pas surprenant, compte tenu de l'importance des enjeux de cybersécurité.

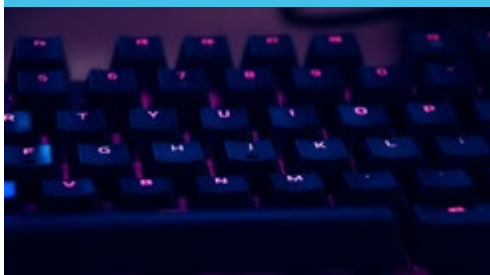
Salaire

Un architecte réseau débutant peut viser un salaire minimum de 2 650 euros mensuels brut environ. Il s'agit là d'une moyenne : cette rémunération peut être revue légèrement à la baisse (pour atteindre 2 500 euros) ou légèrement à la hausse (dans la limite de 2 750 euros) en fonction du profil du candidat (ses études, ses spécialisations, ses formations et ses expériences). En fin de carrière, un architecte réseau peut toucher environ 4 550 euros brut par mois. Une fois encore, une fourchette de négociation est tout à fait possible.

« L'ARCHITECTE RÉSEAU EST LA PERSONNE EN CHARGE DE CONCEVOIR LES RÉSEAUX INFORMATIQUES ET LES RÉSEAUX DE COMMUNICATION DONT A BESOIN UNE STRUCTURE POUR BIEN GÉRER SES COMMUNICATIONS, EN INTERNE COMME EN EXTERNE. C'EST LUI QUI SUPERVISE LA MISE EN PLACE DE CE RÉSEAU. »

QUALITÉS

Pour Sylvia R., *« il est évident qu'il n'y a pas de bon administrateur réseau sans un bon sens pratique. Il faut aussi faire preuve d'une grande réactivité, dans toutes les situations, et d'un goût pour les problèmes complexes et a priori inédits. En tant qu'administrateur réseau, vous vous retrouverez souvent face à une situation que vous n'avez jamais vue auparavant. Et là, c'est la réactivité qui compte pour 1000 points ».* Dans la mesure où l'administrateur réseau doit proposer un matériel qui répond précisément aux besoins d'utilisateurs très différents, l'aptitude au dialogue et de bonnes qualités relationnelles sont indispensables. Ce sont ces qualités qui permettront également de bien gérer les situations de tension, voire de crise.



Où travailler ?

Les administrateurs réseau peuvent compter sur un horizon extrêmement vaste de débouchés. Partout où un réseau a été mis en place, on a besoin d'un administrateur pour l'entretenir et l'ajuster. Or, nous l'avons déjà évoqué : à l'heure actuelle, il n'existe quasiment plus aucune entreprise ne disposant pas de son propre réseau. À travers tous les secteurs, pour toutes les tailles d'entreprise, il existe un besoin réel.

Pour les professionnels en quête de responsabilités importantes, on pourra conseiller de s'orienter vers des entreprises avec de gros enjeux de cybersécurité. C'est le cas de toutes les structures qui touchent aux services du numérique (les fameuses ESN), les structure de services de santé, le secteur de la banque et de l'assurance, les médias, les entreprises de e-commerce, les administrations et bien d'autres encore.

Parmi les structures régulièrement à la recherche d'architectes réseau, on a pu voir se démarquer, au cours des derniers mois :

· Le Groupe La Poste
· EDF
· SPIE, leader européen des services multi-techniques dans les domaines de l'énergie et de la communication
· Le ministère des Armées et Pôle Emploi, du côté des structures publiques
· BNP Paribas et AXA, pour la banque et l'assurance
· L'Hôpital Pellegrin de Bordeaux

Évolution de carrière

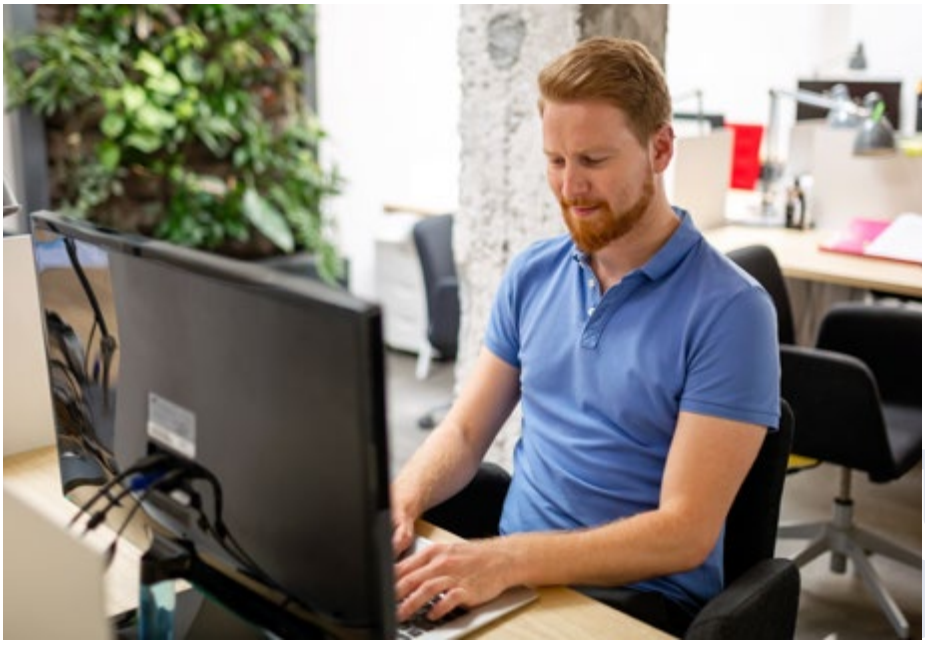
Pour Sylvia R., l'étape la plus naturelle après plusieurs années d'expérience en tant qu'administrateur réseau est assez évidente : *« Lorsqu'on a acquis une connaissance très précise des mécanismes du réseau – de différents types de réseau, on a les bonnes cartes en main pour passer à un poste, non plus de gardien, mais de constructeur en quelque sorte. Mon but, personnellement, est de passer relativement vite sur un poste d'architecte réseau. »*

Il est aussi envisageable de se positionner comme consultant informatique indépendant. Pour se lancer sur cette voie, il est néanmoins recommandé d'avoir une spécialisation forte sur trois sujets au minimum et de pouvoir apporter une compréhension transversale des réseaux et des systèmes informatiques.

