

LES MÉTIERS DE LA SÉCURITÉ DU NUMÉRIQUE : SÉCURITÉ DES SYSTÈMES D'INFORMATION OU CYBERSÉCURITÉ

La cybersécurité est devenue un enjeu majeur pour toutes les organisations, qu'il s'agisse des entreprises ou des institutions publiques. Il est important que la sécurité dans une organisation ne soit pas vécue comme une peur de l'attaque mais comme une "stratégie de réussite" des produits ou des projets, stratégie rentable qui plus est ! Les éléments de sécurité doivent donc être mis en œuvre dès la conception des produits, d'où le renforcement du poids des experts en sécurité dans les entreprises.

DES PLACES À PRENDRE !

Secteur en forte progression, le numérique recrute beaucoup et peine parfois à pourvoir tous les postes proposés. C'est encore plus vrai dans le secteur de la cybersécurité où les offres d'emplois sont largement plus nombreuses que les candidats susceptibles d'y répondre !

Cette pénurie trouve son explication dans le fait que la cybersécurité est une activité relativement récente (seules les banques y recouraient il y a dix ans) : c'est donc un secteur encore mal connu et dans lequel les formations spécifiques sont donc encore peu nombreuses.

On compte aujourd'hui près de 25.000 salariés dans la filière mais ce nombre devrait très rapidement croître. Compte tenu de la concentration des grandes entreprises en région parisienne, les emplois sont majoritairement situés autour de Paris : 7 offres sur 10 émanent d'entreprises situées en Ile-de-France.

DES MÉTIERS VARIÉS QUI SE MULTIPLIENT...

Les métiers liés à la cybersécurité sont très divers et souvent mal connus. Au-delà des compétences techniques très pointues qui sont requises, un certain nombre de compétences transversales revêtent elles aussi une grande importance, selon les employeurs : adaptabilité et flexibilité, respect des règles de confidentialité, curiosité intellectuelle, communication écrite et orale, anglais en contexte professionnel.

DOMAINE PROFESSIONNEL : Pilotage, organisation et gestion des risques

MÉTIERS

Responsable de la Sécurité des Systèmes d'Information (RSSI)

Expérience : 5 à 10 ans

Ayant généralement une expérience professionnelle de plusieurs années, le RSSI définit la politique de sécurité du système d'information et veille à sa mise en application. Il joue un rôle de conseil, d'assistance, d'information, de formation et d'alerte auprès de la direction. Selon la taille de l'entité, il joue un rôle opérationnel dans la mise en œuvre de la politique de sécurité ou encadre une équipe composée d'experts techniques et de consultants. Il propose à l'autorité compétente la politique de sécurité du SI et veille à son application. Il peut intervenir en matière de SSI sur tout ou partie des systèmes informatiques et télécoms de son entité, tant au niveau technique qu'organisationnel. Il effectue un travail de veille

technologique et réglementaire sur son domaine et propose les évolutions qu'il juge nécessaires pour garantir la sécurité du système d'information dans son ensemble. Il est l'interface reconnue des exploitants et des chefs de projets, mais aussi des experts et des intervenants.

Métiers associés : OSSI : Officier de la sécurité des systèmes d'information – ISSM : Information Systems Security Manager – CISO : Chief Information Security Officer – CSO : Chief Security Officer

Correspondant sécurité

Expérience : quelques années dans un ou plusieurs domaines « métier » et formation continue en sécurité

Assure un rôle d'intermédiaire ou de relai entre le RSSI, à qui il remonte des tableaux de bord, et les lignes métiers. Selon les organisations, il s'agit d'une fonction à temps partiel ou à temps plein. Sa forte proximité avec le métier lui permet d'intervenir sur des thématiques de gestion des risques, de gouvernance et de sensibilisation auprès des utilisateurs. En particulier, il a pour rôle d'analyser, de concevoir, d'intégrer ou de mettre en œuvre les techniques de sécurisation dans le cadre de son domaine « métier ». Maîtrisant les référentiels des domaines « métier », il est en mesure de faire converger les objectifs de sécurité et de sûreté de fonctionnement. Il conduit des analyses de risques et propose des solutions résilientes afin de minimiser sans concession les impacts « métiers ». Il peut être amené à conseiller les directions métiers, contribuer à l'expression de besoin globale et technique de sécurité en conception, en intégration et en gestion de la sécurité. À ce titre, il dispose d'une compétence et d'une expérience dans son domaine métier et d'une compétence dans le domaine de la sécurité, souvent acquise à travers la formation continue (courte ou longue).

