

Welcome  
TO THE  
Jungle

# — Guide des métiers —

sopra  steria

# 01

—  
Cyber  
Sécurité  
&  
Intelligence  
Artificielle



Welcome  
TO THE  
Jungle



sopra  steria



# INTRO

Intelligence artificielle  
et cybersécurité, piliers de  
la transformation numérique et...  
secteurs créateurs d'emplois!

Le numérique s'est immiscé dans toutes nos activités, privées comme professionnelles. Il transforme nos façons de nous informer, d'acheter, de nous déplacer, de travailler, de nous divertir, etc. Cette transformation numérique est possible grâce aux importants progrès réalisés dans plusieurs domaines, notamment en intelligence artificielle (IA). Conséquence de cette évolution, la malveillance et le crime ont eux aussi migré vers le monde numérique, et la cybersécurité a évolué pour réagir à ces nouvelles menaces. Ces domaines nécessitant de nouvelles compétences et de nouveaux profils, les métiers associés offrent des perspectives de carrière attractives en constante évolution.

## **L'intelligence artificielle, un ensemble de disciplines d'ores et déjà utilisées au quotidien en entreprise**

L'IA ne date pas d'aujourd'hui. Le mathématicien Alan Turing a été le premier à poser la question «les machines peuvent-elles penser?» dans l'article Computer machinery and Intelligence, publié en 1950. En 1956, le scientifique Marvin Minsky, qui avait déjà évoqué les réseaux de neurones dans sa thèse en 1951 et qui co-fondra ensuite le groupe d'IA du Massachusetts Institute of Technology (MIT), parle pour la première fois d'IA lors de la conférence de Dartmouth, une «école d'été» organisée avec d'autres chercheurs.

Il n'y a pas «une» définition de l'IA, en tout cas, pas une qui fasse l'unanimité! L'IA regroupe plusieurs disciplines scientifiques, comme par exemple les moteurs de règles, les apprentissages machine (supervisé ou

non, deep learning, réseaux de neurones, big data) ou encore les arbres de décisions ou la programmation par contraintes. Cette

## **«L'intelligence artificielle, un ensemble de disciplines d'ores et déjà utilisées au quotidien en entreprise... parfois sans le savoir.»**

gamme de technologies permet de reproduire certaines des capacités de l'intelligence humaine : la perception (reconnaissance d'images, de sons), le raisonnement (si... alors... sinon), la mémorisation (référence à des éléments connus), etc.

Alors pourquoi l'IA suscite-t-elle aujourd'hui un tel engouement? Depuis ses débuts, elle a connu des hauts et des bas. Les capacités qu'on lui prêtait ont suscité de forts enthousiasmes auxquels ont succédé de profondes désillusions. Le regain d'intérêt qu'elle connaît depuis le début des années 2010, particulièrement dans le domaine de l'apprentissage, tient à ce que l'on dispose à la fois de la puissance de calcul et des grands volumes de données nécessaires pour lui faire réaliser différentes tâches. L'IA est aujourd'hui utilisée pour la compréhension de la parole et du langage naturel (assistants conversationnels Siri, Alexa), pour la traduction instantanée (Google Traduction, Skype Translator), mais aussi pour la reconnaissance de formes (tri et localisation d'objets), la planification d'actions et le raisonnement faisant appel à de l'analyse de données, etc.

Et l'IA est déjà bien présente dans notre quotidien, partout où elle exécute plus vite voire mieux que les humains des tâches répétitives qui prennent du temps ou qui ont une faible valeur ajoutée. Elle permet de réaliser des programmes complexes qui ne sont habituellement pas à la portée des composants logiques classiques. Les robots qui simplifient notre travail au quotidien peuvent alors utiliser ces technologies d'IA, qui les rendront plus performants et plus à même de s'adapter à leur environnement. Ils seront alors en mesure de mieux collaborer avec l'homme pour augmenter son efficacité opérationnelle, assurer la meilleure expérience possible aux clients de l'entreprise et faciliter la conception de nouveaux produits.

Un assistant conversationnel répond à nos questions, il apprend à nous connaître pour diffuser la musique ou les informations que nous préférons, il appelle ou envoie un message directement sur le portable de la personne que nous voulons joindre, etc. Nos voitures savent déjà se garer - presque - toutes seules et très bientôt, elles trouveront l'itinéraire le mieux adapté pour nous amener là où nous voulons aller pendant qu'un logiciel triera pour nous les e-mails les plus urgents ou les plus pertinents.

Les entreprises utilisent de plus en plus massivement les technologies d'IA pour améliorer leur efficacité opérationnelle et assurer la meilleure expérience possible à leurs clients. Grâce au big data par exemple, l'IA analyse d'importants volumes de données pour identifier les clients dont la fidélité diminue ou ceux à qui proposer un nouveau produit. Elle détecte les risques de fraude, les vulnérabilités informatiques ou les cyberattaques. Associée au RPA (robotic process automation), elle automatise le traitement d'opérations comme traiter



et répondre à une demande de prêt, de rendez-vous ou de formation.

### **Possibilités et limites de l'intelligence artificielle**

Pour bien utiliser l'IA, il faut en connaître ses potentialités, mais aussi ses limites. Un algorithme d'IA peut battre le champion du monde aux échecs ou au jeu de Go en apprenant les règles de ces jeux. Mais là où un enfant saura distinguer une pomme d'une poire ou un âne d'un cheval après en avoir vus quelques-uns, il faudra des centaines voire des millions d'exemples à un algorithme pour qu'il en fasse autant, et encore avec une marge d'erreur non négligeable.

Le fonctionnement des outils utilisant l'IA reste par ailleurs fondamentalement différent de la façon de fonctionner d'un être humain. Et c'est dans la collaboration entre l'humain et le logiciel que l'IA trouve toute sa place et sa valeur. L'IA amène une capacité à digérer de grandes quantités de données et à présélectionner les informations pertinentes tandis que l'être humain apporte lui son expérience, son raisonnement, son intuition et sa conscience dans le choix de la solution.

Si un algorithme a regardé des centaines de milliers de radiographies et qu'on lui a appris à reconnaître les tâches suspectes qui pourraient indiquer un cancer, il peut rapidement proposer un pré-diagnostic aux médecins. Ceux-ci n'ont plus qu'à vérifier les images et à valider ou infirmer le diagnostic.

### **Le rôle de la cybersécurité**

La transformation numérique en cours dans toutes nos activités a accéléré le développement d'une autre discipline:

la cybersécurité. Maintenant que toute la valeur, la richesse, la connaissance sont dématérialisées, la convoitise, la malveillance et le crime se sont eux aussi adaptés au numérique. Pendant longtemps, les attaques ont essentiellement consisté en des virus pour PC qui causaient peu de dégâts et faisaient la fierté de leurs auteurs, qui en revendiquaient la paternité.

Le monde a considérablement changé. Aujourd'hui, le cybercrime est l'œuvre d'officines criminelles structurées et organisées comme de véritables entreprises quand il n'est pas piloté par des Etats. Vol de données personnelles, rançonnement par chiffrement de systèmes complets, destruction à distance de fichiers stratégiques, blocage de sites via des attaques par déni de service, piratage d'objets connectés comme les caméras de surveillance sans parler de la diffusion d'infos, etc, les armes du cybercrime sont devenues aussi dangereuses que celles du monde physique.