Avantages et inconvénients

« Lorsqu'une panne de réseau intervient, le risque est que les collaborateurs – un certain nombre d'entre eux du moins – vous perçoivent comme la personnification du problème. En d'autres termes, il n'y a pas de problème technique : en tant que responsable du réseau, c'est vous, le problème. Je sais que nous, les administrateurs réseau, nous pouvons être fréquemment pris dans ce genre de situations peu agréables. Pour éviter de créer de nouveaux problèmes (humains) et avoir la concentration suffisante pour gérer le problème technique, il faut alors savoir faire preuve de beaucoup de sang-froid, de beaucoup de patience et de beaucoup de diplomatie. Et ce n'est pas toujours facile », explique Sylvia R. *« Il ne faut pas oublier de mentionner les phases de maintenance : il y a un côté répétitif qui peut entamer la motivation. Mais c'est comme dans tout métier : certaines tâches sont moins stimulantes que d'autres. On se rattrape largement avec les phases de mise en place de projet. Là, il y a de la stimulation intellectuelle ».*

Quelles seraient les contreparties positives ? *« Je pense que l'on peut dire que l'administrateur réseau a une fonction centrale dans l'entreprise. En cas de problème, on fait basculer pour vous une grande responsabilité. Au jour le jour, il y a aussi le sentiment d'être valorisé. C'est un peu vous qui faites en sorte que la maison tient debout ! Et puis, de mon côté, j'essaie d'aborder les grosses crises comme un casse-tête, un défi de rapidité et d'ingéniosité, avec ce que cela peut avoir de ludique – c'est une façon de valoriser son poste aussi ! ».*



Niveau d'études : Bac+3

Spé Conseillée : Scientifique

Employabilité : Très bonne

Salaire débutant : 2 500 €

Code ROME : M1802 - Code FAP : M2Z

VOUS AVEZ CE QU'IL FAUT D'INTUITION ET DE VIRTUOSITÉ TECHNIQUE POUR ANTICIPER LES PROBLÈMES DANS UN SYSTÈME INFORMATIQUE, QUEL QUE SOIT SON DEGRÉ DE COMPLEXITÉ ? VOUS AVEZ LE SENS DU DÉTAIL ET LA CAPACITÉ À TRAVAILLER EN PARFAITE AUTONOMIE ? LE POSTE D'ADMINISTRATEUR SYSTÈME EST DONC PEUT-ÊTRE FAIT POUR VOUS. TOUTES LES ENTREPRISES SONT À LA RECHERCHE D'AS DE L'INFORMATIQUE À QUI LES TÂCHES D'ORGANISATION ET D'ORCHESTRATION LOGISTIQUE NE FONT PAS PEUR. NOUS VOUS PROPOSONS DE DRESSER LE PORTRAIT-ROBOT DE L'ADMINISTRATEUR SYSTÈME ET DE METTRE EN LUMIÈRE CE MÉTIER ESSENTIEL DANS LA GALAXIE INFORMATIQUE.

Missions

Parmi les missions principales de l'administrateur système, on peut notamment retenir :

· Les tâches d'installation, de paramétrage et de maintenance globale des infrastructures informatiques
· La rédaction d'un cahier des charges servant de bases aux mises à jour des outils existants ou à la mise en place de nouveaux outils
· L'assistance technique et la résolution des pannes
· La sécurisation de l'ensemble des installations
· Un travail de maintenance ponctuelle sur les différents appareils informatiques
· Des points de sécurité afin de s'assurer que les degrés de protection restent pertinents dans le temps
· Un travail de veille technologique visant à identifier l'évolution des menaces et à repérer les outils de cyberdéfense à acquérir en priorité
· La remise de propositions pour améliorer les processus internes et gagner ainsi en efficacité et en sécurité
· Un travail de formation et de sensibilisation des employés à la bonne utilisation des systèmes informatiques
· Un travail de diffusion des bonnes pratiques en matière de sécurité cyber.

« L'administrateur réseau intervient à la fois sur le temps long et sur le temps court », analyse Thomas L., administrateur système. *« Il a un rôle qui se joue sur le terrain de la patience : c'est lui qui assure qu'on pose bien les bases, sur le plan informatique, et que chaque collaborateur*

peut gérer ses tâches en toute fluidité. Mais c'est lui aussi qui intervient dans l'urgence quand il y a une panne sur les systèmes. Et c'est là qu'on détecte son niveau de responsabilité : plus on perd de temps sur une panne, plus le manque à gagner est conséquent pour l'entreprise. C'est un enjeu de taille qu'on a entre nos mains. Dans mon cas précis, quand on se trouve au cœur d'un groupe qui produit des films, des émissions, des séries, il y a des enjeux de livraison, de diffusion, de continuité de service qui rehaussent encore un peu plus le niveau de responsabilité. Mais c'est aussi cela qui valorise mon métier. »

Compétences

L'administrateur système doit connaître les langages informatiques, même s'il ne sera pas amené à programmer. De même, il doit avoir une bonne maîtrise du codage. Son expertise est surtout attendue sur le matériel informatique et les solutions réseaux en règle général. Son niveau d'éducation et d'information sur ces derniers points doit être très largement supérieur à la moyenne.

La parfaite maîtrise de l'anglais technique est un autre point souvent mentionné dans les fiches de poste. Cette compétence se révélera précieuse :

· Pour être efficace et complet dans le travail de veille technologique
· Pour maintenir un haut degré de réactivité face à une panne

« L'ADMINISTRATEUR SYSTÈME POURSUIT DEUX OBJECTIFS : PROPOSER UN SYSTÈME À LA FOIS FONCTIONNEL ET À MOINDRE COÛT. »

Études

Pour aborder la profession d'administrateur système, il faut avoir validé un Bac +3 au minimum. La détention d'un Bac +5 est néanmoins un atout apprécié par les recruteurs, notamment par les grands groupes. Avec l'augmentation des risques cyber, une formation plus longue et les spécialisations en cybersécurité deviennent en effet de plus en plus incontournables. Cette recherche de profils plus solides sur les questions de menaces informatiques devraient d'ailleurs être de plus en plus intégrée par les petites et moyennes entreprises, qui sont tout aussi exposées aux cyberattaques que les grandes structures.

Salaire

Un administrateur système débutant dans une structure de taille petite à moyenne peut miser sur un salaire brut de 2 500 euros mensuels. Cette rémunération peut être revue à la hausse si le professionnel intègre une grosse structure, une entreprise en charge de données particulièrement sensible ou une organisation dont la réputation est particulièrement importante. De même, plus une structure reconnaît l'importance des enjeux de cybersécurité, plus le salaire de l'administrateur système est susceptible d'être légèrement majoré.

Le salaire d'un administrateur système confirmé peut avoisiner les 3 550 euros mensuels brut. Selon les mêmes règles que celles énoncées auparavant, cette somme « de base » peut être dépassée dans de nombreux cas de figure.