Métiers associés : CSSI : Correspondant Sécurité du Système d'Information – Gestionnaire de Risques cyber – Expert connexe – CRO : Correspondant risques opérationnels – Assistant RSSI

Spécialiste en gestion de crise cyber

Expérience / niveau de diplôme : Bac+5

Le spécialiste en gestion de crise cyber conseille l'organisme pour lui permettre de disposer d'une capacité de gestion de crise majeure dédiée aux systèmes d'information, ou avec un volet cyber prépondérant.

Il organise la gestion de crise pour :

- agir et résoudre la crise
- communiquer l'état de la crise aux personnes et aux organismes concernés
- coordonner l'action des différentes parties en présence

Il limite les volets organisationnels, l'entraînement et la simulation aux acteurs susceptibles d'intervenir en cas de crise majeure liée aux systèmes d'information et à leurs interlocuteurs métiers ou support concernés (gestionnaire de crise, RSSI, responsables de l'ingénierie, administrateurs systèmes / données). À un niveau plus opérationnel et sous la pression d'une attaque en cours, le profil de gestionnaire de crise peut être également identifié dans la catégorie « maintien en condition opérationnelle ».

Métiers associés : Cyber Defense Infrastructure Support Specialist

Responsable du plan de continuité d'activité (RPCA)

Expérience / niveau de diplôme : Bac+4/5 et 3 ans d'expérience

Élabore et met en œuvre dans son organisation un Plan de Continuité d'Activité (PCA)

DOMAINE PROFESSIONNEL : Management de projets et cycle de vie

MÉTIERS

Chef de projet sécurité

Expérience / niveau de diplôme : Bac+5 et 3 à 5 ans d'expérience

S'assure de la bonne prise en compte des aspects sécurité liés au développement d'un projet.

En général, le chef de projet sécurité assiste le chef de projet sur ces aspects.

Les tâches associées à ce métier peuvent être :

- analyse des besoins de la sécurité (analyse de risques, cible de sécurité)
- sécurité du développement
- prise en compte des aspects liés aux évaluations/audits de la sécurité
- tests liés à la sécurité
- formation des utilisateurs

À ce titre, le métier peut être considéré comme spécifique à la sécurité. Tous les projets ne nécessitant pas la présence d'un chef de projet sécurité, la responsabilité de ces aspects peut être prise en charge par le chef de projet qui s'appuie ponctuellement sur des experts du domaine.

Métiers associés : Chef de projet sécurité informatique – Chef de projet sécurité des systèmes d'information – Security Project Manager Officer (PMO) – Program Manager – IT program manager

Développeur sécurité

Expérience / niveau de diplôme : Bac+5

Le développeur de sécurité assure le sous-ensemble des activités d'ingénierie nécessaire au développement de logiciels (spécifications, conception, codage, production de binaire, assemblage, tests, gestion des sources, gestion de configuration, gestion des faits techniques, archivage, documentation) répondant à des exigences de sécurité. En plus de sa connaissance des fondamentaux de la SSI qui lui permet de comprendre les problématiques à traiter et de ses compétences en développement, on attend du développeur sécurité des connaissances dans les domaines des vulnérabilités, des contre-mesures logicielles et/ou matérielles, des règles de développement sûr (au sens de la sécurité), des langages et de leurs propriétés, des chaînes de développement et de leur paramétrage, du test (de sécurité) et éventuellement des méthodes formelles. Il développe de façon méthodique, en appliquant des règles de conception / codage / tests (qu'il définit au besoin ou qu'il contribue à définir) et s'assure que les composants qu'il produit sont testables en termes de conformité fonctionnelle, de robustesse (tests aux limites et hors limites), de sécurité (résistance aux attaques identifiées en entrée de la conception) et de performance. Ses compétences lui permettent également de faire des revues, audits ou évaluations de code (Secure Software Assessor, Source Code Auditor).

Note : toute personne faisant du développement devrait avoir été initiée à la prise en compte des bonnes pratiques et des méthodes pour limiter l'introduction de vulnérabilités de construction. Cette initiation est typiquement ce que propose une formation labellisée CyberEdu. Le métier décrit ici correspond à une spécialité qui va au-delà de ce que l'on attend d'un développeur formé.