### **Des dégâts considérables causés par les cybercrimes**

Ces attaques vont jusqu'à mettre en danger la survie des entreprises attaquées, notamment celles cotées en bourse, comme cela a été le cas en 2017 avec les attaques par ransomware NotPetya et WannaCry qui ont touché de nombreuses sociétés dans le monde, dont Saint-Gobain en France. Déjà fin 2014, les employés de Sony Pictures avaient découvert un matin que leurs postes de travail étaient bloqués par un ransomware. En fait, les pirates, installés depuis plusieurs semaines dans le système informatique de l'entreprise, avaient volé plusieurs films pas encore diffusés, les

e-mails des dirigeants et les données relatives au personnel. La société a mis des mois à se redresser. Plus récemment, des attaques ransomware d'un genre nouveau ont été menées contre des entreprises françaises, dans les secteurs de l'aéronautique et de l'industrie. Les dégâts, longs à évaluer, se chiffreront en dizaines de millions d'euros et affecteront durablement les entreprises visées.

La cybersécurité est devenue un métier essentiel pour l'entreprise, au même titre que la gestion des ressources humaines, le marketing ou la production. Avec une difficulté supplémentaire: si la menace est constante et les attaques lourdes de conséquences, elles sont difficiles à détecter car invisibles. Parfois, elles ne sont déclenchées que longtemps après avoir été installées dans les systèmes




---

**« Dans un monde de plus en plus interconnecté où l'entreprise échange des données avec ses fournisseurs, ses partenaires et ses clients, il faut protéger les réseaux, les serveurs, les postes de travail, les objets connectés, mais aussi les données. »**

---

informatiques de l'entreprise où elles n'agissent que par petites touches. La plupart ne sont repérées qu'après plusieurs mois. Et les cybercriminels, qui font preuve d'une grande créativité, renouvellent sans cesse leurs techniques d'attaque. La cybersécurité nécessite donc une veille permanente.

#### **Des métiers variés, des carrières passionnantes**

Grâce aux importants progrès accomplis récemment dans son domaine, l'IA vient au secours des responsables de la sécurité informatique des entreprises. Des algorithmes d'IA sont à même de détecter des comportements atypiques au cœur même des systèmes d'information (SI), ils sont notamment utilisés pour lutter contre la fraude. D'autres logiciels peuvent identifier si un e-mail est un spam ou si sa pièce jointe est suspecte. D'autres encore savent repérer des tentatives d'intrusion ou de saturation du réseau.

De nouveaux métiers liés à l'IA sont apparus depuis le début des années 2010. La plupart sont essentiellement centrés

sur les données, c'est le cas des data scientists. Ils développent les modèles et les algorithmes qui aideront l'entreprise à tirer le meilleur parti de ses données. Le rôle des « fouilleurs » de données, alias les data miners, consiste à identifier, à nettoyer et à analyser les données pour y dénicher des relations qui serviront à optimiser l'activité de l'entreprise. D'autres nourrissent et entraînent les modèles algorithmiques de machine learning, on les appelle les « éleveurs » ou les « entraîneurs » de robots, etc. Enfin, les questions de responsabilité, d'éthique et de conformité des usages de l'IA donnent elles aussi naissance à de nouveaux métiers.

Pour se protéger des cyber-risques, les entreprises créent des équipes dédiées en interne. De plus en plus souvent, elles nomment un responsable de la sécurité des systèmes d'information (RSSI) et utilisent les services d'un SOC (security operations center), interne ou externalisé auprès d'un prestataire, pour détecter les incidents de sécurité et y réagir. Mais leurs équipes ne couvrent pas toujours l'ensemble de leurs besoins, tant la pénurie de compétences est criante dans la cybersécurité, domaine qui évolue rapidement et de manière constante. C'est pourquoi les entreprises comme Sopra Steria sont de plus en plus sollicitées par leurs clients pour les accompagner dans la définition et la mise en œuvre de leurs stratégies de cybersécurité, les aider à mettre en place des mesures de prévention, des solutions de protection ainsi que des services de détection et de réaction.

Les enjeux sont multiples. Dans un monde de plus en plus interconnecté où l'entreprise échange des données avec ses fournisseurs, ses partenaires et ses clients, il faut protéger les réseaux, les serveurs, les postes de travail, les objets



connectés, mais aussi les données. Et ce, que les infrastructures soient dans des data centers propres à l'entreprise ou dans le cloud.

#### **Le cycle de la donnée en toute sécurité**

Sopra Steria met son expertise au service de ses clients sur tout le cycle du traitement des données et de la cybersécurité des SI. En IA, levier de la transformation numérique, les consultants et les ingénieurs de Sopra Steria accompagnent les entreprises tout au long de leurs projets ainsi que dans l'optimisation de leurs performances. Assistants vocaux, maintenance prédictive, aide à la décision ou intelligence collective, ils conçoivent et réalisent les nouvelles solutions au service de l'entreprise, de ses clients et de ses collaborateurs.

L'entité dédiée à la cybersécurité intervient à chaque étape du cycle de vie sur des domaines d'expertise

clés: gouvernance, gestion des risques et conformité (CRC), protection des applications et des données ou encore SOC. La cybersurveillance fait appel à des compétences pointues de détection et de gestion d'attaques ou d'intrusion, de veille via un CERT (computer emergency response team), d'enquêtes numériques (ou forensique) et de gestion de crise. Cela se traduit dans les métiers d'ingénieur, d'analyste ou de consultant spécialisés

---

**«Les formations à l'IA, la data science et la cybersécurité se multiplient mais les effectifs sont encore insuffisants pour couvrir les besoins des entreprises.»**

---

en cybersécurité. Les audits techniques, comme les tests d'intrusion, requièrent également des compétences techniques avancées et fortement recherchées. En effet, il faut pouvoir détecter les risques ainsi que les vulnérabilités pour être en mesure de les gérer.

À ces sujets s'ajoutent les aspects liés à la conformité réglementaire qui sont de plus en plus présents. Le règlement général de protection des données (RGPD) mis en œuvre en Europe le 25 mai 2018 illustre combien la mise en conformité peut être complexe. Les profils des consultants en conformité réglementaire sont atypiques: ils sont dotés d'une double compétence juridique et SI pour adapter la mise en conformité à la réalité opérationnelle du client.

Tous ces métiers, qui n'existent pour la plupart d'entre eux que depuis peu, offrent d'importantes perspectives à des profils variés, curieux et désireux de progresser dans un univers en constante évolution. Sopra Steria leur assure des programmes de formation et de certification en phase avec les nombreuses innovations de leur domaine ainsi que des évolutions de carrière rapides et stimulantes.

Les formations à l'IA, la data science et la cybersécurité se multiplient mais les effectifs sont encore insuffisants pour couvrir les besoins des entreprises. De fait, la transformation numérique multiplie les opportunités tout comme les perspectives d'avenir dans ces métiers. Ces technologies, dont les appellations sont encore très génériques, se structureront en nombreux sous-domaines pour répondre à la spécialisation croissante de leurs applications. En même temps que les travaux de recherche et développement en cours feront progresser les outils, les intitulés des postes vont se préciser et se multiplier. Un ingénieur en IA pour conduite autonome aura besoin d'un spécialiste en conformité des données et des procédures d'accès pour s'assurer que le système qu'il développe respecte les Ws en vigueur. Les entreprises feront appel à des consultants en data science et à des experts des tests d'intrusion pour s'assurer de la résilience de leurs SI. Un expert de l'IA sera amené à travailler avec un chirurgien, un logisticien ou un juriste pour concevoir les solutions dont il aura besoin. Car l'IA et la cybersécurité sont entrées dans notre quotidien et elles vont y rester, longtemps!

les

INTELLIGENCE

ARTIFICIELLE

fiches métiers .



