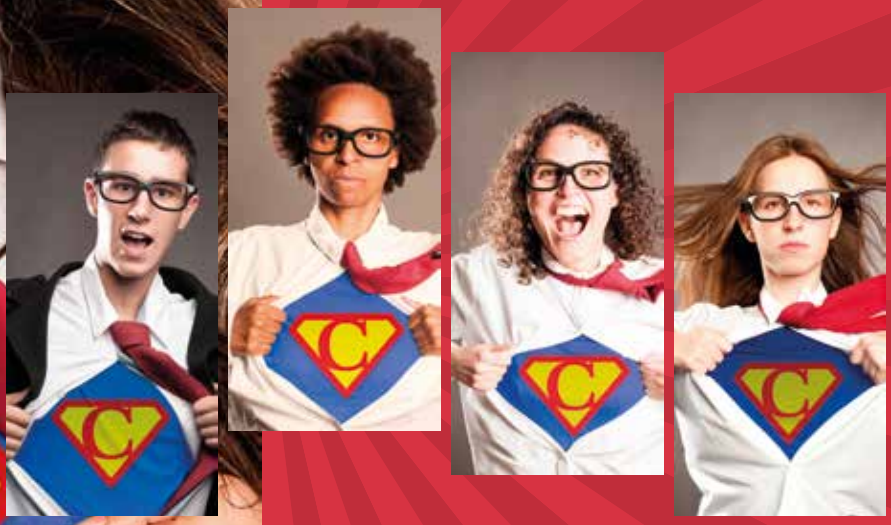
Guide des

CYBER MÉTIERS



Devenez les cyber héros de demain !

l'Europe s'engage en Hauts-de-France avec le FSE

MEL MÉTROPOLE EUROPÉENNE DE LILLE

mie

UNION EUROPÉENNE

Ce document est cofinancé par le Fonds Social Européen dans le cadre du PON "Emploi et Inclusion en Métropole" 2014-2020.

SOMMAIRE

Document édité par la MiE du Roubaisis : 78b Boulevard du Général Leclerc, 59100 ROUBAIX. Impression : Nord Imprim - 4 Impasse, Impasse Route de Godewaersvelde, 59114 Steenvoorde. **Directeur de la publication & rédactrice en chef :** Catherine DORPE, directrice. Rédacteurs : l'équipe numérique de la MiE du Roubaisis. **Conception graphique et mise en page** : Service communication de la MiE et Isabelle Triboulloy, graphiste. **Crédits photos** : MiE/Photo, Pixabay, Unsplash. La MiE remercie chaleureusement l'ensemble des contributeurs, collaborateurs et partenaires. Imprimé en mai 2022 - Série limitée à 500 exemplaires.

ÉDITO

Le marché de l'emploi « cyber » est en plein essor.

La sécurité des systèmes informatiques est devenue un enjeu économique et stratégique face aux attaques informatiques sur les systèmes d'informations dans le but de voler, détruire ou modifier des informations confidentielles des organisations.

D'ici 2025, l'ANSSI, agence nationale pour la sécurité des systèmes informatiques, prévoit un doublement des besoins en emplois à l'échelle nationale, passant de 37 000 salariés à 75 000, autant dans les PME que les collectivités.

Or :

→ Les profils actuellement disponibles et formés en cybersécurité sont insuffisants au regard des besoins des entreprises.

→ Les entreprises de cyber sécurité et les start-up recrutent des profils de haut-niveau, mais les besoins des employeurs de petite ou moyenne taille (TPE, PME, collectivités, …) ont des besoins de compétences en détection et traitement des incidents qui ouvrent des portes à des profils de **niveaux de qualifications BAC +2.**

→ La plupart des organisations n'ont pas besoin d'une ressource cyber à temps complet.

→ Les intitulés métiers demeurent peu parlants pour une grande partie de la population.

→ **Les femmes** sont encore moins représentées dans la profession que dans toute celle de la filière numérique en général : seulement 11% de femmes sont effectivement présentes sur des métiers techniques de la filière cybersécurité.