Il faut d'ailleurs rappeler que les entreprises ont relevé leurs exigences à l'embauche, préférant de plus en plus les Bac +5 aux Bac +3. La formation longue est supposée apporter une garantie supplémentaire pour répondre efficacement aux questions de cybersécurité. On peut espérer que cette « revalorisation du bagage » s'accompagne d'une revalorisation de salaire générale dans les années à venir.

QUALITÉS

Pour mener à bien et le plus facilement possible sa mission d'administrateur systèmes et réseaux, il faut tout d'abord faire preuve d'une grande flexibilité. *« Nous sommes là pour être à l'écoute d'équipes diverses, qui n'ont pas toutes les mêmes besoins et les mêmes niveaux de compréhension des outils informatiques. Il faut donc être malléable, à l'écoute, pédagogue et patient – c'est essentiel ! »*, explique Thomas L. *« De manière plus concise, on peut dire que la qualité première de l'administrateur système est la disponibilité. »*
La curiosité est une autre qualité essentielle. *« C'est la petite flamme qui doit nous pousser à nous tenir informés des dernières évolutions informatiques, afin de procéder aux changements et améliorations nécessaires pour l'entreprise. La curiosité va de pair avec l'autonomie : à nous d'aller chercher, fouiller, déterrer les informations cruciales, sans attendre que les niveaux d'alerte passent à l'orange. »*
Que se passe-t-il lorsque les voyants passent au rouge, c'est-à-dire en cas de panne ou de blocage du système informatique ? *« Les qualités indispensables, pour cette phase plus intense du métier, sont la réactivité – sans surprise – et une grande vivacité d'esprit. Il faut pouvoir analyser rapidement et garder son sang-froid pour initier le retour à la normale dans les meilleures conditions »*, précise Thomas L.
La prise d'initiative est un autre élément important : cela tient au rôle moteur de l'administrateur système pour proposer des solutions de remise en état du réseau et les exécuter. *« Il faut aussi faire preuve d'une capacité à la gestion multitâche, parce qu'en même temps que l'on pense le côté technique des solutions, il faut garder en tête les critères relatifs au budget, au cahier des charges et aux délais de résolution ! »*.

Enfin, l'aptitude à la gestion d'équipe peut s'avérer bien utile, notamment lorsque l'administrateur système évolue dans un grand groupe et s'appuie sur différents agents techniques pour mettre en œuvre ses solutions.

Où travailler ?

« Il va sans dire que les administrateurs système ont l'embarras du choix pour se positionner. Toutes les entreprises de tous les secteurs, ou à peu près tous, sont obligés de s'appuyer sur un système informatique pour prospérer. Dès lors, tout le monde a besoin d'un administrateur système ! Ses tâches et ses responsabilités pourront varier de manière assez large, en fonction du secteur et de la taille de l'entreprise. Mais peu importe la configuration : l'administrateur système a toujours une importance centrale. Il a le potentiel pour avoir une importance capitale en cas de défaut dans le système », analyse Thomas L.

Dès lors, ce professionnel des « premières couches de la pyramide informatique » pourra aussi bien s'épanouir dans une entreprise de services numériques (ESN), chez un développeur de jeux vidéo, dans une banque, une grande administration, auprès d'un site de revente en ligne ou aux côtés d'une grande référence du luxe – tous les scénarios sont possibles.

Les offres d'emplois pour administrateurs systèmes et réseaux sont loin d'être rares. Parmi les grandes références en recherche active de personnes compétentes, on aura pu repérer récemment des offres signées par :

- Le Groupe La Poste
- Groupama
- Radio France
- Le grand groupe d'édition Editis
- McDonald's France
- La Banque de France
- AXA Finance
- La Ville de Bordeaux
- Stellantis

Évolution de carrière

Plusieurs voies se présentent à l'administrateur système lorsqu'il souhaite changer de perspective. Son expertise des réseaux peut le mener naturellement vers un poste d'administrateur réseau ou d'architecte réseau. On le voit aussi souvent évoluer vers des fonctions similaires, mais à plus grande échelle : il peut ainsi devenir responsable de parc informatique.

À un niveau de responsabilité plus élevée, il peut se voir confier un poste de Responsable de la sécurité informatique. *« Cette option est de plus en plus envisageable, dans la mesure où les recruteurs tablent de plus en plus sur les compétences en sécurité cyber pour bien choisir leur administrateur réseau. Ce dernier a donc tout à fait les compétences et le profil pour devenir, à terme, responsable de la sécurité informatique. Au final, c'est une façon un peu plus claire de dire ce qu'il faisait déjà en partie auparavant ! »,* selon Thomas L.

On peut enfin imaginer une bifurcation sur un poste de chef de projet informatique ou, pour les plus experts et les plus téméraires, une activité de consultant informatique en indépendant.

Avantages et inconvénients

« Le principal inconvénient – ou plus exactement challenge – que j'associe à mon métier est celui du stress qui peut arriver par vagues, au moment des pannes. Ce sont vraiment des moments où il faut faire preuve d'une grande maîtrise de soi, pour bien gérer à la fois les aspects techniques et les aspects humains de la panne. Parce qu'un système informatique par terre, ce n'est pas seulement un défi technique qui demande de saisir le pourquoi du problème. C'est aussi résoudre des équations humaines. Les autres collaborateurs ne sont pas toujours en mesure de contenir leur mécontentement et il faut alors savoir faire preuve de patience. Il faut redoubler de diplomatie, là où ces mêmes personnes n'en ont pas ! ». Telle est l'expérience de Thomas L., qui évolue depuis un peu plus de 6 ans sur ce type de poste.

« Du côté des avantages, je dirais que les phases de calme sont particulièrement appréciables. Non pas parce qu'il s'agit de phases d'inactivité, loin de là. Pour ma part, j'approche ces périodes – les plus fréquentes – comme une opportunité pour m'enrichir, pour effectuer avec minutie mon travail de veille technologique. J'ai l'impression d'apprendre en permanence, parfois même d'aller au devant des problèmes, avant même qu'ils ne surgissent. Le sentiment d'apprendre, c'est certainement le facteur d'adéquation numéro un d'une personne avec son métier ».