Architecte sécurité

Expérience / niveau de diplôme : Bac+3 à Bac+5 – 5 à 10 ans d'expérience

L'architecte de sécurité structure les choix techniques, technologiques et méthodologiques d'un ensemble [système, logiciel] répondant à des exigences de sécurité. Il s'assure de la déclinaison des exigences techniques (fonctionnalités à offrir, contraintes de performance, d'interopérabilité, d'interchangeabilité, de robustesse, d'intégration de solutions sur étagère, d'exportabilité) selon des critères de coût, d'efficacité, de stabilité, de maîtrise, de niveau de risque, de respect des standards, d'aptitude à la production, au déploiement et à la maintenance MCO (Maintien en Condition Opérationnelle) et MCS (Maintien en Condition de Sécurité). Il valide la cartographie du système d'information et s'assure notamment que les hypothèses de sécurité relatives à l'environnement de son architecture sont clairement énoncées et prises en compte dans sa conception.

Il veille à ce que les exigences de sécurisation applicables aux différents constituants de son architecture ou aux outils permettant de la produire soient effectivement mises en œuvre. Il prépare les dossiers de conception et de justification sur les aspects sécurité. Il participe à la conception de l'architecture et de l'implémentation du produit ou système à développer en s'assurant que les différentes briques disposent du niveau de sécurité adapté aux contextes du projet sur les aspects techniques, usages, métiers...

Métiers associés : Architecte Sécurité Informatique – Architecte Réseaux et Télécom – System architect – Information Security Architect – Security architect

Intégrateur de sécurité

Expérience / niveau de diplôme : Bac+3 à Bac+5

L'intégrateur de sécurité système analyse et prend en charge les volets sécurité (objectifs, niveau de criticité et attentes en termes de résilience) en liaison avec l'architecte informatique et/ou l'architecte sécurité et programmes dans l'infrastructure. Il définit et met en œuvre des plates-formes nécessaires à l'intégration des solutions (services ou produits de sécurité) dans les nouvelles applications. Il planifie, coordonne, en relation avec les autres secteurs concernés (systèmes, réseaux, système de gestion base de données, etc.), les besoins d'intégration exprimés. Il installe des composants matériels, des composants logiciels ou des sous-systèmes supplémentaires dans un système existant ou en cours de développement, respecte les processus et procédures établis (i.e. gestion de configuration) en tenant compte de la spécification, de la capacité et de la compatibilité des modules existants et des nouveaux modules afin de garantir intégrité et interopérabilité. Il contribue à la qualification technique et à l'intégration dans l'environnement de production. Il documente les processus de mise en œuvre, de mise à jour et d'exploitation des composants de sécurité et organise les conditions de mise en œuvre du maintien en condition de sécurité.

DOMAINE PROFESSIONNEL : Opération et maintien en condition opérationnelle

MÉTIERS

Administrateur sécurité

Expérience / niveau de diplôme : Bac+3

Met en œuvre la politique de sécurité de l'entreprise et administre des solutions de sécurité de type antivirus, antispam, IPS, la gestion des habilitations (départ, arrivée, mobilité) et les

dérogations. En général, la fonction d'administration de la sécurité est une des fonctions de l'administrateur système/réseaux. Mais certaines organisations peuvent dédier des personnes à ce seul métier. Ces personnes agissent alors en complément des administrateurs réseaux et systèmes.

Métiers associés : Administrateur Sécurité Informatique -Opérateur en sécurité des systèmes d'information – System Administrator -Cyber Defense Infrastructure Support Specialist

Technicien sécurité

Expérience / niveau de diplôme : Bac+2/3

Le technicien sécurité est responsable d'activités de support, de gestion ou d'administration de la sécurité aux plans technique ou administratif : conception, production, conditionnement et gestion des réseaux de chiffrement et des éléments secrets. Selon le profil d'emploi et la formation reçue, il est en mesure de déployer et d'administrer des solutions de gestion de la sécurité, ainsi que de paramétrer les éléments de sécurité des équipements serveurs et des terminaux traitants. Il est en capacité d'effectuer des tâches de contrôle administratif de conformité dans les domaines des habilitations du personnel, du suivi comptable et des inventaires réglementaires, de l'application des procédures d'exploitation de sécurité, apportant ainsi son soutien aux opérations d'audit et de contrôle. Il contribue aux séances de sensibilisation pour l'usage des ressources par les utilisateurs finaux.