# Consultant en cybersécurité et digital trust

## en bref

**Le consultant en cybersécurité et en digital trust est avant tout un consultant. Il est au service de clients, essentiellement des grands comptes, pour les aider à définir leur stratégie de cybersécurité et à la mettre en œuvre, ainsi qu'à augmenter la confiance accordée par leurs utilisateurs de produits digitaux via des stratégies visant à améliorer la crédibilité, la transparence, la sécurité et l'intégrité de ces outils.**

## LES MISSIONS

Concrètement, le consultant en cybersécurité et en digital trust accompagne les entreprises sur différentes problématiques :

- Dans un contexte de numérisation généralisée, il aide à évaluer les risques et les menaces propres à l'activité de l'entreprise. Il réalise des audits pour identifier les besoins et participe à la définition puis à la mise en œuvre des stratégies de prévention les mieux adaptées pour détecter toute tentative d'intrusion. Son rôle est d'anticiper ce qui peut se passer pour éviter les attaques. Il met en place des tests de vulnérabilité pour s'assurer de l'efficacité des solutions mises en place. En cas d'attaque, il aide l'entreprise à réagir, éventuellement à riposter et participe activement à la gestion de crise.

**Exemples de projets :** identification des points critiques de l'infrastructure informatique, définition des règles de sécurité, choix d'une solution de détection d'intrusion, sensibilisation et formation des personnels etc...

- La transformation numérique engendre des volumes de données de plus en plus importants quel que soit le secteur d'activité de l'entreprise (banque, industrie, commerce, énergie, etc...). Ces données stratégiques pour l'entreprise font partie intégrante de son patrimoine. La mission du consultant en cybersécurité et en digital trust est d'évaluer le risque lié à ces données et d'apporter le juste niveau de cybersécurité pour les protéger.

**Exemples de projets :** mise en œuvre d'une solution de gestion des identités et de contrôle des accès (IAM) aux serveurs de l'entreprise, mise en place d'un plan de reprise d'activité, récupération des données et des applications après incident etc...

- Le consultant contribue à la conformité numérique de l'entreprise, condition nécessaire pour susciter et conserver la confiance des clients. Il participe à la mise en œuvre des réglementations en vigueur, notamment celles relatives au respect de la vie privée et à la confidentialité des données.

**Exemples de projets :** conformité RGPD, audit de conformité, référentiels de sécurité, suivi des licences logicielles etc...

## LES OUTILS ET LANGAGES À MAÎTRISER

Vous maîtrisez bien l'anglais, tant à l'écrit qu'à l'oral, ainsi que le pack Office.

## LES QUALITÉS ESSENTIELLES À AVOIR

Attiré par les métiers du conseil, vous avez le goût du challenge. Vous possédez les qualités du consultant, et des qualités rédactionnelles et relationnelles. Vous alliez rigueur et passion, autonomie et esprit d'équipe.

## LA VEILLE

Vous êtes au courant de l'actualité en cybersécurité et en conformité numérique. Vous suivez les comptes Twitter et LinkedIn de personnes et d'entreprises du secteur ainsi que les blogs et la presse spécialisés (le Blog du Hacker, Cyberini, Sécurité & Défense magazine, MagSecurs etc...).

## les formations

Niveau bac+5, vous démarrez ou vous avez déjà une expérience en tant que consultant auprès de clients grands comptes et la cybersécurité vous attire. Le métier de consultant en cybersécurité et en digital trust existe depuis peu, c'est pourquoi les entreprises vous aideront souvent à construire votre carrière en vous proposant des formations certifiantes adaptées à votre parcours.

## qui recrute ?

Vous travaillez essentiellement pour des ESN et des cabinets de conseil.

## la rémunération

La fourchette de salaire (brut annuel) pour un débutant : **37 - 40 k€**

La fourchette de salaire (brut annuel) pour un confirmé : **45 - 70 k€**



# Architecte IA

## en bref

**Grâce à sa double compétence en architecture de solutions logicielles et en IA, l'architecte en IA conçoit et structure des écosystèmes intelligents robustes, performants et évolutifs qui apportent des réponses efficaces aux besoins des clients. Il est la personne clé de tout projet qui met en œuvre de l'IA.**

## LES MISSIONS

Pour bâtir ces écosystèmes, l'architecte IA identifie sur le marché les composants les mieux adaptés. Si nécessaire, il supervise la construction de composants intelligents spécifiques par des experts IA. Capable de vulgariser les problématiques, il a un rôle d'interface entre les spécialistes et les consultants.

**Exemples de projets :** architecture de modules de traitement de sons, d'images et de vidéos, conception de plateformes de chatbots, d'outils d'analyse prédictive ; élaboration de processus de traitement automatique d'e-mails, de robots d'interaction etc...

## LES OUTILS ET LANGAGES À MAÎTRISER

Vous suivez les innovations et les travaux de recherche menés dans les domaines de l'architecture de solutions et de l'IA pour maintenir vos compétences au meilleur niveau.

Vous connaissez les environnements de développement et les outils de modélisation et de présentation.

Vous maîtrisez les plateformes d'IA disponibles chez les principaux CSP ainsi que les services de type AutoML, DL, TensorFlow. Vous connaissez les repositories d'algorithmique et de datasets disponibles sur Kaggle ou GitHub.

Vous maîtrisez bien l'anglais tant à l'écrit qu'à l'oral.

## LES QUALITÉS ESSENTIELLES À AVOIR

Communicant et pédagogue, vous avez un très bon relationnel et un bon esprit d'équipe. Vous faites grandir et transmettez votre savoir aux équipes que vous accompagnez. Vous faites preuve d'agilité et n'hésitez pas à vous remettre en question pour tenir compte des avancées technologiques dans vos domaines. Expert passionné par les innovations, vous avez à cœur de construire des écosystèmes intelligents qui soient durables.

## LA VEILLE

Vous suivez les sections « research » des grands acteurs du secteur (CAFA, IBM, Microsoft, etc...) et les sites des laboratoires des écoles, instituts et universités qui travaillent dans ces domaines (AfIA, INRIA, etc). Vous suivez également des sites comme Hacker News ou arXiv.

## les formations

De formation bac+5, vous avez un diplôme d'ingénieur ou équivalent. Un master d'informatique ou de mathématiques spécialisé en IA, Android, reconnaissance des formes, ou un graduate degree en IA et advanced visual computing constituent un plus indéniable. Éventuellement, vous avez un master spécialisé en big data et en cloud.

## qui recrute ?

Vous travaillez avec les équipes de conseil, d'innovation, de projet, de R&D appliquée ou fondamentale pour des ESN, des start-ups, des PME, des CSP ou des prestataires de cybersécurité. Vous travaillez en entreprise ou chez des clients.

## la rémunération

La fourchette de salaire (brut annuel) débutant à confirmé : **37 - 80 ke**



# Consultant conformité réglementaire - cybersécurité

## en bref

La transformation des sociétés induite par le numérique, la migration des applications dans le cloud, l'ouverture des SI aux partenaires et aux clients, ainsi que la forte augmentation des actes de cybercriminalité ont conduit à la multiplication des réglementations et des législations dans le domaine numérique. Le consultant en conformité réglementaire - cybersécurité aide les clients à se mettre en conformité avec ces réglementations. Il possède des connaissances à la fois dans le domaine juridique sur la protection des données et en cybersécurité sur les normes qui s'appliquent aux SI.

## LES MISSIONS

Le consultant en conformité réglementaire - cybersécurité assure la veille juridique et technologique afin de garantir à ses clients une transformation de leurs SI sécurisée et conforme à la réglementation.