L'AVIS DU PROFESSIONNEL

« Si je devais résumer mon métier de manière extrêmement simple, je dirais que je suis la personne chargée de s'assurer que tous les segments de toutes les infrastructures informatiques de mon entreprise fonctionnent. C'est peut-être l'une des fonctions informatiques les plus ancrées dans le concret, le quotidien et la logistique en général. On est, en quelque sorte, le maître du matériel informatique et de la bonne interconnexion de ses différentes composantes. »

Thomas L.
Administrateur système

« L'ADMINISTRATEUR SYSTÈME JOUE UN RÔLE ESSENTIEL DANS LA CONCEPTION DU SYSTÈME D'EXPLOITATION D'UNE ENTREPRISE. »

Niveau d'études : Bac+5

Spé Conseillée : Scientifique

Employabilité : Bonne

Salaire débutant : 3 300 €

Code ROME : M1802 - Code FAP : M2Z

DANS LA LARGE PALETTE DES MÉTIERS CYBER, ON TROUVE UN CERTAIN NOMBRE DE POSITIONS STRATÉGIQUES : DES PROFESSIONNELS DOTÉS D'UNE EXPERTISE FORTE SUR UN DOMAINE OU UN ASPECT TECHNIQUE JOUENT LE RÔLE DE VIGIE. C'EST SUR EUX QUE COMPTENT LES ENTREPRISES ET LES AUTRES STRUCTURES POUR TIRER LA SONNETTE D'ALARME EN CAS DE PRATIQUE NON RESPECTUEUSE DE LA CONFIDENTIALITÉ OU DE LA LOI. LE FRAUD ANALYST FAIT PARTIE DE CES EXPERTS EN POSITION DÉFENSIVE. IL A POUR RÔLE DE JETER UN COUP DE PROJECTEUR SUR TOUT USAGE OU PRÉSENCE FRAUDULEUSES DANS LES SYSTÈMES INFORMATIQUES. VOYONS PLUS EN DÉTAIL QUELLES SONT LES QUALITÉS REQUISES POUR EXCELLER SUR CETTE MISSION DE VIGILANCE ET COMMENT LE MÉTIER SEMBLE ÉVOLUER DANS UN CONTEXTE DE MULTIPLICATION DES RISQUES CYBER.

Missions

Le fraud analyst a un triple rôle :

- De détection et prévention
- D'analyse détaillée
- De conseil

« Il exerce ces fonctions sur tout ou partie des systèmes informatiques internes, mais aussi sur les ponts avec l'extérieur. Lorsqu'une transaction ou une opération implique un appareil appartenant à un tiers, il s'agit de repérer la tentative de transaction frauduleuse avant qu'elle ne se concrétise. Il faut donc élargir son périmètre de surveillance au-delà de la structure. J'aime bien dire qu'il faut faire rayonner sa surveillance, tout autour de la meute centrale que nous représentons, nous les employés de la structure. C'est une mission œil de lynx, et l'objectif est de réussir à avoir le regard qui porte loin, en mode 360° ! », explique Delphine J., fraud analyst.

Le fraud analyst a un rôle de cyberdéfense active. Il intervient sur un point de détail, à savoir la sécurité des transactions et opérations informatiques en échange avec l'extérieur. Ce travail se révèle primordial pour certains activités en particulier, notamment les télécoms et l'e-commerce.

Compétences

L'analyste des fraudes doit pouvoir s'appuyer sur un certain nombre de connaissances techniques. Il est important qu'il puisse :

- Maîtriser parfaitement les mécanismes relatifs aux systèmes d'information

en général et ceux de sa structure en particulier
· Bien connaître les outils d'analyse des vulnérabilités et des virus informatiques
· Analyser les flux de réseaux
· Avoir une vision claire et sans cesse à jour du panorama des techniques d'attaque
· Maîtriser les techniques du scripting
· Maîtriser le SQL (Structured Query Language) et la formulation de requêtes
· Maîtriser plusieurs applications de suivi des analyses, comme Business Objects ou Access

Études

Pour aborder sereinement le poste de fraud analyst et être crédible face aux recruteurs, il est nécessaire de valider au préalable un Bac +5. Les spécialisations en langage informatique et en cybersécurité pourront être des avantages considérables au moment de l'embauche.

Salaire

Au cours de ses trois premières années à ce poste, l'analyste des fraudes peut espérer gagner environ 3 300 euros brut par mois. Cette rémunération peut être revue à la hausse dès lors que le professionnel justifie d'une formation en cybersécurité particulièrement poussée. La même règle peut s'appliquer lorsque le professionnel apporte la maîtrise d'un code ou d'un langage encore peu connu. Pour un niveau senior, on relève un salaire mensuel moyen de 6 250 euros brut. La sensibilité des données que gère l'entreprise ou l'importance des pendants financiers de chaque transaction peuvent aussi être des arguments pour revoir les rémunérations à la hausse.

Où travailler ?

Comme déjà évoqué, le fraud analyst est un allié de premier plan pour toutes les entreprises traitant des données particulièrement sensibles ou amenées à gérer des mannes financières importantes. Son rôle est important, en règle générale, pour toutes les structures désireuses de protéger la confidentialité de leurs opérations, quelle que soit leur nature.

Pour être plus précis, on pourra donc être particulièrement attentif aux offres postées par les structures de santé, les banques et assurances, les entreprises de services numériques (ESN), les assureurs cyber, les entreprises de télécoms et fournisseurs d'accès à internet, entre autres.

Parmi les entreprises particulièrement intéressées par des Analystes des fraudes, on voit souvent apparaître les noms de :

· Lydia, le service de paiement instantané
· La CACIB dans le secteur bancaire
· Axa pour ses services banque et assurance
· Bouygues Telecom
· Orange
· Le groupe Thales
· Les hôpitaux de Paris
· Air France

« LE MÉTIER DE FRAUD ANALYST EST INTIMEMENT LIÉ AUX SUJETS DES DONNÉES ET DE LA CONFIDENTIALITÉ. IL CONSISTE À ASSURER LE RESPECT DE L'INTÉGRITÉ DES OPÉRATIONS OU D'UNE ENTREPRISE EN PASSANT AU CRIBLE TOUTE UNE SÉRIE DE TRANSACTIONS. »

QUALITÉS

Les trois qualités principes du fraud analyst sont :
· L'autonomie
· L'esprit d'analyse
· Le sens de l'organisation

Le sens du détail et la curiosité sont deux autres atouts indispensables. Ils sont indispensables pour repérer les opérations frauduleuses, souvent discrètes pour maximiser les chances de réussite, et pour mener à bien le travail de veille sur l'évolution des menaces. L'analyste des fraudes peut aussi être amené à exposer un cas de transaction frauduleuse à ses collègues ou à sa hiérarchie. Cela permettra de relever le niveau de vigilance de toutes les équipes et de mettre en place des mécanismes de blocage à grande échelle. Dans ce cas précis, des talents de pédagogue sont attendus, de même qu'une aptitude à la patience, à la clarté et à la synthèse.