Métiers associés : Technicien support SSI – Télé-assistant – Technical Support Specialist

DOMAINE PROFESSIONNEL : Support et gestion des incidents

MÉTIERS

Analyste SOC

Expérience / niveau de diplôme : Bac+3

Paramètre les systèmes de supervision de la sécurité (SIEM, sondes, honeypots, équipements filtrants). Catégorise, analyse et traite les alertes de sécurité de façon régulière pour en améliorer l'efficacité. Assure la détection, l'investigation et la réponse aux incidents de sécurité. Dans le domaine de la cybersécurité, l'analyste SOC analyse et interprète les alertes, les événements corrélés et recherche les vulnérabilités.

Métiers associés : Analyste Cyber SOC – Analyste détection d'incident – Veilleur-Analyste – Cyber Defense Analyst

Expert réponse à incident

Expérience / niveau de diplôme : Bac+3 à Bac+5

Analyse et traite les incidents de sécurité au sein d'une structure ou d'une équipe de réponse à incident. Communique et fournit des recommandations de sécurité aux services clients de la cellule de réponse à incident. L'expert en réponse à incident travaille sous forte contrainte pour reprendre la main lors d'attaques/compromissions de systèmes d'information. Disposant de la cartographie du système d'information, il doit interagir avec les experts en investigation numérique (afin d'appréhender rapidement le contexte) et les architectes qui maîtrisent le système d'information. Il formule des recommandations de mesures de contournement et de mesures d'urgence et d'amélioration des capacités de détection (journalisation notamment).

Métiers associés : Spécialiste en investigation numérique – Analyste traitement d'incident - Cyber Crime Investigator – Forensics Analyst – Cyber Defense Forensics Analyst

DOMAINE PROFESSIONNEL : Conseil, audit et expertise

MÉTIERS

Consultant sécurité « organisationnel »

Expérience / niveau de diplôme : Bac+4/5 – Qualification ANSSI possible : PASSI

« Consultant » est un terme générique souvent utilisé par les sociétés de services pour désigner toute personne en mesure de prodiguer des conseils à un client. Dans le domaine de la sécurité, on peut distinguer les consultants intervenant plutôt sur les aspects organisationnels ou non techniques de la sécurité de ceux qui interviennent dans les domaines techniques.

Typiquement, le consultant organisationnel effectuera des prestations dans tout ou partie des domaines suivants :

- travaux méthodologiques
- analyses de risques
- activités d'analyse de risques, d'audit, de gestion de projet sécurité
- définition et mise en place de politiques de sécurité ou de systèmes de management de la sécurité
- entraînement au management de la sécurité
- etc.

Ses compétences peuvent l'amener à réaliser des prestations d'audit dans tout ou partie des domaines précédemment cités.

Métiers associés : Consultant sécurité – Consultant gouvernance, risques et conformité – Consultant en SSI – Auditeur organisationnel – Lead auditor – Lead implementer – Systems auditor -Information security auditor

Consultant sécurité « technique »

Expérience / niveau de diplôme : Bac+4/5 – Qualification ANSSI possible : PASSI

« Consultant » est un terme générique souvent utilisé par les sociétés de services pour désigner toute personne en mesure de prodiguer des conseils à un client. Dans le domaine de la sécurité, on peut distinguer les consultants intervenant plutôt sur les aspects organisationnels ou non techniques de la sécurité de ceux qui interviennent dans les domaines techniques.

Selon son domaine d'expertise, le consultant technique effectuera des prestations dans les domaines suivants :

- les travaux en lien avec les applications et les services sécurisés (mise en œuvre et configuration, analyse de la sécurité...)
- les travaux en lien avec les systèmes d'exploitation (mise en œuvre et configuration, audit de configuration, test de pénétration...)
- les travaux en lien avec les réseaux (mise en œuvre et configurations d'équipements sécurité, test de pénétration...)
- les travaux en liens avec du matériel (mesures de signaux compromettants, analyse logique, conception de produits matériels sécurisés...)
- la rétro ingénierie (logicielle ou matérielle)
- la cryptographie (implémentation sûres... pour ce thème voir « Cryptologue »)

Source : www.onisep.fr/www.ssi.gouv.fr

A jour > mars 2021

- l'analyse post-mortem (investigation numérique, forensique)
- et de manière générale, les activités à caractère technique ou scientifique.

Ses compétences peuvent l'amener à réaliser des prestations d'audit dans tout ou partie des domaines précédemment cités.