→ La cybersécurité a besoin de compétences techniques variées mais également de personnes possédant des **qualités relationnelles** car la sécurité informatique passe avant tout par la **formation des collaborateurs.** En effet, les menaces de piratage ne viennent pas uniquement de l'extérieur de l'entreprise, elles peuvent aussi être dû à un problème interne lié notamment à un manque de communication.

Un de nos objectifs est de vulgariser et simplifier l'information sur les métiers et les formations au numérique.

Vous trouverez dans ce guide des cyber-métiers une sélection de métiers que notre équipe numérique a réalisée à partir des travaux de l'ANSSI, que nous remercions chaleureusement pour leur autorisation d'exploitation.

Bonne lecture, et belle route vers la cyber !

Catherine DORPE
Directrice de la MiE

Ce document a été réalisé sur la base du Panorama des métiers de la cybersécurité (édition 2020) de l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI).

CONSEILS, SERVICES ET RECHERCHE

/// DÉVELOPPEUR·EUSE DE SOLUTIONS DE CYBERSÉCURITÉ

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

Types d'entreprises › Entreprises spécialisées en cybersécurité.

Formations › Niveau Bac+3 à Bac +5, dont une spécialisation en développement sécurisé.

/// INTÉGRATEUR·TRICE DE SOLUTIONS DE SÉCURITÉ

Missions essentielles › Au sein d'une société d'intégration de solutions, l'intégrateur·trice 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·elle intègre dans l'environnement de production la solution de sécurité et en assure le déploiement. Il·elle peut également assurer l'exploitation et le maintien en conditions opérationnelles dans la durée à travers la fourniture d'un service de sécurité managé.

Types d'entreprises › Grandes entreprises ou entreprises spécialisées en cybersécurité.

Formation › Niveau Bac+3 à Bac+5, dont une spécialisation en informatique.

/// CONSULTANT·E EN CYBERSÉCURITÉ

Missions essentielles › Le·la consultant·e en cybersécurité intervient au sein d'une société de services ou du pôle de conseil interne d'une organisation. Il·elle propose, à partir d'un diagnostic, des solutions, méthodes, outils, etc. qui répondent aux enjeux posés. Il·elle mobilise pour ce faire des éléments issus de son expertise et de son expérience ainsi que des outils développés en interne.

Il·elle anticipe les évolutions du contexte de cybersécurité, apporte un retour d'expérience et une vision des pratiques du marché. Il·elle peut contribuer à la définition de la stratégie de cybersécurité de l'organisation et à la mise en oeuvre des solutions de cybersécurité. Il·elle apporte son expertise aussi bien sur des sujets méthodologiques que techniques.

Types d'entreprises › Entreprises spécialisées en cybersécurité ou grandes entreprises. Le·la consultant·e sécurité est souvent spécialisé dans un ou plusieurs domaines de cybersécurité : sécurité organisationnelle, sécurité technique, IAM, etc.

Formation › Niveau Bac +5, dont une spécialisation en cybersécurité.

/// FORMATEUR·TRICE EN CYBERSÉCURITÉ

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

Types d'entreprises › Grandes entreprises ou entreprises spécialisées en cybersécurité.

Formation › Niveau Bac +5, dont une spécialisation en informatique.

GESTION DES INCIDENTS ET DES CRISES DE SÉCURITÉ

/// TECHNICIEN·NE SUPÉRIEUR·E SYSTÈME RÉSEAU SPÉCIALISÉ·E EN CYBERSÉCURITÉ OU OPÉRATEUR·TRICE ANALYSTE SOC

Missions essentielles › L'opérateur·trice analyste SOC assure la supervision du système d'information de l'organisation afin de détecter des activités suspectes ou malveillantes. Il·elle 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·elle contribue au traitement des incidents de sécurité avérés en support des équipes de réponse aux incidents de sécurité.