Ses missions de conseil et d'audit consistent à :

- aider le client à définir sa stratégie de conformité du SI, la classification des données et leur sécurité
- définir les politiques de sécurité adaptées aux contraintes légales qui s'appliquent en matière de sécurité des SI
- concevoir et mettre en œuvre les programmes de (re)mise en conformité du SI
- assurer la conformité tant des projets informatiques aux contraintes légales que celle des opérations de cybersécurité au cadre légal de cybersurveillance
- effectuer les contrôles de conformité du SI

## LES OUTILS ET LANGAGES À MAÎTRISER

Vous maîtrisez le pack Office. Vous connaissez bien RGPD ainsi que les normes ISO 27001 et 27005.

## LES QUALITÉS ESSENTIELLES À AVOIR

Vous savez conjuguer votre solide culture juridique et de bonnes connaissances en informatique pour aider à identifier les mesures techniques les mieux adaptées aux règles juridiques applicables. Vous êtes à la fois proactif, dynamique, curieux et avez une bonne aisance relationnelle. En plus de ces qualités,

le métier de consultant exige de la flexibilité et une grande mobilité.

## LA VEILLE

Vous suivez l'actualité de vos domaines et développez votre réseau de contacts sur Twitter et LinkedIn. Vous pratiquez la veille sur les blogs et la presse spécialisés tant dans les domaines juridiques qu'en cybersécurité (Legalis, Dalloz, Lextenso, Global Security Mag etc).

## les formations

Vous êtes titulaire d'un master 2 en droit, idéalement en NTIC/ gestion de la conformité.

## qui recrute ?

Vous travaillez essentiellement pour des ESN et des cabinets de conseil.

## la rémunération

La fourchette de salaire (brut annuel) pour un débutant : **37 - 40 k€**

La fourchette de salaire (brut annuel) pour un confirmé : **45 - 70 k€**



# Expert produit cloud

## en bref

**L'expert produit cloud aide les entreprises à réussir la migration de leurs applications et de leurs données dans le cloud. Il assiste les clients dans la définition de leur stratégie, le choix des solutions, leur mise en œuvre et leur intégration au SI.**

## LES MISSIONS

L'expert produit cloud fait vivre et évoluer l'infrastructure cloud de l'entreprise en gérant les phases de conception, de réalisation, de sécurisation et d'intégration. Il conçoit et dimensionne l'architecture de l'ensemble du SI ou d'une partie du SI: urbanisation, systèmes, composants applicatifs et techniques, infrastructures, piles logicielles, etc...

Il assure la viabilité à la fois technique et économique de la solution ainsi que sa maintenabilité, son évolutivité, sa pérennité, sa sécurité et ses performances.

Il définit les cadres techniques et propose l'élaboration de solutions innovantes. Il participe et encadre la conception et la réalisation de ces solutions en s'assurant de leur conformité. Enfin, il participe à l'animation de la communauté d'experts et de l'équipe en charge de l'innovation.

**Exemples de projets:** migration d'application, accompagnement des équipes, gestion financière des opérations (FinOps), transformation numérique etc...

## LES OUTILS ET LANGAGES À MAÎTRISER

Dans le domaine du cloud où l'évolution est constante, vous êtes certifié pour un ou plusieurs CSP comme AWS, Azure, Google, etc...

Vous maîtrisez bien l'anglais professionnel.

## LES QUALITÉS ESSENTIELLES À AVOIR

Vous avez été sensibilisé aux méthodes agiles, qui vous permettent de travailler en étroite collaboration avec les métiers. Vous savez anticiper les modes de production, de fabrication et d'exploitation. Tout à la fois proactif, curieux et rigoureux, vous êtes reconnu pour votre écoute et vos capacités d'analyse et d'innovation.

Grâce à d'excellentes qualités relationnelles, vous vous adaptez à vos interlocuteurs, «métier» ou «technique»; vous savez présenter et convaincre à haut niveau, DSI, RSSI ou directions métiers, et ce en interne comme en externe.

## LA VEILLE

Vous vous informez continuellement sur le cloud et sur le numérique en général. Vous suivez les comptes Twitter et LinkedIn de spécialistes et d'entreprises du secteur ainsi que leurs blogs et la presse spécialisés.

## les formations

Niveau bac+5 au minimum, vous avez un diplôme d'ingénieur ou équivalent.

## qui recrute ?

Vous travaillez aussi bien pour des start-ups que des PME ou des ESN, dans des équipes agiles et de consultants.

## la rémunération

La fourchette de salaire (brut annuel) débutant / confirmé: **34 - 65 k€**



# Ingénieur sécurité MCO au sein d'un SOC

## en bref

**Deux acronymes pour un métier stratégique !  
L'ingénieur sécurité MCO garantit le maintien en condition opérationnelle (MCO) du security operations center, le SOC. Il apporte une vraie valeur ajoutée technique à la sécurité de l'information.  
Il travaille dans une équipe qui rassemble des ingénieurs sécurité et des analystes SOC.**

## LES MISSIONS

Les missions se déroulent au sein du SOC des clients, souvent en environnement international.

Le rôle de l'ingénieur sécurité MCO au sein d'un SOC est de :

- configurer les équipements du SOC (matériels et logiciels) pour permettre la récupération des informations de sécurité
- conseiller le client en fonction de son contexte et des préconisations de l'éditeur de sa solution
- créer, modifier et optimiser les alertes de sécurité
- mettre en place et assurer le monitoring des données collectées pour le client
- garantir le MCO des outils du SOC
- enquêter sur les causes d'incidents, alerter le client et rétablir le service pour assurer le bon fonctionnement du système

## LES OUTILS ET LANGAGES À MAÎTRISER

Vous maîtrisez les environnements Unix et/ou Windows. Vous avez des compétences en installation, configuration, exploitation, optimisation, déploiement et MCO des architectures réseau (commutateur - routeur - firewall).

Idéalement, vous connaissez les outils RSA, QRadar, Splunk, OSSIM, FireEye, SourceFire, etc... Vous êtes à l'aise avec les créations de scripts et la manipulation de fichiers Excel. Vous avez déjà eu l'occasion d'utiliser des RegEx.

Vous maîtrisez bien l'anglais, tant à l'écrit qu'à l'oral.

## LES QUALITÉS ESSENTIELLES À AVOIR

Vous conciliez rigueur, autonomie et force de proposition. Curieux, vous vous auto-formez et savez vous documenter. Lors des investigations, vous faites preuve de sens logique et de discernement. Vous savez prendre du recul et estimer rapidement l'impact de vos actions. Vous fonctionnez en mode agile, vous avez appris à maîtriser les procédures sans vous y limiter.

## LA VEILLE

Vos missions sont liées aux solutions d'un éditeur. Vous pratiquez une veille ciblée sur cet éditeur et les solutions équivalentes. Vous suivez l'actualité en cybersécurité et développez votre réseau de contacts sur Twitter et LinkedIn. Vous consultez régulièrement les blogs et la presse spécialisés (le Blog du Hacker, InfoSecurity, TrendLabs Security Intelligence, Hacker News etc).

## les formations

Niveau bac+4/5 en informatique, vous avez une première expérience en système et réseau sur un SI critique et/ou à forte visibilité. Grâce à cette expérience, vous êtes capable d'identifier rapidement les éléments critiques à surveiller dans un SI (système, réseau, applicatifs) et d'en décliner les remontées d'informations nécessaires de façon pertinente.

## qui recrute ?

Vous travaillez essentiellement pour des ESN et des cabinets de conseil.