Évolution de carrière

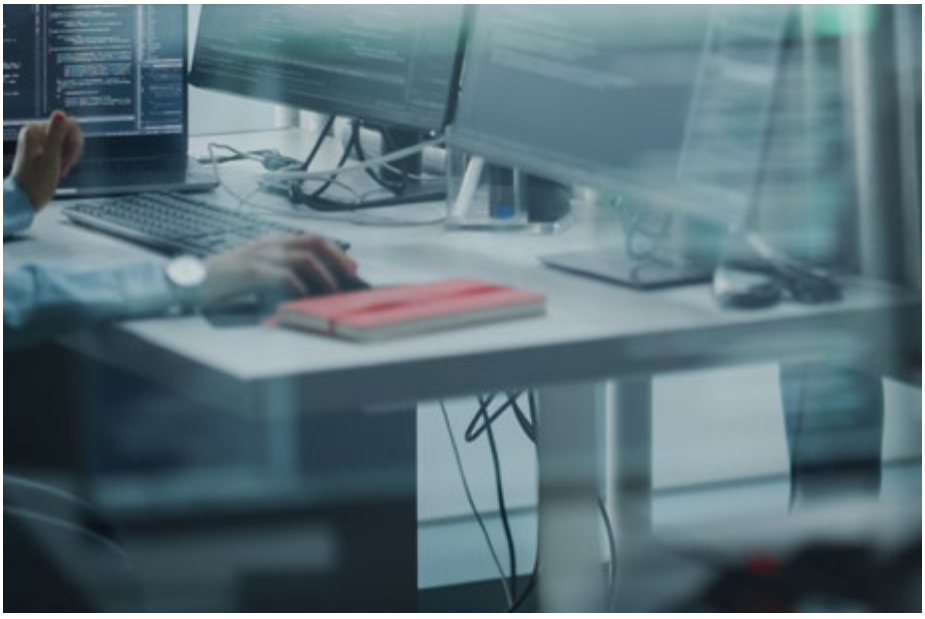
Le fraud data analyst peut décider d'opérer une « défocalisation » sur son métier, pour exercer une fonction plus générale de data analyst ou d'analyste en menaces cyber. Il aura dès lors la responsabilité de rester en alerte sur plusieurs problèmes de cybersécurité à la fois.

Si c'est la voie du travail en indépendant qui le tente, il peut aussi envisager une activité de Consultant en sécurité informatique.

Un rôle en évolution

« Si on veut retracer en quelque sorte la biographie de l'analyste des fraudes, il y a un mot clé à mentionner : numérisation. C'est dans la mesure où les opérations se sont de plus en plus numérisées que le fraud analyst a vu sa fonction prendre de l'ampleur », rappelle Delphine J. Il y a une quinzaine d'années, le travail de détection des fraudes reposait encore largement sur un travail humain : « *Je sais que mes prédécesseurs devaient observer un certain nombre de règles prédéfinies, qui aidaient à repérer à l'œil nu si une transaction posait un problème. La principale difficulté est que ces ensembles de règles étaient certes très précis, mais trop compliqués à gérer de par leur multiplicité, les interconnexions… D'autre part, avec la numérisation croissante de tous les processus, il fallait vraiment aller plus vite. Par la force des choses, le fraud analyst a donc dû s'appuyer sur des outils d'analyse pour mener ses investigations. De fin analyste, il est plutôt devenu fin technicien. Cela n'empêche pas qu'il faut toujours faire preuve de beaucoup de vigilance face aux transactions et que chacun de nous mobilise une vraie capacité à comprendre les mouvements observés ! Mais nous sommes passés sur une identité beaucoup plus technicienne. »*

De fait, les analystes des fraudes se sont beaucoup rapprochés du machine learning : cela leur permet d'avoir, d'entrée de jeu, des patterns de transactions frauduleuses à filtrer en permanence. *« Cela permet d'élaguer déjà beaucoup de problèmes et de se concentrer sur les fraudes aux formats inconnus, pour les entrer elles aussi dans nos systèmes de surveillance et continuer à maintenir un niveau de sécurité maximal. Bien entendu, ce sont souvent les machines elles-mêmes qui vont repérer ces nouvelles pratiques – parce qu'elles ne suivent pas le schéma de fonctionnement général d'une transaction. Notre mission principale, dès lors, consiste à optimiser ces outils de surveillance et d'analyse. Et la réalité est qu'il y a beaucoup à faire. La mise à jour est un exercice de tous les instants »,* confie Delphine J.



Avantages et inconvénients

« Au début de ma toute première prise de poste, il y avait peut-être une petite angoisse : la possibilité de laisser passer une action frauduleuse est réelle et il n'est pas toujours facile d'assumer son côté faillible, surtout lorsque l'opération met en cause des sommes ou des données importantes. Il y a donc un stress inhérent au métier, mais c'est certainement le cas de tous les métiers qui touchent aux questions de sécurité cyber. Cela implique aussi qu'il faut faire preuve d'une concentration soutenue, et tenir cette concentration sur la durée : il y a une charge mentale importante sur ce point et un côté rébarbatif parfois », reconnaît Delphine J.

« Mais c'est aussi un poste sur lequel on peut avoir la satisfaction de faire des découvertes. Repérer une fraude dont le format n'était pas connu jusque-là, c'est une petite réussite et il y a une satisfaction personnelle directe. C'est un peu comme décrocher le pompon sur les manèges quand on est enfant. Je pense qu'il est important de croire à cet aspect ludique du job, c'est aussi cela qui permet de tenir sur la durée et de rester opérationnel. Il ne faut pas non plus oublier le côté très satisfaisant du travail de veille : en essayant de repérer les nouveaux types de menaces, ceux que les fraudeurs essaient justement de cacher, on a toujours et encore cet aspect ludique du défi et on apprend tellement de choses, tout le temps. Au final, c'est ce qui nous rend légitimes. »

65

CYBERSTRATÉGISTE

Niveau d'études : Bac+5

Spé Conseillée : Scientifique

Employabilité : Très bonne

Salaire débutant : 3 850 €

Code ROME : M1802 - Code FAP : M2Z

UNE BONNE CYBERDÉFENSE DOIT PRENDRE EN COMPTE LES TENDANCES À VENIR. LA TÂCHE EST DE FAIT COMPLEXE, MAIS LES EXPERTS CYBER SE DOIVENT DE COMMENCER À DÉFINIR DÈS AUJOURD'HUI LES POINTS CENTRAUX DE LA CYBERSÉCURITÉ POUR LES DIX ANS À VENIR (LIEN VERS ARTICLE GUARDIA CYBER 2033). POUR MENER À BIEN CETTE MISSION AUX ENJEUX TRÈS LOURDS, LES ENTREPRISES FONT DE PLUS EN PLUS APPEL À UN EXPERT À LA VISION LARGE : LE CYBERSTRATÉGISTE. VOYONS ENSEMBLE QUELS SONT LES DÉFIS AUXQUELS CE PROFESSIONNEL EST APPELÉ À ÊTRE CONFRONTÉ ET QUELLES SONT LES FORCES DONT IL A BESOIN POUR MENER À BIEN SA TÂCHE.