Types d'entreprises › Grandes entreprises ou entreprises spécialisées en cybersécurité. L'opérateur·trice du SOC pourra être amené à développer des compétences en machine learning afin de renforcer les capacités de détection.

Formation › Niveau Bac +2, dont spécialisation en cybersécurité.

Métier accessible à partir d'une première expérience en ingénierie des réseaux et des systèmes.

/// ANALYSTE RÉPONSE AUX INCIDENTS DE SÉCURITÉ

Missions essentielles › 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·elle identifie le mode opératoire de l'attaquant et qualifie l'étendue de la compromission. Il·elle fournit des recommandations de remédiation pour assurer l'assainissement et le durcissement des systèmes attaqués.

Types d'entreprises › Grandes entreprises ou entreprises spécialisées en cybersécurité. L'analyste réponse aux incidents de sécurité peut être spécialisé en tant qu'analyste système, analyste réseau, analyste de codes malveillants.

Formation ›Niveau Bac +5, dont spécialisation en cybersécurité.
Des formations de niveaux Bac+2/3 vont se developper dans les prochaines années.

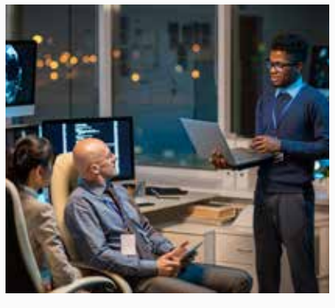
/// RESPONSABLE DU SOC

Missions essentielles › Le·la 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·elle met en place le service de détection des incidents de sécurité. Il·elle 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·elle définit et pilote le plan d'amélioration des services du SOC.

Types d'entreprises › Grandes entreprises ou entreprises spécialisées en cybersécurité.

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

/// ANALYSTE DE LA MENACE CYBERSÉCURITÉ



Missions essentielles › 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·elle 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.

Types d'entreprises › Grandes entreprises ou entreprises spécialisées en cybersécurité. Ce métier est en développement au sein des organisations qui possèdent une structure de type SOC.

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

/// GESTIONNAIRE DE CRISE DE CYBERSÉCURITÉ

Missions essentielles › Le·la 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·elle 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·elle conseille les directions métiers afin de résoudre les crises de cybersécurité. Il·elle organise la capacité de l'organisation à affronter de nouvelles menaces en matière de cybersécurité.

Types d'entreprises › Grandes entreprises ou entreprises spécialisées en cybersécurité. Au sein des organisations qui ne disposent pas d'une structure de réponse à incidents spécifiques, ce métier n'est pas toujours dédié ; ses missions peuvent être assurées par le RSSI ou par d'autres acteurs de l'organisation de gestion de crise.

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

/// RESPONSABLE DU CSIRT

Missions essentielles › Le·la 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·elle contribue à la préparation de l'organisation pour garantir une réponse efficace. Lors d'incidents à fort impact, e·la responsable du CSIRT est amené à interagir avec l'équipe de gestion de crise.

Types d'entreprises › Grandes entreprises ou entreprises spécialisées en cybersécurité. Le·la responsable du CSIRT peut être amené à contribuer à la gestion d'incidents liés à des raisons autres que la sécurité des SI, comme par exemple la fraude via des moyens informatiques.

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

CONCEPTION ET MAINTIEN D'UN SI SÉCURISÉ

/// ADMINISTRATEUR·TRICE DE SOLUTIONS DE SÉCURITÉ

Missions essentielles › L'administrateur·trice de solutions de sécurité installe, met en production, administre et exploite des solutions de sécurité (antivirus, sondes, firewalls, IAM, etc.). Il·elle participe au bon fonctionnement des solutions de sécurité en garantissant le maintien en conditions opérationnelles et de sécurité.

Types d'entreprises › Tous types d'entreprises : grands comptes, entreprises spécialisées en cybersécurité, ETI (Entreprise de taille intermédiaire) ou PME.