## la rémunération

La fourchette de salaire (brut annuel) pour un débutant : **37 - 40 k€**

La fourchette de salaire (brut annuel) pour un confirmé : **45 - 70 k€**



# Consultant IA

## en bref

**Le consultant en IA met sa connaissance du domaine au service des clients. Il les accompagne dans leurs projets qui visent à améliorer leur efficacité opérationnelle, conçoit les solutions et réalise les traitements complexes qui répondent à leurs attentes. Il s'appuie pour cela sur sa bonne connaissance et sa maîtrise des différentes technologies de l'IA que sont le ML, le DL, le NLP, les systèmes multi-agents, la résolution de contraintes, les systèmes experts...**

## LES MISSIONS

Le consultant IA est l'interlocuteur privilégié des clients tout au long des projets. Il tient compte des spécificités du contexte de son intervention pour choisir les outils et les méthodes les mieux adaptés parmi tous ceux que propose l'IA. Il veille tout particulièrement à éclairer et à limiter les différents biais qui pourraient affecter la solution.

**Exemples de projets :** conception et réalisation de modules de traitement d'images et de vidéos, de chatbots, d'outils d'analyse prédictive; élaboration de processus de traitement automatique d'e-mails; réalisation d'assistants ou de conseillers virtuels; définition du comportement d'un robot social etc...

## LES OUTILS ET LANGAGES À MAÎTRISER

Vous disposez d'une bonne culture technologique générale dans le domaine de l'IA puisque les applications croisent de multiples disciplines et technologies. Vous enrichissez vos domaines de compétence au fur et à mesure des projets. Vous faites évoluer votre capacité à réaliser des services «intelligents» et évolutifs, qui pourront être réutilisés dans d'autres applications et dans le cloud.

Vous connaissez parfaitement les langages Python, C++, JavaScript, les bibliothèques TensorFlow, Keras et les frameworks Caffe et Jade.

Vous maîtrisez bien l'anglais, tant à l'écrit qu'à l'oral.

## LES QUALITÉS ESSENTIELLES À AVOIR

Doté(e) de fortes compétences informatiques, vous avez également un très bon relationnel et un bon esprit d'équipe.

## LA VEILLE

Vous suivez les comptes Twitter et LinkedIn de spécialistes et d'entreprises du domaine. Vous faites de la veille sur différents blogs et sites tels que KDnuggets, AfIA, INRIA, ActuaIA etc...

## les formations

De formation bac+5, vous avez un diplôme d'ingénieur ou équivalent. Un diplôme complémentaire (neurosciences, linguistique, philosophie, droit, biologie, physique, marketing...) est de plus en plus apprécié. Un master d'informatique ou de mathématiques spécialisé en IA, Android, reconnaissance des formes, ou un graduate degree en IA et advanced visual computing constituent un plus indéniable.

## qui recrute ?

Vous travaillez avec les équipes de consultants, d'innovation ou de réalisation de projet pour des ESN, des start-ups, des éditeurs de logiciels ou chez les clients finaux (grands groupes, entreprises de taille intermédiaire ou PME). Généralement en équipes pluridisciplinaires, vous partagez votre temps entre des moments d'échanges avec les utilisateurs et des moments de réflexion, de recherche et d'implémentation des solutions développées.

## la rémunération

La fourchette de salaire (brut annuel) débutant à confirmé : **37 - 80 k€**



# Architecte cloud

## en bref

**Plus qu'un nouveau métier, le métier d'architecte cloud est une évolution de celui d'architecte en SI. Dans le contexte de transformation numérique et de migration de tout ou partie des infrastructures et des applications vers le cloud, la conception des solutions doit prendre en compte de nombreux paramètres nouveaux. L'architecte s'assure de la cohérence transversale des applications, de la bonne intégration des solutions cloud au SI existant et de la maîtrise des coûts des ressources. C'est pourquoi ses missions sont multiples.**

## LES MISSIONS

Concrètement, l'architecte cloud :

- Contribue au développement des nouvelles solutions qui vont être hébergées dans le cloud, que celui-ci soit public, privé ou hybride. Il participe à la définition des architectures fonctionnelles et techniques, à la rédaction du cahier des charges, au choix des solutions, à la mise en œuvre technique des infrastructures. Une tâche importante de son poste est d'assurer le maintien en condition opérationnelle des solutions déployées dans le cloud, c'est-à-dire de faire en sorte qu'elles fonctionnent harmonieusement et en cohérence avec les autres applications au fil du temps, et qu'elles continuent de répondre aux besoins des métiers.

**Exemples de projets :** migration vers le cloud du système de communication Skype ou de la suite bureautique Office 365 de Microsoft, déploiement d'un ERP dans le cloud pour des filiales à l'étranger

- Veille à ce que ces solutions répondent précisément aux besoins des utilisateurs tout en étant alignées sur les enjeux métiers et en conformité avec la stratégie de l'entreprise. Il doit aussi assurer la sécurité de leur utilisation, en coopération avec les équipes dédiées de la DSI. Enfin, il doit avoir des notions de FinOps (financial and operations), c'est-à-dire participer activement à la gestion des contrats liés au cloud et à la maîtrise des coûts afin d'éviter les dérapages financiers.

**Exemples de projets :** réintégration dans le cloud privé d'une solution exploitée jusque-là sur un cloud public pour des raisons de sécurité et de cohérence des applicatifs

- Participe à la définition des standards d'architecture qui tiennent compte des performances, des conditions de sécurité et des coûts des solutions. Il rédige les différentes documentations qui serviront de références dans l'entreprise. Il expertise les nouveaux produits, solutions ou modèles qui apparaissent sur le marché afin d'en évaluer la pertinence pour l'entreprise.

**Exemples de projets :** détermination des conditions d'utilisation d'une technologie de conteneurs pour les applications ou de plateformes de cloud public

## LES OUTILS ET LANGAGES À MAÎTRISER

Dans le domaine du cloud où l'évolution est constante, vous êtes certifié pour un ou plusieurs CSP comme AWS, Azure, Google, etc...

Vous maîtrisez bien l'anglais professionnel.

## LES QUALITÉS ESSENTIELLES À AVOIR

Vous avez été sensibilisé aux méthodes de développement agiles, qui vous permettent de travailler en étroite collaboration avec les métiers. Vous savez anticiper les modes de production, de fabrication et d'exploitation.

Grâce à d'excellentes qualités relationnelles, vous vous adaptez à vos interlocuteurs, métier ou technique; vous savez présenter et convaincre à haut niveau, DSI, RSSI ou directions métiers, et ce en interne ou en externe.

## LA VEILLE

Vous vous informez continuellement sur le cloud. Vous suivez les comptes Twitter et LinkedIn de spécialistes et d'entreprises du secteur ainsi que leurs blogs et la presse spécialisés...

## la rémunération

Niveau bac+5 au minimum, vous avez un diplôme d'ingénieur ou équivalent.

## qui recrute ?

Vous travaillez aussi bien pour des start-ups que des PME ou des ESN, dans des équipes agiles et de consultants.

## la rémunération

La fourchette de salaire (brut annuel) débutant / confirmé :  
40 - 70 ke

# Tanguy Le Floch

23 ans

• Data Scientist



## Comment êtes-vous devenu data scientist ?

• **TANGUY LE FLOCH** – J'ai toujours été très intéressé par les données. Après mon baccalauréat, j'ai directement intégré l'Université Technologique de Compiègne (UTC), qui prépare au diplôme d'ingénieur. J'étais en classe préparatoire intégrée, appelée le Tronc Commun à l'UTC. J'ai alors suivi un cours sur les systèmes experts. C'était une entrée dans le monde de l'IA que j'ai beaucoup aimée. J'ai suivi la filière « fouille de données et décisionnel ». Tout ce que j'adore : des mathématiques, des statistiques, de l'informatique et de l'IA.