Missions

« On attend deux choses de la part du cyberstratégiste : qu'il soit force de proposition pour prévenir les risques cyber et qu'il participe à la compréhension des attaques subies », explique Sylvain M. *« Il s'agit donc à la fois de planifier et de réagir ».*

Dans le cadre de son activité de prévention, plusieurs tâches doivent être réalisées :

· Opérer une veille sur les menaces émergentes en matière de cybersécurité
· Communiquer de manière pédagogique auprès de tous les décisionnaires et acteurs décisifs de la structure sur les enjeux de la cybermenace en général
· Dresser un panorama des menaces susceptibles d'affecter l'organisation et déterminer son niveau d'exposition au risque
· Collecter, vérifier et analyser les données brutes relatives aux attaques informatiques, en élargissant au maximum les sources d'information
· Entretenir un rapport d'échange et d'émulation avec d'autres experts n'appartenant pas à la structure
· Mettre à jour des bases de données et de connaissances sur l'ensemble des sujets concernés

Le deuxième volet de la mission est plus ponctuel. Il s'agit d'apporter les bons éléments en cas de cyberattaque. Cela passe notamment par :

· La rédaction de documents d'alerte et de rapports d'analyse destinés à faciliter la compréhension des menaces détectées

· Des analyses sur les possibles évolutions de la menace auprès de toutes les parties impliquées, accompagnées de propositions de solutions concrètes
· On attend du cyberstratégiste qu'il entre en dialogue étroit avec le CERT (computer emergency response team) ou le CSIRT (computer security incident response team), de même qu'avec le SOC, lorsqu'il existe. C'est grâce à la bonne collaboration entre tous ces acteurs clés que peuvent être mis en place les bons outils de protection cyber

Protéger les ressources de la structure pour laquelle il travaille : telle est la responsabilité principale du cyberstratégiste. Ces ressources, ce sont les données de l'entreprise et les données personnelles de ses clients : leur compromission est synonyme de pertes financières pour l'entreprise, et c'est le rôle du cyberstratégiste d'éviter cette situation.

À ce titre, il est notamment chargé de prévenir les attaques. Cela passe par des propositions de mise à jour des systèmes informatiques, des idées de formation à destination des différents collaborateurs, … C'est à lui d'argumenter pour faire accepter les investissements en matière de cybersécurité.

Compétences

Pour réussir à son poste, le cyberstratégiste ne peut en aucun cas faire l'impasse sur un certain nombre de compétences techniques. Celles-ci doivent cependant être complétées par des aptitudes plus générales à la prospection et à l'analyse, mais aussi par des compétences de type managérial. Même si le cyberstratégiste ne remplit pas un rôle de manager, il a besoin de capacités propres à ce rôle pour approcher les équipes et recueillir les informations nécessaires, puis pour les faire adhérer à sa vision des choses. Cette position de « leader » doit pouvoir être exercée aussi bien auprès des agents techniques que des personnes à responsabilité dans l'entreprise.

Le cyberstratégiste doit par ailleurs se montrer opérationnel sur plusieurs points. Il doit être capable :

· D'utiliser des sources ouvertes de manière sécurisée
· De construire des plans de veille opérationnels sur plusieurs questions et plusieurs secteurs en parallèle
· D'assurer une veille géopolitique et géostratégique, en plus de la veille purement technique, afin de mesurer l'évolution des risques cyber en provenance de l'extérieur

Il doit faire de bonnes capacités pour :

· La gestion des crises de sécurité
· La veille opérationnelle et la synthèse, afin de capter les tendances et les facteurs d'évolution du métier

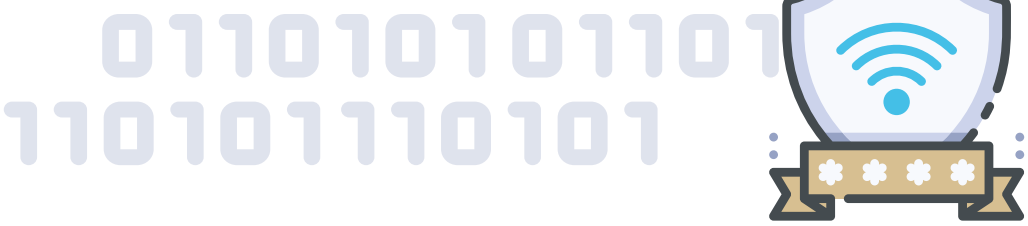
On requiert enfin des connaissances solides en matière :

· De techniques d'attaque et d'intrusion informatique
· De la vulnérabilité propre à chaque environnement
· D'analyse des flux de réseau

La connaissance des procédures légales propres au domaine cyber est également appréciée : en cas d'incident, on attend parfois du cyberstratégiste un conseil sur les actions de recours juridiques possibles contre l'attaquant, même s'il peut être épaulé dans cette tâche par d'autres experts cyber.

QUALITÉS

« Le cyberstratégiste doit être capable de mettre au diapason des spécialistes très différents de par leurs compétences et – surtout – de par leur manière de penser. Il doit donc faire preuve de très grandes capacités d'écoute, de dialogue et de pédagogie, mais aussi avoir suffisamment de charisme et de force de conviction pour embarquer tout le monde derrière lui », explique Sylvain M., cyberstratégiste. *« L'enjeu n'est pas des moindres: s'il ne réussit pas à réellement convaincre toutes les équipes de la stratégie qu'il dessine, alors cela veut dire que certains seront peut-être moins attentifs dans la réalisation de leurs tâches, et c'est dans cette brèche que s'engouffrent les cyberattaquants : c'est la fameuse faille humaine, la première cause de réussite des cyberattaques ! J'ai toujours l'image du cyberstratégiste comme un électron libre : il gravite d'équipe en équipe. Mais, au bout du compte, il doit s'imposer comme le noyau dur – au nom de cette stratégie globale d'entreprise ».*



Études

La détention d'un Bac +5 est un prérequis minimum pour se positionner sur un emploi de cyberstratégiste. Les profils combinant compréhension des enjeux techniques et capacités managériales seront particulièrement appréciés.

Salaire

En moyenne, un cyberstratégiste peut espérer débuter sa carrière avec un salaire de 3 850 euros mensuels brut. C'est, sans surprise, l'étendue de ses expériences et le poids de ses références qui vont permettre de négocier cette rémunération à la hausse. À un niveau senior, un cyberstratégiste peut gagner jusqu'à 9 450 euros brut par mois environ.