Souvent, la fonction d'administration de la sécurité est une des fonctions de l'administrateur systèmes et réseaux, mais certaines organisations peuvent dédier des personnes à ce seul métier. Ces dernières agissent alors en complément de l'administrateur systèmes et réseaux.

Formations › Niveau Bac +3, avec une spécialisation en informatique. Métier accessible à partir d'une expérience préalable en environnement de production, d'exploitation ou de support.

/// CHEF·FE SÉCURITÉ DE PROJET

Missions essentielles › Le·la chef·fe 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·elle 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.

Types d'entreprises › Tous types d'entreprises : grands comptes, entreprises spécialisées en cybersécurité, ETI ou PME.

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

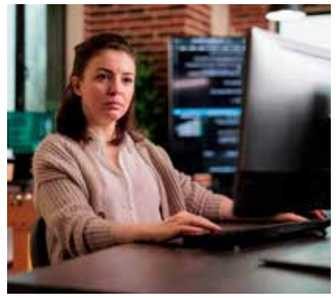
/// AUDITEUR·TRICE DE SÉCURITÉ TECHNIQUE / PENTESTER

Missions essentielles › L'auditeur·trice de sécurité technique réalise des évaluations techniques de la sécurité d'environnements informatiques. Il·elle identifie les vulnérabilités et propose des actions de remédiation. Il·elle peut réaliser différents types d'audits en fonction de son périmètre d'activité (tests d'intrusion, audit de code, revue de configuration, etc.).

Types d'entreprises › Tous types d'entreprises : grands comptes, entreprises spécialisées en cybersécurité, ETI ou PME.

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

/// SPÉCIALISTE EN DÉVELOPPEMENT SÉCURISÉ



Missions essentielles › Le·la 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·elle teste la sécurité des développements et suit la correction des vulnérabilités identifiées.

Types d'entreprises › Tout types d'entreprises : grands comptes, entreprises spécialisées en cybersécurité, ETI ou PME.

Formations › Niveau 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.

/// AUDITEUR·TRICE DE SÉCURITÉ ORGANISATIONNELLE

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

Types d'entreprises › Tous types d'entreprises : grands comptes, entreprises spécialisées en cybersécurité, ETI ou PME.

Formations › Niveau Bac +5. Métier accessible à partir d'une expérience professionnelle en audit IT.

GESTION DE LA SÉCURITÉ ET PILOTAGE DES PROJETS DE SÉCURITÉ

/// COORDINATEUR·TRICE SÉCURITÉ

Missions essentielles › Le·la 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·elle apporte un support aux équipes opérationnelles pour la réalisation des actions de sécurité et assure le suivi des plans d'actions.

Types d'entreprises › PME/ TPE et structures publiques (mairies, Hôpitaux...).

Formations › Niveau Bac + 3, dont une spécialisation en lien avec la cybersécurité.

/// DIRECTEUR·TRICE CYBERSÉCURITÉ

Missions essentielles > Au sein de grandes organisations, le·la Directeur. trice 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·elle 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·elle 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.

Types d'entreprises > Grandes entreprises ou entreprises spécialisées en cybersécurité

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

/// RESPONSABLE DE LA SÉCURITÉ DES SI

Missions essentielles > Le·la 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·elle 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·elle 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·elle 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·elle joue un rôle opérationnel dans la mise en œuvre de la politique de sécurité des SI ou encadre une équipe.

Types d'entreprises > Grandes entreprises ou entreprises spécialisées en cybersécurité PME/TPE

Formations >: Niveau Bac + 5 avec une spécialisation en cybersécurité. Expérience professionnelle : supérieure à 5 ans dans le domaine de la cybersécurité.

MÉTIERS CONTRIBUANT À LA DÉMARCHE DE CYBERSÉCURITÉ

/// DÉLÉGUÉ·E À LA PROTECTION DES DONNÉES

Missions essentielles > Il·elle est chargé·e de mettre en oeuvre la conformité au Règlement Européen sur la Protection des Données (RGPD) au sein de l'organisation qui l'a désigné, et ce pour l'ensemble des traitements de données à caractère personnel mis en oeuvre par cette organisation. La filière cybersécurité analyse les risques du point de vue de la protection de la donnée tandis que le DPO s'intéresse au risque lié à l'utilisation de la donnée sur la vie privée des personnes concernées.