« Il y a un mythe autour duquel il faudrait avoir des années d'expérience avant d'espérer faire ce métier. »

Quand j'ai effectué mes premières recherches de stage, j'avais entendu dire que le métier de data scientist n'était pas immédiatement accessible après les études : il y a un mythe autour duquel il faudrait avoir des années d'expérience avant d'espérer faire ce métier. J'ai donc recherché des stages dans le secteur, sans espérer être data scientist et j'ai commencé à me former à l'IA. C'est à ce moment-là que Sopra Steria m'a contacté ! J'ai rencontré

le responsable du Data Lab, une branche du centre d'expertise digitale (CED), qui m'a expliqué son projet : il constituait une équipe de data scientists pour réunir en un même lieu toutes les compétences de ce vaste domaine. La reconnaissance de formes ou le traitement du langage naturel demandent en effet des savoir-faire très différents.

## Qu'est-ce qui vous plaît dans ce poste ?

• **T. LE F.** – Tout d'abord, en tant que data scientist, je travaille au quotidien sur ce que j'aime : réaliser des calculs et des mathématiques, lire des articles de recherche et coder de la manière la plus élégante et efficace possible tout en répondant à des problématiques clientes concrètes. Ensuite j'aime le contact avec les clients. Pour répondre à leurs enjeux business, il faut commencer par comprendre leur métier et entendre leur besoin. Cela demande donc des compétences d'écoute et d'empathie.

## À quoi ressemblent vos journées ?

• **T.LEF.** – Les projets commencent toujours par la compréhension du problème du client : il faut s'approprier son métier. Parallèlement, on explore les données, on essaie différentes visualisations, on extrait des patterns. Puis on produit. La production varie en fonction de la demande du client. Cela peut consister à déterminer si un facteur en influence un autre ou à élaborer un modèle prédictif par exemple.

### Quelles sont les difficultés que vous rencontrez au quotidien?

• **T. LE F.** – Plutôt que de difficultés, je parlerais d'une exigence pour la rigueur, qui est indispensable dans le monde de la data science. Nous sommes nombreux et nous avons tous des backgrounds différents. Nous devons donc avoir des pratiques de développement communes pour que chacun

« Nous devons donc avoir des pratiques de développement communes. »

puisse récupérer le travail des autres et l'utiliser. Pour ce faire, nous nous devons d'être rigoureux. C'est d'autant plus important en data science car nous fonctionnons par boucle «essai-erreur». Il faut aussi prendre le temps au quotidien d'échanger sur notre code et nos productions.

### Quels outils utilisez-vous?

• **T. LE F.** – Le langage Python, l'IDE PyCharm et l'outil Jupyter Notebook, qui permet d'exécuter des cellules de codes et d'obtenir rapidement le résultat. Tout cela s'accompagne d'un ensemble de librairies Python pour répondre à nos besoins comme Scikit-Learn, NumPy, Pandas ou encore TensorFlow.

### Comment pensez-vous que le métier de data scientist va évoluer?

• **T. LE F.** – Je pense qu'il va connaître de profondes mutations dans les années à venir! L'IA générera elle-même les modèles les plus simples. On voit déjà que l'automated machine learning prend de l'ampleur. Le métier de data scientist va donc évoluer pour devenir un consultant expert en compréhension des données et être en mesure de répondre à la question suivante «qu'est-ce qui doit être automatisé?»: son travail sera de challenger les outils et d'en expliquer les résultats.

### Quels conseils donneriez-vous à un étudiant qui voudrait devenir data scientist?

• **T. LE F.** – Je conseillerais d'avoir l'équivalent du niveau d'un diplôme d'ingénieur en statistiques pour être en mesure de comprendre les données et les calculs. Des compétences en informatique sont également nécessaires car 60% du travail consiste à coder. Enfin, il faut s'intéresser à la data science, aller sur Kaggle, essayer des choses sur des datasets, pratiquer Python, etc. pour se construire sa propre réflexion de base.

# Clarisse Rivon

28 ans

Consultante cybersécurité



## Comment êtes-vous devenue consultante cybersécurité ?

• **CLARISSE RIVON** – Pas tout à fait par hasard, mais presque ! À la base j'ai une formation d'ingénieure en matériaux, métier que j'ai exercé pendant un an après mon diplôme chez un prestataire d'études. Mais j'avais envie d'autre chose. J'aimais beaucoup le collaboratif, l'accompagnement des clients et le fait de pouvoir les conseiller, etc. J'étais intéressée par le secteur de l'informatique, mais je ne voulais pas faire uniquement de la programmation. C'est à ce moment-là que Sopra Steria m'a proposé une reconversion pour devenir consultante en cybersécurité. Je me suis renseignée pour savoir en quoi cela consistait exactement. On m'a expliqué qu'il s'agissait surtout d'être curieuse, d'aimer apprendre et d'avoir des connaissances en informatique. J'ai suivi une formation de 3 mois au cours de laquelle j'ai passé 4 certifications dont celles de lead auditor et de risk manager. Puis j'ai enchaîné avec une période d'intégration de 3 mois en mission au sein de l'entité cybersécurité de Sopra Steria.

## Sur quels projets travaillez-vous ?

• **C. R.** – La cybersécurité fait partie de tous les projets. Je suis actuellement spécialisée en GRC et je travaille sur la protection des données et la conformité au nouveau règlement général entré en vigueur en mai 2018 (RGPD). J'ai travaillé sur des missions d'analyses de risques pendant lesquelles j'ai accompagné les équipes clients pour les aider à détecter les risques cyber associés à leurs

projets et à mettre en œuvre des mesures pour les réduire. Je rencontre les clients, je prends connaissance de leurs besoins, des projets en cours et des données qu'ils recueillent, et je leur propose des solutions pour qu'ils soient en conformité avec ce règlement. Et quand cela sort de mon domaine, je remonte les messages vers l'équipe technique. Mais mon domaine de spécialisation pourra être amené à évoluer dans le futur.

## Qu'est-ce qui vous plaît dans ce métier de consultante cybersécurité ?

• **C. R.** – La diversité des missions principalement ! Les journées ne se ressemblent pas. Il faut faire des recherches et savoir changer de regard pour voir les choses du point de vue du client.

## À quoi ressemble votre quotidien aujourd'hui à ce poste ?

• **C. R.** – Je passe une grande partie de mon temps à faire de la veille et à trier les informations pour sélectionner celles que je veux conserver, celles qui me seront utiles dans mon travail. Je suis également quotidiennement en contact avec les clients puisque je suis garante du fonctionnement des projets et des réponses apportées à leurs besoins. Je fais donc régulièrement des points avec eux.

## Quels outils utilisez-vous ?

• **C. R.** – La maîtrise d'outils techniques de cybersécurité n'est pas essentielle à mon métier, qui est un poste de consultant avant tout. La suite Office, les e-mails et l'utilisation d'outils collaboratifs sont donc les outils que j'utilise au quotidien.

## Quelles difficultés rencontrez-vous à votre poste ?

• **C. R.** – Ce qui me paraît parfois difficile pour l'instant est de comprendre l'ensemble des enjeux d'un projet ou les technologies que je ne connais pas. Un exemple tout simple qui date de mes débuts sur le poste : quand on me parlait d'une application faisant appel à une API, je devais comprendre ce qu'était une API. Aussi, la sécurité et la conformité ont longtemps été perçues comme des empêcheurs d'avancer, mais cela évolue, car les gens commencent à prendre conscience des risques.