Les deux chiffres précédents correspondent à la situation d'un salarié. Lorsqu'il exerce en indépendant, le cyberstratégiste nouvellement apparu sur le marché peut fixer son taux journalier moyen à 650 euros brut. À un niveau confirmé, il peut prétendre à une rémunération journalière qui atteint presque le double, pour atteindre 1 250 euros brut.

Où travailler ?

« Les experts en cyberstratégie ont l'embarras du choix concernant les secteurs où ils peuvent exercer. Il n'y a pas vraiment de conseils à donner en matière de domaine d'activité à viser. Le vrai point à retenir, c'est que ce sont les grandes entreprises et les grands groupes qui ont besoins de cyberstratégistes – du moins, qui sont prêts à investir sur ce poste », analyse Sylvain M.

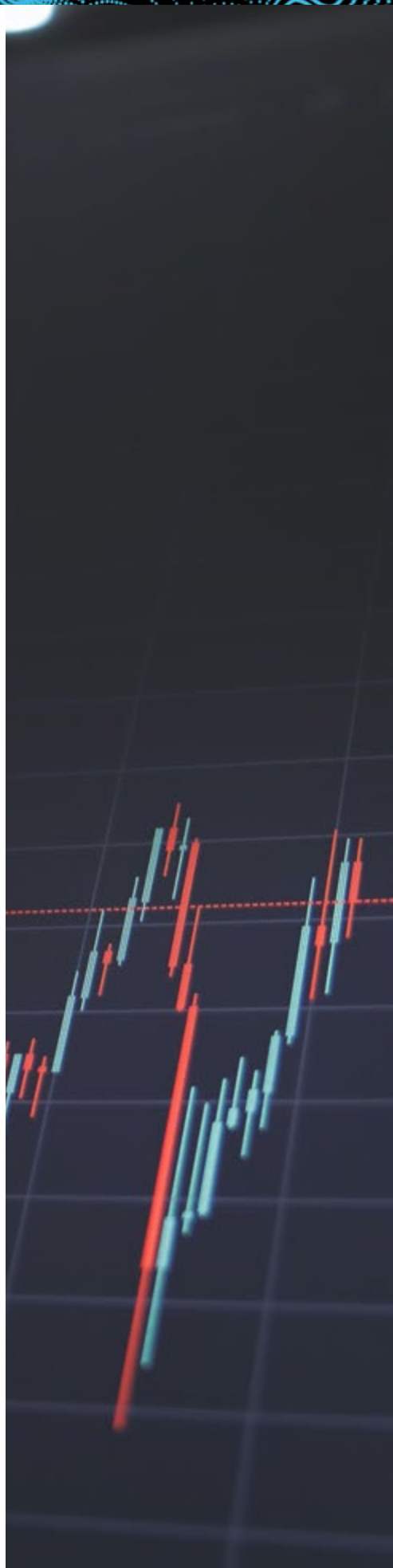
On relève néanmoins certains pans d'activité où ces analystes de la direction à suivre sont particulièrement demandés. C'est le cas des entreprises proposant des services numériques en général, des banques et assurances, et plus particulièrement des cyber-assureurs. On note aussi de forts besoins du côté des GAFAM et des services de santé – sans grande surprise, puisque toutes les structures traitant un volume important de données personnelles ont tout intérêt à mettre en place une bonne stratégie de cyberdéfense.

De manière générale, on pourra aussi retenir que toutes les entités disposant d'une structure de type SOC ont besoin, en théorie, de cyberstratégistes !

À l'heure actuelle, on note un boom des assureurs en risque cyber, dont le nombre se multiplie, notamment en France. Il s'agit de structures particulièrement friandes en analystes cybersécurité, puisque ce sont ces derniers qui pourront proposer aux clients l'analyse de situation et l'arsenal de protection adapté pour faire face aux menaces extérieures.

Parmi les autres recruteurs en puissance, on repère également :

· Des géants du divertissement et des réseaux sociaux, comme Facebook et Meta, le groupe auquel il appartient, Netflix ou Banijay, gros producteur et diffuseur de contenus audiovisuels
· Des incontournables de l'aéronautique et de l'aérospatiale, comme Safran, Airbus ou Thales
· De nombreux acteurs du secteur bancaire, comme BNP Paribas, Axa ou la Société générale, notamment
· Des assureurs cyber comme Hiscox, Aviva et Chubb
· Des spécialistes des services informatiques en tous genres



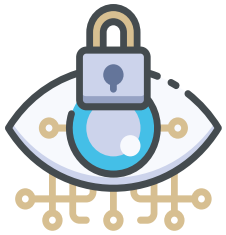
L'AVIS DU PROFESSIONNEL

« Le cyberstratégiste, c'est un peu celui qui définit la politique générale de l'entreprise qui est prête à faire face aux menaces des hackers – qui veut être prête ! C'est la ligne de commandement que devra suivre l'armée de talents cyber que mobilise la structure. Mais attention : en aucun cas le cyberstratégiste n'impose sa vision. Le bon cyberstratégiste, c'est celui qui a la capacité de comprendre et d'agréger des besoins divers, des analyses et des préoccupations qui changent selon les équipes métiers, et de les faire concorder pour apporter une réponse globale aux menaces cyber. »

Sylvain M.
Cyberstratégiste

Évolution de carrière

Le cyberstratégiste engageant une responsabilité importante sur chacune de ses préconisations, il est particulièrement bien placé pour évoluer sur des postes de haut niveau. *« Lorsque les compétences techniques, analytiques et managériales de ce professionnel sont confirmées, il peut sans trop de problèmes se positionner sur un poste de Responsable de la Sécurité des Systèmes d'Information ou, mieux encore, de Directeur de la cybersécurité d'une entreprise »,* estime Sylvain M. *« Il a aussi la possibilité de développer une activité de consultant en cyberdéfense : c'est la voie qui semble la plus naturelle. Et puis il peut aussi avoir envie de prendre en main une mission moins large, plus précise. J'ai vu des cyberstratégistes de talent se reconvertir en chefs de sécurité projet, en auditeurs spécialistes des questions cyber ou en chercheurs en sécurité : tout dépend des affinités et des envies de changement de cadre qu'éprouve chacun ! ».*



Avantages et inconvénients

« Je crois qu'une des premières motivations dans un métier, c'est le fait d'apprendre : c'est ce qui fait que l'on ne s'ennuie pas – et ce qui donne du sens à ce que l'on fait. Le cyberstratégiste a ça pour lui. Il est obligé de se plonger en permanence dans la découverte des dernières innovations technologiques pour savoir quels types de menaces planent sur les entreprises.