Elle·il mène des analyses de risques complémentaires dans les projets (security & privacy by design).

Types d'entreprises > Grandes entreprises ou entreprises spécialisées en cybersécurité ou ETI.

/// MANAGER·EUSE DE RISQUES

Missions essentielles > Il·elle s'assure que tout ou partie des risques de l'organisation sont bien identifiés et couverts : il·elle présente à la Direction générale les risques de l'organisation, il·elle propose des solutions de maîtrise des risques optimisées en termes de financement, afin de poser des limites acceptables à la prise de risques ; il·elle coordonne les actions de maîtrise des risques. La filière cybersécurité aide à la prise en compte du risque de cybersécurité en éclairant les managers de risques sur ce risque particulier et en travaillant à la quantification des risques de façon cohérente avec les autres risques opérationnels.

Types d'entreprises > Grandes entreprises ou entreprises spécialisées en cybersécurité ou ETI.

/// RESPONSABLE DU PLAN DE CONTINUITÉ D'ACTIVITÉ

Missions essentielles > Il·elle élabore et met en oeuvre dans son organisation un Plan de Continuité d'Activité (PCA) permettant d'assurer la continuité des activités de l'entreprise en cas de sinistre majeur. Il·elle doit prendre en compte les scénarios de résilience liés à des cyber-attaques (cyber-résilience). La filière cybersécurité éclaire le RPCA sur les risques de continuité liés à des cybermenaces et valide les mesures proposées pour traiter les risques portant sur les critères de disponibilité et d'intégrité. Elle vérifie que les tests de plans sont bien en place et que les résultats des tests sont satisfaisants et en amélioration continue.

Types d'entreprises > Grandes entreprises ou entreprises spécialisées en cybersécurité ou ETI.

/// DIRECTEUR·TRICE SÛRETÉ

Missions essentielles > Il·elle définit et organise les moyens, dispositifs et systèmes visant à la protection des installations et des personnes. Il·elle est garant de la sûreté des moyens de production. Il·elle met en oeuvre les modes de contrôle et de surveillance adaptés et définit des plans de prévention. La filière cybersécurité veille à ce que la sécurité physique permette de protéger l'accès à des zones sensibles (datacenters, locaux techniques, matériels exposés dans des zones publiques). Les deux filières coopèrent sur l'identification des menaces.

Types d'entreprises > Grands comptes, entreprises spécialisées en cybersécurité ou ETI.

/// RESPONSABLE DES ASSURANCES

Missions essentielles > Il·elle assure la cohésion des politiques d'assurance des risques et négocie auprès des compagnies d'assurance les garanties nécessaires à la couverture des risques. La filière cybersécurité aide à la prise en compte du risque de cybersécurité dans la politique d'assurance (cyber-assurance).

Types d'entreprises > Grands comptes, entreprises spécialisées en cybersécurité ou ETI.

/// RESPONSABLE DU CONTRÔLE INTERNE

Missions essentielles > Il·elle assure le déploiement opérationnel des dispositifs de contrôle interne et de gestion des risques opérationnels et s'assure de son efficacité. La filière cybersécurité contribue à la définition des contrôles internes liés à la cybersécurité, voire à la lutte contre la fraude..

Types d'entreprises > Grands comptes, entreprises spécialisées en cybersécurité ou ETI.

MÉTIERS POUVANT SE SPÉCIALISER EN CYBERSÉCURITÉ

/// JURISTE SPÉCIALISÉ·E EN CYBERSÉCURITÉ

Missions essentielles > 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·elle peut présenter une expérience d'avocat à même d'éclairer l'organisation 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. Il·elle est un acteur essentiel de la contractualisation avec les fournisseurs en intégrant des clauses de sécurité résultant de sa collaboration étroite avec les équipes cybersécurité.

