LES MÉTIERS DE LA CYBERSÉCURITÉ

Virulentes, massives, en mutation constante, les attaques informatiques menacent chaque jour le fonctionnement des organisations… si ce n'est leur survie. Et les structures publiques comme privées en prennent progressivement conscience ! Elles sont nombreuses à partir en quête de nouvelles recrues expertes en cybersécurité.

Or, les spécialistes en cybersécurité sont aujourd'hui des perles rares. L'intérêt pour la filière est grandissant, mais le vivier de talents peine encore à répondre à l'importance des besoins. Et ces profils sont d'autant plus difficiles à dénicher que le champ des missions et compétences de la cybersécurité est vaste, complexe, hétérogène. Soit, difficile à appréhender pour qui n'y est pas familier.

Ce panorama propose une nomenclature complète des métiers de la cybersécurité, élaboré par l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI).

Gestion de la sécurité et pilotage des projets de sécurité

• Directeur Cybersécurité

Au sein de grandes organisations, le Directeur Cybersécurité est un cadre dirigeant en charge de définir la stratégie de cybersécurité de manière à répondre aux enjeux de cybersécurité de l'organisation et d'être conforme aux réglementations en vigueur dans les pays où opère l'organisation. Il anime la filière cybersécurité et peut piloter un réseau de Responsables de la Sécurité des Systèmes d'Information (RSSI) permettant de couvrir l'ensemble du périmètre de l'organisation. Il définit les indicateurs stratégiques et managériaux permettant de mesurer le niveau de maturité de l'organisation en matière de cybersécurité et rend compte à la Direction générale et au comité d'audit.

Formation : Bac + 5, dont une spécialisation en cybersécurité
Expérience professionnelle : supérieure à 10 ans dans le domaine de la cybersécurité

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

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.

Formation : Bac + 5 avec une spécialisation en cybersécurité
Expérience professionnelle : supérieure à 5 ans dans le domaine de la cybersécurité

Centre d'information de l'éducation nationale
Source : « Agence Nationale de la Sécurité des Systèmes d'Information »

- ### Coordinateur sécurité

Le coordinateur sécurité assure un appui au pilotage des actions de sécurité des SI 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.

Formation : Bac + 3, dont une spécialisation en lien avec la cybersécurité

- ### Directeur de programme de sécurité

Dans le cadre d'un programme de transformation de la sécurité des SI, le Directeur de programme de sécurité met en œuvre une trajectoire et un portefeuille de projets de sécurité selon une cible répondant à des objectifs de sécurité métiers et IT stratégiques ainsi qu'à l'augmentation de la cybermenace. Il pilote l'ensemble des projets de sécurité dans leurs différentes dimensions (technique, organisationnelle, métier).

Formation : Bac + 5
Expérience : de 5 à 10 ans d'expérience dans la conduite de programmes IT

- ### Responsable de projet de sécurité

Le responsable de projet de sécurité des SI 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.

Formation : Bac +3 à Bac +5, dont une spécialisation en informatique
Métier accessible à partir d'une expérience préalable en gestion de projet informatique

Conception et maintien d'un SI sécurisé

- ### Chef sécurité de projet

Le chef sécurité de projet s'assure de la bonne prise en compte des aspects de sécurité des SI dans le cadre de la conception et de la réalisation d'un projet informatique ou métier. En général, le chef sécurité de projet assiste le chef de projet métier et le chef de projet IT sur ces aspects. Il travaille avec les juristes et le DPO si le projet intègre le traitement de données à caractère personnel. Tous les projets ne nécessitant pas la présence d'un chef sécurité de projet, certaines de ces missions peuvent être prise en charge par le chef de projet qui s'appuie ponctuellement sur des experts du domaine.

Formation : Bac +3 à Bac +5, dont une spécialisation en cybersécurité
Métier accessible à partir d'une expérience préalable en gestion de projet informatique

• Architecte sécurité

L'architecte sécurité des SI s'assure que les choix techniques et technologiques des projets IT et métiers respectent les exigences de sécurité de l'organisation. Il constitue l'autorité technique sur les architectures de sécurité, définit les modèles de sécurité et accompagne le développement des architectures de sécurité au sein du SI, en cohérence avec la stratégie IT et les politiques de sécurité de l'organisation.