Il y a aussi cette dimension de jeu – avec de grands enjeux, certainement, mais il y a une notion de pari très stimulante. Savoir si l'on va placer ses pions au bon endroit, en matière de cyberdéfense, cela a quelque chose de très excitant. Mais c'est aussi très stressant : ce qui fait le sel du métier pèse aussi dans la balance des désavantages », explique Michael N. *« Il faut aussi parler de cet aspect très gratifiant : vous avez face à vous des responsables de départements informatiques et des créateurs d'entreprises qui placent toute leur confiance en vous. C'est valorisant, mais c'est aussi beaucoup de pression qu'il faut pouvoir supporter, sur une durée assez longue ! ».*

LES SALAIRES
DE LA CYBERSÉCURITÉ

Classement des métiers de la cybersécurité selon le salaire moyen en France (moyenne entre le salaire brut débutant et le salaire brut confirmé).

Source : enquête interne auprès des professionnels.

#	MÉTIER	SALAIRE
01	DIRECTEUR CYBERSÉCURITÉ	12500 €
02	CHIEF INFORMATION SECURITY OFFICER (CISO)	11000 €
03	RESPONSABLE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION (RSSI)	10900 €
04	MEDIA EXPLOITATION ANALYST	9150 €
05	RESPONSABLE GRC	8700 €
06	THREAT HUNTER	8330 €
07	CHERCHEUR EN SÉCURITÉ DES SYSTÈMES D'INFORMATION	7000 €
08	MALWARE ANALYST	6860 €
09	OSINT ANALYST	6800 €
10	VULNERABILITY RESEARCHER & EXPLOIT DEVELOPER	6700 €
11	CYBERSTRATÉGISTE	6650 €
12	AUDITEUR DE SÉCURITÉ TECHNIQUE	6603 €
13	RESPONSABLE DU CONTRÔLE INTERNE	6590 €
14	EVALUATEUR DE LA SÉCURITÉ DES TECHNOLOGIES DE L'INFORMATION	6500 €
15	CLOUD SECURITY ANALYST	6115 €
16	ARCHITECTE CYBERSÉCURITÉ	6000 €
17	ANALYSTE CYBERSÉCURITÉ	5900 €
18	SECURITY AWARENESS OFFICER	5830 €
19	HACKER ÉTHIQUE	5750 €
20	DEVOPS	5735 €
21	SECURITY SERVICE DELIVERY MANAGER	5625 €
22	EXPERT EN CYBERSÉCURITÉ	5400 €
23	MANAGER DE RISQUES	5025 €
24	RESPONSABLE DU CSIRT	5000 €
25	CHEF DE PROJET CYBERSÉCURITÉ	5000 €
26	PROMPT ENGINEER	4950 €
27	DEVSECOPS	4900 €
28	FRAUD ANALYST	4775 €
29	INCIDENT RESPONSE TEAM MEMBER	4775 €
30	ANALYSTE CSIRT	4750 €
31	CHARGÉ DE COMMUNICATION SPÉCIALISÉ EN CYBERSÉCURITÉ	4750 €
32	CONSULTANT EN CYBERSÉCURITÉ	4650 €
33	ANALYSTE EN RÉPONSE À INCIDENTS	4584 €

#	MÉTIER	SALAIRE
34	RESPONSABLE DU PLAN DE CONTINUITÉ D'ACTIVITÉ	4500 €
35	DÉVELOPPEUR DE SOLUTIONS DE SÉCURITÉ	4400 €
36	RED TEAMER	4350 €
37	GESTIONNAIRE DE CRISE DE CYBERSÉCURITÉ	4250 €
38	RESPONSABLE DU SOC (SECURITY OPERATION CENTER)	4250 €
39	ANALYSTE DE LA MENACE CYBERSÉCURITÉ	4250 €
40	SPÉCIALISTE EN DÉVELOPPEMENT SÉCURISÉ	4200 €
41	BLUE TEAMER	4100 €
42	DÉLÉGUÉ À LA PROTECTION DES DONNÉES	4085 €
43	DIRECTEUR DE PROGRAMME DE SÉCURITÉ	4000 €
44	PENTESTER	4000 €
45	INGÉNIEUR CYBERSÉCURITÉ	4000 €
46	AUDITEUR DE SÉCURITÉ ORGANISATIONNELLE	3959 €
47	FORMATEUR EN CYBERSÉCURITÉ	3950 €
48	CRYPTOLOGUE	3900 €
49	ANALYSTE FORENSIC	3900 €
50	CYBERCOMBATTANT	3850 €
51	ARCHITECTE RÉSEAU	3750 €
52	RESPONSABLE DES ASSURANCES	3725 €
53	ADMINISTRATEUR RÉSEAU	3600 €
54	DÉVELOPPEUR BACK-END	3580 €
55	JURISTE SPÉCIALISÉ EN CYBERSÉCURITÉ	3500 €
56	ANALYSTE SOC	3450 €
57	BUG BOUNTY HUNTER	3300 €
58	COORDINATEUR CYBERSÉCURITÉ	3200 €
59	ADMINISTRATEUR CYBERSÉCURITÉ	3150 €
60	DÉVELOPPEUR WEB	3130 €
61	ADMINISTRATEUR SYSTÈME	3050 €
62	ADMINISTRATEUR SYSTÈME	3025 €
63	DÉVELOPPEUR FRONT-END	3000 €
64	INTÉGRATEUR DE SOLUTIONS DE SÉCURITÉ	3000 €
65	DÉVELOPPEUR FULL STACK	2950 €
››	**SALAIRE MOYEN**	**5187 €**

TOP 10
DES MÉTIERS DE LA CYBERSÉCURITÉ

Quels sont les métiers de la cybersécurité les plus populaires ?

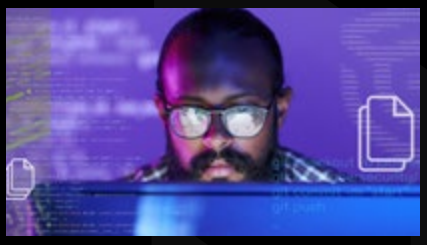
Classement réalisé en fonction du nombre de visiteurs sur nos fiches métiers.

01. HACKER ÉTHIQUE

PAGE 52

02. INGÉNIEUR CYBERSÉCURITÉ

PAGE 56



03. PENTESTER

PAGE 62

04. CONSULTANT EN CYBERSÉCURITÉ

PAGE 26

05. ANALYSTE SOC

PAGE 10

06. ARCHITECTE CYBERSÉCURITÉ

PAGE 18

07. RESPONSABLE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION (RSSI) PAGE 74

08. ANALYSTE DE LA MENACE CYBERSÉCURITÉ

PAGE 6

09. CRYPTOLOGUE

PAGE 32

10. CHEF DE PROJET SÉCURITÉ

PAGE 22