## Comment pensez-vous que votre métier va évoluer ?

• **C. R.** – Il y aura toujours besoin de consultants en cybersécurité, et ce de plus en plus en raison de l'augmentation de la volumétrie des données récoltées et stockées. Ainsi, il n'est pas rare que des entreprises proposent des formations de reconversion pour des profils n'ayant pas de formation initiale en cybersécurité. Ces consultants nouvellement formés auront l'avantage d'apporter un regard

neuf sur les sujets rencontrés en missions. Par ailleurs, un des gros enjeux auquel nous devons faire face aujourd'hui est la migration des données dans le cloud et évidemment leur sécurisation. Ce mode de stockage et de traitement des données à distance pose de nouvelles questions en matière de sécurité. D'ailleurs, j'ai dit à mon responsable que je souhaitais me spécialiser dans ce domaine, acquérir des connaissances. C'est quelque chose que j'apprécie chez Sopra Steria ! Non seulement j'ai fait une reconversion et j'ai été formée, mais cela continue, je peux faire des formations et évoluer dans ma carrière.

## Quels conseils donneriez-vous à un jeune qui voudrait se spécialiser en cybersécurité ?

• **C. R.** – La cybersécurité est un domaine très vaste, qui évolue en permanence. Personne ne le connaît entièrement ni ne connaît tous les métiers. Il faut donc être très curieux, se poser des questions et en poser aux autres, aller sur les réseaux sociaux, échanger, discuter, etc. Aujourd'hui, de nouveaux enjeux apparaissent avec la généralisation des systèmes cloud et l'externalisation des espaces de stockage des données : on voit les structures physiques (les data centers) des entreprises disparaître au profit d'infrastructures virtuelles (le cloud) qui sont elles-mêmes hébergées par les éditeurs. Cette transformation va en s'amplifiant et génère de nombreuses offres d'emploi en cybersécurité. S'orienter vers une formation en cybersécurité spécialisée dans le cloud est donc une bonne opportunité, jusqu'à la prochaine évolution !

# Axel Gogenmos

23 ans

Consultant Data Scientist



## Comment êtes-vous devenu consultant data scientist ?

• **AXEL GOGENMOS** – Au début je ne connaissais pas cette discipline. Après un bac scientifique, j'ai fait des études en génie électrique et informatique industrielle. Pendant ma dernière année aux Arts et Métiers ParisTech, j'ai suivi une spécialisation en SI qui comportait une introduction à la data science. J'ai découvert qu'il s'agissait en fait de beaucoup de mathématiques, ainsi que des statistiques et de l'informatique. Et cela m'a bien plu ! Sopra Steria proposait un projet de reconnaissance d'images par rayons X pour détecter des armes dans les bagages à l'aéroport, j'ai trouvé que c'était un défi intéressant pour mon stage de fin d'études de 6 mois.

## Aujourd'hui, quel est votre poste ?

• **A. G.** – Je suis consultant au Data Lab de Sopra Steria, une branche de notre centre d'expertise digitale (CED) composée exclusivement de data scientists (une vingtaine en ce moment). La plupart sont ingénieurs d'écoles ou d'universités, tous arrivent d'horizons très variés : physique, mathématiques, biologie, etc. L'objectif d'un tel centre de compétences est de réaliser des missions de data science chez nos clients disposant déjà de nombreuses données à exploiter. L'ambiance est très bonne ! D'ailleurs, on se retrouve régulièrement en dehors du bureau.

## À quoi ressemble votre quotidien à ce poste ?

« Je travaille avec des langages et des bibliothèques de DL et de ML comme Python, R, Keras (TensorFlow) et SciKit-Learn pour les principaux. »

À l'issue de mon stage, on m'a proposé un CDI, que j'ai accepté, après avoir rencontré plusieurs personnes de Sopra Steria qui m'ont indiqué les missions sur lesquelles j'allais être amené à intervenir.

• **A. G.** – Il n'y a pas de journée type ! Disons qu'en moyenne, je passe 25% du temps en réunions avec les autres membres du Data Lab, des consultants ou des clients pour faire des points d'avancement des projets et récupérer les briefs clients. Je rédige des rapports et je fais du PowerPoint pendant environ 30% de mon temps. Et enfin je travaille sur des données, je code, je teste, je corrige pendant environ 45% de mon temps. J'apprécie l'ensemble des missions de mon poste mais ce que je préfère, c'est cette partie sur la data science, c'est-à-dire quand je suis sur les données ! J'utilise des langages et des bibliothèques de DL et de ML comme Python, R, Keras (TensorFlow) et SciKit-Learn pour les principaux.

### Sur quels projets travaillez-vous ?

• **A. G.** – Depuis que j’ai intégré le Data Lab, j’ai eu l’occasion de travailler sur plusieurs projets. Mon premier projet consistait à faire des scripts de vérification de données, un sujet formateur même s’il faisait moins appel à la créativité. Aujourd’hui, je travaille sur de la reconnaissance de caractères et de l’extraction d’entités, et cela m’intéresse

« Il n’existe pas une formation unique. »

beaucoup plus. Les missions, qui durent en moyenne un mois, sont très variées et concernent des secteurs très différents. C’est ce qui me plaît ! Au Data Lab, on réalise des POC (proof of concept) pour des clients, mais nous ne sommes pas des développeurs. Donc, après le POC, on passe le relais à l’équipe de développement.

### Quelles sont les difficultés que vous rencontrez en tant que consultant data scientist ?

• **A. G.** – Je rencontre parfois des problèmes que je ne sais pas résoudre. Cela m’est arrivé récemment sur des séries temporelles, par exemple. Dans ce cas, je n’hésite pas à demander de l’aide à un autre data scientist. Nous avons tous des profils et des compétences très différents. Certains sont forts en

mathématiques, d’autres en statistiques ou en informatique. La data science est un domaine très vaste, qui utilise des technologies très variées, cela va des réseaux de neurones à la vérification de bases de données. Il n’existe pas une formation unique.

### Comment pensez-vous que ce métier va évoluer ?

• **A. G.** – Je pense qu’il va évoluer vers plus de spécialisation. Demain, les data scientists seront plus nombreux et plus spécialisés. J’imagine aussi qu’il existera des modules déjà développés que l’on pourra assembler pour résoudre un problème donné. Du coup, on pourra passer plus de temps avec les clients.