/// CHARGÉ·E DE COMMUNICATION SPÉCIALISÉ·E EN CYBERSÉCURITÉ

Missions essentielles > Le·la chargé·e de communication spécialisé en cybersécurité assiste les équipes cybersécurité dans la mise en œuvre opérationnelle de la communication sur l'actualité cybersécurité.

Il·elle peut aussi contribuer à préparer la communication interne et externe dans un contexte de crise de cybersécurité.

LES ACTEURS DE LA CYBERSÉCURITÉ EN FRANCE & DANS LA RÉGION HAUTS-DE-FRANCE

ANSSI : Agence Nationale de la sécurité des systèmes d'information

L'ANSSI est l'autorité nationale chargée d'assurer la sécurité des systèmes d'information de l'État et de contribuer à celle des opérateurs nationaux d'importance vitale (OIV). Elle apporte conseils, expertise et assistance technique pour prévenir la menace et traiter les incidents portant atteinte à la sécurité du numérique. En France comme à l'international, elle agit aux côtés de leurs partenaires pour promouvoir la confiance numérique ainsi que le développement de la filière de cybersécurité à travers trois grandes missions :

- → Prévention de la menace par la réglementation, l'étude et l'anticipation des modes d'attaques, la définition de mesures de protection, l'assistance des administrations et des entreprises sensibles, et la certification/ qualification de produits et services de confiance ;
- → Défense des systèmes d'information par la détection de failles et d'incidents et la réaction au plus tôt en cas de cyber-attaque ;
- → Information et sensibilisation des différents publics sur la nécessaire protection des environnements numériques par la promotion de bonnes pratiques de cybersécurité et la diffusion de recommandations techniques et méthodologiques tout en participant au développement de la formation à la sécurité des systèmes d'information.

L'ANSSI est rattachée au Secrétariat général de la défense et de la sécurité nationale (SGDSN), autorité chargée d'assister le Premier ministre dans l'exercice de ses responsabilités en matière de défense et de sécurité nationale.

Découvrir l'ANSSI et ses missions en vidéo :
https://www.dailymotion.com/video/x4bo6zy_l-anssi-en-9_tech

La plaquette de présentation :
https://www.ssi.gouv.fr/uploads/2018/04/plaquette_institutionnelle_anssi.pdf

INCRT : Institut nationale de la cybersécurité et de la résilience des territoires

L'Institut National pour la Cybersécurité et la Résilience des Territoires est dédié à la réflexion, la veille et au déploiement de concepts nouveaux dans le domaine de la cybersécurité des territoires (réseaux d'énergie départementaux, Services de transport locaux, Infrastructures de production d'eau, Infrastructures portuaires et aéroportuaires, Transformation digitale et services publics dématérialisés, Smart City…). Forum de réflexion et d'échanges pour les collectivités territoriales, les établissements publics de coopération intercommunale (EPCI) et les acteurs sous délégation de service public (DSP), il permettra l'échange d'idées et de projets entre élus locaux, administrateurs et acteurs des territoires.

Ses grandes missions :

- → Coordonner une réflexion innovante sur la résilience et la cybersécurité des territoires.
- → Fournir des formations, à une nouvelle génération d'élus et de gestionnaires des territoires.
- → Développer des collaborations avec l'Industrie et renforcer ses liens avec les territoires.
- → Organiser le symposium annuel sur la résilience et la cybersécurité et la résilience des territoires regroupant les communautés scientifiques et professionnelles, industrielles et politiques.

Le centre de lutte contre les criminalités numériques (C3N)

Le centre de lutte contre les criminalités numériques (C3N) est un service à compétence judiciaire nationale, qui regroupe l'ensemble des unités du pôle judiciaire de la Gendarmerie nationale qui traitent directement de questions en rapport avec la criminalité et les analyses numériques. Le C3N assure également l'animation et la coordination, au niveau national, de l'ensemble des enquêtes menées par le réseau des enquêteurs numériques de la gendarmerie.