Formation : Bac +5, dont une spécialisation en cybersécurité
Métier accessible à partir d'une expérience préalable en architecture technique des systèmes d'information

• Spécialiste sécurité d'un domaine technique

Le spécialiste sécurité possède une expertise sur la sécurité d'un domaine technique particulier (système, réseau, composants industriels, IoT, Active Directory, Cloud, IAM, Intelligence Artificielle, etc.). Il assure un rôle de conseil, d'assistance, d'information, de formation et d'alerte et peut intervenir directement sur tout ou partie d'un projet qui relève de son domaine d'expertise, que ce soit dans les phases d'étude, de mise en œuvre ou de maintien en conditions de sécurité.

Formation : Bac +3 à Bac +5, dont une spécialisation en informatique et en cybersécurité dans son domaine d'expertise
Expérience professionnelle de 5 à 10 ans en sécurité des SI

• Spécialiste en développement sécurisé

Le spécialiste en développement sécurisé intervient en appui des équipes de développement 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.

Formation : Bac +5, avec une spécialisation en développement et en cybersécurité
Expérience professionnelle de 5 ans en sécurité des SI Métier accessible à partir d'une expérience en développement

• Cryptologue

Le cryptologue apporte une expertise sur la spécification, l'utilisation et la mise en œuvre opérationnelle de moyens cryptographiques permettant d'assurer la confidentialité, l'intégrité et l'authenticité des données. Le cryptologue intervient notamment au sein de laboratoires de recherche dans le secteur privé ou public, ses activités dépendant du contexte.

Formation : Bac+5 à doctorat

• Administrateur de solutions de sécurité

L'administrateur de solutions de sécurité 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 le maintien en conditions opérationnelles et de sécurité.

Formation : Bac +3, avec une spécialisation en informatique
Métier accessible à partir d'une expérience préalable en environnement de production, d'exploitation ou de support

• Auditeur de sécurité organisationnelle

L'auditeur en sécurité organisationnelle réalise des audits et des contrôles des processus de sécurité. Il s'assure de la conformité aux politiques internes et aux réglementations qui s'appliquent à l'organisation. Il contrôle que les politiques et règles de sécurité définies pour assurer le maintien en conditions de sécurité sont mises en œuvre, respectées et efficaces ; il identifie les vulnérabilités et propose des actions de remédiation.

Formation : Bac +5
Métier accessible à partir d'une expérience professionnelle en audit IT

• Auditeur de sécurité technique

L'auditeur de sécurité technique réalise des évaluations techniques de la sécurité d'environnements informatiques. Il identifie les vulnérabilités et propose 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.).

Formation : Bac +3 à Bac+5 dont spécialisation en cybersécurité
Type de certification : PASSI (Prestataire d'Audit de Sécurité des Systèmes d'Information)

Gestion des incidents et des crises de sécurité

• Responsable du SOC (Security Operation Center)

Le responsable du SOC (Security Operation Center) planifie et organise les opérations quotidiennes du SOC afin d'évaluer le niveau de vulnérabilité et de détecter des activités suspectes ou malveillantes. Il met en place le service de détection des incidents de sécurité. Il valide la bonne exécution des processus de supervision et de gestion des évènements de sécurité et assure un reporting complet et précis des indicateurs clés. Il définit et pilote le plan d'amélioration des services du SOC.

Formation : Bac +5, spécialisation en cybersécurité
Expérience professionnelle de 5 ans minimum au sein d'un SOC

• Opérateur analyste SOC

L'opérateur analyste SOC assure la supervision du système d'information de l'organisation afin de détecter des activités suspectes ou malveillantes. Il identifie, catégorise, analyse et qualifie les évènements 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.

Formation : Bac +3, dont spécialisation en cybersécurité
Métier accessible à partir d'une première expérience en ingénierie des réseaux et des systèmes

• Responsable du CSIRT

Le responsable du CSIRT (Computer Security Incident Response Team) ou du CERT (Computer Emergency Response Team) est responsable d'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. Il contribue à la préparation de l'organisation pour garantir une réponse efficace. Lors d'incidents à fort impact, le responsable du CSIRT est amené à interagir avec l'équipe de gestion de crise.

Formation : Bac +5, spécialisation en cybersécurité avec une forte composante en systèmes et réseaux
Expérience professionnelle de 5 ans minimum au sein d'un CSIRT

• Analyste réponse aux incidents de sécurité

L'analyste réponse aux incidents de sécurité intervient généralement au sein d'un CERT (Computer Emergency Response Team) ou CSIRT (Computer Security Incident Response Team). En cas de soupçons sur une activité malveillante ou d'attaque au sein du système d'information, l'analyste réponse aux incidents de sécurité analyse les symptômes et réalise les analyses techniques sur le système d'information. Il identifie le mode opératoire de l'attaquant et qualifie l'étendue de la compromission. Il fournit des recommandations de remédiation pour assurer l'assainissement et le durcissement des systèmes attaqués.