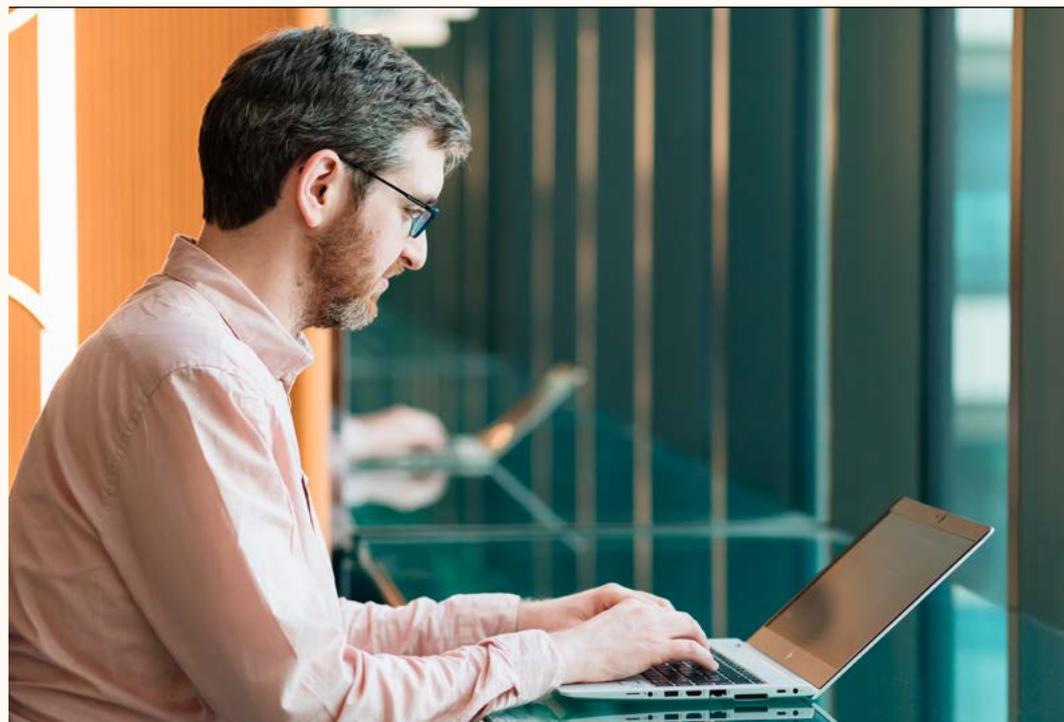
### Quels conseils donneriez-vous à un étudiant qui voudrait devenir consultant data scientist ?

• **A. G.** – Ça tient en quelques mots : avoir des bases solides en mathématiques et en statistiques, faire des concours et des projets, sur Kaggle par exemple, et suivre l’actualité ! Il faut aussi maîtriser l’anglais, surtout en lecture, pour pouvoir lire les nombreux articles sur le sujet qui sont la plupart du temps écrits dans cette langue.

# Corentin Chiron

32 ans

• Leader Technique SIEM



## Comment êtes-vous devenu leader technique SIEM ?

• **CORENTIN CHIRON** – Après une classe préparatoire, je suis entré à Télécom SudParis, une école d'ingénieurs de l'Institut Mines-Télécom, initialement pour faire de l'électronique. Mais lors des différents cours, je me suis finalement tourné vers la sécurité. A l'époque, il était question de firewalls, d'audits, de créations de réseaux sécurisés, etc. Cela m'a plu. Mon projet de fin d'études portait sur la sécurité sur Android.

« C'est une fonction utile, il s'agit de protéger les entreprises. »

J'ai ensuite eu la chance de découvrir les multiples volets de la cybersécurité grâce à mes différents postes : consultant cybersécurité chez Altran, analyste SOC chez Thales, puis à la gestion des menaces, qu'on appelle le "threat management", chez Orange Cyberdefense. C'est là que j'ai découvert le security information and event management, le SIEM, notamment la solution QRadar d'IBM.

## Qu'est-ce qui vous a attiré vers la cybersécurité ?

• **C. C.** – C'est une fonction utile, il s'agit de protéger les entreprises ! Surtout qu'elles n'ont

souvent pas conscience des risques et que les attaques sont de plus en plus nombreuses.

## À quoi ressemblent vos journées ?

• **C. C.** – Il n'y en a pas deux pareilles ! Nous conseillons les clients sur l'architecture à mettre en place puis nous réglons et faisons vivre la solution déployée. Mais cette solution diffère d'un client à l'autre, car leurs SI sont différents.

## Sur quels projets travaillez-vous ?

• **C. C.** – En tant que leader technique SIEM, autrement dit responsable technique de l'équipe d'intégration, j'installe des solutions SIEM pour nos clients. Un SIEM est un système complexe qui récupère les logs du système d'information de l'entreprise et enregistre des millions de données chaque jour – des gigaoctets ! Le second volet du SIEM consiste à analyser les données collectées, les corréliser pour détecter des anomalies et remonter des alertes. C'est de l'analyse comportementale en quasi temps réel, donc très rapide sur des machines très puissantes. Nos projets commencent souvent par une prise de conscience des dangers, car les entreprises ne sont pas assez matures sur ce sujet. Or il ne s'agit plus seulement de virus, mais de menaces diverses comme par exemple des ransomwares et des phishing. Après avoir installé une solution SIEM, nous la réglons pendant les premiers mois pour enlever le « bruit », les faux positifs et améliorer son efficacité. Un projet dure environ 6 mois.

Compte tenu de la diversité des technologies et des clients, les projets varient en fonction des enjeux des clients et de leur maturité sur leur niveau de sécurité. Aucun projet ne se ressemble.

## Quels outils utilisez-vous ?

• **C. C.** – Nous intégrons plusieurs solutions SIEM : QRadar d'IBM, RSA NetWitness et Splunk essentiellement. Nous utilisons des outils d'administration Linux, des scripts Python ou Perl, et des outils de parsing, d'extraction de données, comme RegEx. Et bien sûr, la suite Office pour faire des dossiers d'architecture, d'installation, d'exploitation ou de maintien en condition d'exploitation opérationnelle.

## Quelles sont les difficultés que vous rencontrez à votre poste ?

• **C. C.** – Il y a beaucoup de projets en ce moment, car les obligations légales font que les entreprises prennent conscience des risques et donc veulent s'équiper. Nous travaillons donc pour de nombreux clients. J'en gère 3 ou 4 en même temps. Cela demande de la rigueur, il faut être carré. D'autant plus que l'équipe est en train de monter en puissance !

## Comment pensez-vous que votre métier va évoluer ?

• **C. C.** – Il évolue dans trois directions. D'abord, il concerne de plus en plus l'industrie,

c'est-à-dire que nous commençons à installer des SIEM dans des systèmes informatiques industriels de type SCADA, systèmes de contrôle et d'acquisition de données. Ensuite, le cloud pose de nouveaux problèmes, par exemple, comment récupérer les logs et les données lorsqu'une application est hébergée dans un cloud public comme Azure ou AWS ? Enfin, les objets connectés seront le prochain domaine à intégrer au SIEM.

## Quels conseils donneriez-vous à un étudiant qui voudrait se spécialiser en cybersécurité ?

• **C. C.** – Il y a beaucoup d'opportunités car ce sont des métiers en tension. Il faut aimer travailler en équipe et donc bien s'entourer. Bien sûr, il faut un solide bagage technique, connaître le fonctionnement du protocole IP, les systèmes d'exploitation, etc. Surtout, je crois qu'il faut être curieux, avoir envie d'apprendre, mais aussi se remettre en question car la cybersécurité évolue très vite !

# LEXIQUE

## DES ABRÉVIATIONS.

Chaque industrie a ses propres codes et ses nombreux acronymes. Voici le lexique indispensable pour vous y retrouver!

CERT	Computer Emergency Response Team
CSP	Cloud Solution Provider
DL	Deep Learning
DSI	Directeur/Directrice/Direction des Systèmes d'Information
ERP	Enterprise Resource Planning
ESN	Entreprise de Services du Numérique
GRC	Gouvernance/Gestion des Risques et Conformité

IA	Intelligence Artificielle
IDE	Integrated Development Environment
MCO	Maintien en Condition Opérationnelle
ML	Machine Learning
NLP	Natural Language Processing
NTIC	Nouvelles Technologies de l'Information et de la Communication
POC	Proof Of Concept
RGPD	Règlement Général de Protection des Données
RPA	Robotic Process Automation
RSSI	Responsable de la Sécurité des Systèmes d'Information
SI	Systèmes d'Information
SIEM	Security Information & Event Management
SOC	Security Operations Center

Welcome  
TO THE  
Jungle



sopra  steria



Welcome  
to the  
Jungle

|

sopra  steria

**01**

— Cyber Sécurité & Intelligence Artificielle