EuraTechnologies

Précurseur de la French Tech et fer de lance de l'économie numérique en France, le pôle d'excellence et d'innovation EuraTechnologies est implanté à Lille depuis 2009.

Incubateur et accélérateur de startups, EuraTechnologies est présent sur 4 campus : Lille, Roubaix, Saint-Quentin et Willems. A Lille, **c'est plus de 80 000 m²** entièrement dédiés au développement économique du territoire, en plein cœur de la métropole lilloise. Avec des restaurants, une cafétéria, une crèche, une conciergerie, une accessibilité multimodale. **Des bureaux, des espaces de co-working, des lieux de vie intérieurs et extérieurs, des salles pour organiser des événements (réunions, conférences, séminaire, congrès, ateliers, événements Tech).**

Un nouvel ensemble immobilier a été développé à côté d'Euratechnologies : **WENOV qui forme les futurs entrepreneurs et talents du numérique de demain.** C'est au sein de ce nouveau lieu que le Campus Cyber est implanté.

Campus Cyber

Ce lieu inédit dédié aux enjeux de la sécurité numérique vise à renforcer les synergies entre une diversité d'acteurs et d'activités au sein d'un même lieu de dimension nationale, attractif, connecté aux développements en régions et visibles en Europe et à l'international. Le projet est porté par Euratechnologies en Hauts-de-France. Outre des aires de travail « classiques » type bureaux, le Campus Cyber pourrait s'organiser autour d'un auditorium et d'un ensemble d'espaces :

- → partagés et mutualisés comprenant des plateaux projets (lieux de travail thématiques modulables rassemblant différentes entités) ;
- → dédiés à l'organisation de conférences et d'évènements
- → dédiés aux cycles de formation et de réunion ;
- → de coworking ;
- → permettant la mise en place de services ;
- → et de convivialités.

Ce campus hébergerait des équipes orientées cyber mais aussi des entreprises qui souhaiteraient s'inscrire dans ce nouvel écosystème.

CITC

Le Centre d'Innovation des Technologies sans Contact – EuraRFID favorise la compréhension des technologies innovantes en matière du sans contact et de l'Internet des Objets.

Le CITC dispose d'un laboratoire R&D et pilote des projets de recherche intégrative et collaborative. Il collabore avec des organismes de recherche (INRIA, IRCICA, CNRS) et initie des projets de Recherche et Développement : thèses, chaire industrielle…

Le CITC met à disposition de ses adhérents des moyens concrets : des plateformes techniques pour la réalisation de diagnostics techniques et une équipe R&D composée d'ingénieur·es qualifié·es.

Le CITC dispense des formations dans les technologies émergentes (IA, cybersécurité, systèmes embarqués, RFID, NFC, conception d'objets connectés, design d'antennes, sécurité…).

www.cyberterritoires.fr

VOUS RECHERCHEZ UNE FORMATION ?

Trois outils pour naviguer dans la richesse des formations :

Vous pourrez explorer les formations de la filière Numérique présentes sur la Métropole Lilloise grâce au **SPOT**, une cartographie dynamique et interactive des formations numériques.

https://agoraa.me/spot/mie-du-roubaisis

Vous pourrez également élargir vos recherches à l'échelle régionale grâce au **C2RP**.

www.c2rp.fr

Ma Formation de Pôle Emploi vous permettra de naviguer sur l'ensemble des formations présentent au niveau national.

www.maformation.fr

Guide des

CYBER MÉTIERS

Devenez
les cyber
héros
de demain !

MIE - 78 bis Boulevard du General Leclerc - 59100 Roubaix - SIRET 185 921 68100028

l'Europe s'engage en Hauts-de-France avec le FSE

MEL MÉTROPOLE EUROPÉENNE DE LILLE

mie

UNION EUROPÉENNE

Ce document est cofinancé par le Fonds Social Européen dans le cadre du PON "Emploi et Inclusion en Métropole" 2014-2020.