Formation Bac +5, dont spécialisation en cybersécurité

• Gestionnaire de crise de cybersécurité

Le gestionnaire de crise de cybersécurité intervient souvent au sein d'un CSIRT (Computer Security Incident Response Team) ou d'un CERT (Computer Emergency Response Team) externe ou interne pour grandes organisations, ou bien dans une équipe dédiée à la gestion de crise travaillant étroitement avec le CSIRT. Il 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.

Formation : Bac + 5, dont une spécialisation en cybersécurité
Expérience professionnelle de 5 ans minimum

Centre d'information de l'éducation nationale
Source : « Agence Nationale de la Sécurité des Systèmes d'Information »

- ### Analyste de la menace cybersécurité

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

Formation : Bac + 5, dont spécialisation en intelligence économique / veille ou spécialisation en cybersécurité
Connaissance d'une ou plusieurs langues étrangères

Conseil, services et recherche

- ### Consultant en cybersécurité

Le consultant en cybersécurité intervient au sein d'une société de services ou du pôle de conseil interne d'une organisation. Il propose, à partir d'un diagnostic, des solutions, méthodes, outils, etc. qui répondent aux enjeux posés. Il mobilise pour ce faire des éléments issus de son expertise et de son expérience ainsi que des outils développés en interne. Il anticipe les évolutions du contexte de cybersécurité, apporte un retour d'expérience et une vision des pratiques du marché. Il peut contribuer à la définition de la stratégie de cybersécurité de l'organisation et à la mise en œuvre des solutions de cybersécurité. Il apporte son expertise aussi bien sur des sujets méthodologiques que techniques.

Formation : Bac +5, dont une spécialisation en cybersécurité

- ### Formateur en cybersécurité

Le formateur en cybersécurité assure la formation et/ou la sensibilisation sur les volets réglementaires, techniques ou opérationnels de la cybersécurité. Il construit des supports de formation adaptés aux publics cible et illustre ses messages par des travaux pratiques, démonstrations ou exercices participatifs. Il peut évaluer le niveau de connaissances avant et à l'issue des formations.

Formation : Bac +5, dont une spécialisation en informatique

- ### Évaluateur de la sécurité des technologies de l'information

L'évaluateur 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 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 agit en tant que tierce partie indépendante des développeurs de produits et des commanditaires de l'évaluation de sécurité.

L'évaluateur peut être spécialisé sur l'évaluation de produits matériels (hardwares) ou logiciels (softwares).

Formation : Bac+3 à Doctorat dont spécialisation en cybersécurité
Métier 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)

• Développeur de solutions de sécurité

Le développeur de solutions de sécurité intervient au sein de sociétés d'éditions de produits informatiques. Il assure les spécifications et la conception de solutions et de produits de sécurité adaptés au contexte des menaces de cybersécurité.

Formation : Bac+3 à Bac +5, dont une spécialisation en développement sécurisé

• Intégrateur de solutions de sécurité

Au sein d'une société d'intégration de solutions, l'intégrateur de solutions de sécurité contribue au choix de l'architecture de la solution de sécurité et en assure l'assemblage au sein du SI. Il intègre dans l'environnement de production la solution de sécurité et en assure le déploiement. Il peut également assurer l'exploitation et le maintien en conditions opérationnelles dans la durée à travers la fourniture d'un service de sécurité managé.

Formation : Bac+3 à Bac+5, dont une spécialisation en informatique

• Chercheur en sécurité des systèmes d'information

Le chercheur en sécurité des systèmes d'information se consacre à l'expérimentation et au progrès de sa discipline. Il met en œuvre, aux frontières de plusieurs champs scientifiques constitués, ses acquis techniques et académiques au service d'une problématique de sécurité, au plus haut niveau scientifique. Il mobilise des connaissances expertes pour contribuer à l'émergence de technologies novatrices et de savoirs inédits. Il respecte les attendus et contraintes de la construction du savoir scientifique en matière de méthode et de restitution des résultats. 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.

Formation : Bac+5 à doctorat ou post-doctorat, Habilitation à Diriger les Recherches