Métiers associés : Auditeur technique sécurité et test d'intrusion – Pen testeur -Expert audit sécurité et intrusion – Spécialiste cybersécurité – Expert technique -Consultant sécurité – Security Control Assessor – Vulnerability Assessment Analyst – Ethical Hacker – Penetration tester – Vulnerability assessor

Cryptologue

Expérience / niveau de diplôme : Bac+5 à doctorat

Il apporte son expertise dans tout ou partie des domaines suivants :

- utilisation d'algorithmes cryptographiques
- utilisation / conception de protocoles cryptographiques
- gestion des clés
- implémentation sécurisée d'algorithmes cryptographiques
- utilisation de bibliothèques cryptographiques
- évaluation de l'utilisation et de l'implémentation d'algorithmes cryptographiques
- analyse cryptographique

Exceptionnellement, il peut être amené à concevoir des algorithmes cryptographiques.

Métiers associés : Expert crypto – Cryptographer – Cryptanalyst

Juriste spécialisé en cybersécurité

Expérience / niveau de diplôme : Bac+5/6

Le juriste spécialisé en cybersécurité est un expert du droit des technologies de l'information et de la communication qui est spécialiste des thèmes et des corpus concernés par la cybersécurité, la cybercriminalité et la protection des données à caractère personnel. Il peut opportunément présenter une expérience d'avocat à même d'éclairer la direction sur les conséquences pénales ou civiles d'une cyberattaque, dès lors qu'une décision voire la gestion d'une crise avec une composante « cybersécurité » requiert son expertise.

Conseil de la direction en matière de responsabilités civile et pénale, il se tient informé des évolutions de la réglementation internationale, européenne et nationale. Il effectue une veille juridique depuis le simple projet jusqu'à la publication et l'entrée en vigueur des textes régissant les conflits armés, le droit des affaires (notamment le secret des affaires) ainsi que la jurisprudence, en différenciant selon que la décision est un cas d'espèce ou au contraire amène des réflexions plus générales sur la pratique du droit.

Métiers associés : Consultant juridique en cyberdéfense – Cyber Legal Advisor

Évaluateur sécurité

Expérience / niveau de diplôme : Bac+5

Le métier concerne les laboratoires qui réalisent les évaluations de la sécurité des technologies de l'information et les développeurs de produits devant être évalués.

- Côté évaluateur :

L'évaluateur sécurité vérifie la conformité d'un produit, voire d'un système, par rapport à sa spécification de sécurité (cible de sécurité...) selon des critères et une méthode normalisée ou réglementaire (CC, CSPN...) ou privée (PCI, EMVCo...). Le résultat de cette évaluation peut donner lieu à une certification (ou assimilée).

– Coté développeur :

Les mêmes compétences peuvent être utilisées chez les développeurs de produits ou de systèmes qui doivent subir une évaluation sécurité. En termes de titre, on parlera plutôt de « responsable évaluation » ou de « responsable certification ». Son rôle est de gérer la relation avec les laboratoires qui réalisent les évaluations, de s'assurer que toutes les fournitures attendues sont disponibles etc.

Métiers associés : Responsable évaluation – Responsable certification – System Testing and Evaluation Specialist

Analyste de la menace

Expérience / niveau de diplôme : Bac+3/5

De niveau licence à master, l'analyste peut contribuer à plusieurs domaines d'activité de la cybersécurité, dans les domaines de :

- l'anticipation technologique avec de la veille technique
- l'anticipation dans le domaine du renseignement sur les menaces, avec de l'analyse d'impact des codes d'exploitation (activités CERT et intégrateur de solutions)
- l'anticipation en conduite pour évaluer les dommages subis par un système compromis, participer à la conception de la solution technique visant à restituer le service et apporter ses compétences de spécialiste en matière de mise en œuvre des principes de sécurisation SSI.

Il peut contribuer au schéma directeur et à l'urbanisation sécurisée des systèmes.

Métiers associés : Threat Intelligence

Délégué à la Protection des Données (DPD)

Expérience / niveau de diplôme : Bac+5 – 10 ans d'expérience

S'assure que les données personnelles sont traitées par l'entreprise conformément aux règles internes et aux lois en vigueur.

Métiers associés : Correspondant informatique et libertés (CIL) – Data protection officer (DPO) – Privacy Compliance Manager – Privacy officer – Data protection officer