RÉPUBLIQUE
FRANÇAISE
Liberté
Égalité
Fraternité

PANORAMA DES MÉTIERS DE LA CYBERSÉCURITÉ

ÉDITION 2020

syntec numérique

SOMMAIRE

Edito 3

Préambule 4

Partie 1 : Métiers de la cybersécurité

Gestion de la sécurité et pilotage des projets de sécurité

Directeur Cybersécurité *8*
Responsable de la Sécurité des Systèmes d'Information (RSSI) *10*
Déclinaison pour le Responsable de sécurité des SI au sein d'une PME / TPE *12*
Coordinateur sécurité *14*
Directeur de programme de sécurité *15*
Responsable de projet de sécurité *17*

Conception et maintien d'un SI sécurisé

Chef sécurité de projet 20
Architecte sécurité 22
Spécialiste sécurité d'un domaine technique 24
Spécialiste en développement sécurisé 26
Cryptologue 28
Administrateur de solutions de sécurité 29
Auditeur de sécurité organisationnelle 31
Auditeur de sécurité technique 33

Gestion des incidents et des crises de sécurité

Responsable du SOC 36
Opérateur analyste SOC 38
Responsable du CSIRT 40
Analyste réponse aux incidents de sécurité 42
Gestionnaire de crise de cybersécurité 44
Analyste de la menace cybersécurité 46

Conseil, services et recherche

Consultant en cybersécurité 49
Formateur en cybersécurité 51
Évaluateur de la sécurité des technologies de l'information 52
Développeur de solutions de sécurité 54
Intégrateur de solutions de sécurité 56
Chercheur en sécurité des systèmes d'information 58

Partie 2 : Métiers connexes

Métiers contribuant à la démarche de cybersécurité 61
Métiers pouvant se spécialiser en cybersécurité 65

Annexes

Eléments de méthologie 69
Glossaire 72

ÉDITO

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.

Dans ce contexte, la formation et le recrutement sont des enjeux fondamentaux. Aujourd'hui, faute de connaissance des spécificités du domaine, les services en charge des ressources humaines peinent parfois à identifier les profils capables de répondre aux besoins de leur organisation. Ce panorama leur propose, ainsi qu'aux écoles et aux futurs talents, une nomenclature complète des métiers de la cybersécurité.

Nous faisons le pari que ce travail contribuera, en intégrant les enjeux cyber au sein des services des ressources humaines et des organismes de formation, à structurer et fortifier tout un écosystème cyber. Et à faire émerger une vision partagée des compétences de cette filière d'avenir.

Guillaume Poupard
Directeur général de l'ANSSI

Nolwenn Le Ster
Présidente du comité cybersécurité de Syntec Numérique

AVEC L'ENGAGEMENT DE :

ACN	Alliance pour la confiance numérique
CESIN	Club des experts de la sécurité de l'information et du numérique
CIGREF	Club informatique des grandes entreprises françaises
CLUSIF	Club de la sécurité de l'information français
CPME - Cinov IT	Confédération des petites et moyennes entreprises
Forum des compétences	Cercle d'échanges autour de la sécurité des systèmes d'information des acteurs de la banque, de la finance et des assurances

PRÉAMBULE

La numérisation croissante des échanges et des activités économiques ainsi que le développement et la complexification de la menace cyber rendent chaque jour plus urgent le besoin de doter les entreprises et les administrations de personnels formés, qualifiés et compétents en matière de cybersécurité. Ce constat fait aujourd'hui l'objet d'un consensus partagé.

Dans ce contexte, l'ANSSI a mis en place des dispositifs pour impulser, encourager et reconnaître les initiatives en matière de développement des formations et de diffusion des bonnes pratiques. Afin de guider les entreprises dans leur politique de recrutement, d'accompagner les porteurs de formation et d'encourager les étudiants ou les salariés en reconversion, elle poursuit son effort d'accompagnement en contribuant à la structuration du marché de l'emploi de la sécurité des systèmes d'information (SSI).

C'est tout l'objet de ce *Panorama des métiers de la cybersécurité* : un travail d'exploration, de caractérisation et de mise en commun autour des métiers -établis ou en émergence- qui constituent le domaine vaste et varié de la sécurité du numérique. Appellations, missions, compétences, domaines d'intervention, tendances d'évolution sont autant de dimensions sur lesquelles il est nécessaire de faire émerger des visions partagées. Ceci afin de fluidifier et dynamiser un marché de l'emploi cyber en plein essor.

DÉMARCHE DE TRAVAIL

En 2015, un groupe de travail composé de représentants de l'enseignement supérieur, du monde industriel et de l'ANSSI a élaboré une liste de 16 « profils métiers » dans le domaine de la sécurité du numérique. Cette liste a été publiée sur le site de l'ANSSI et intégrée dans le dispositif de labellisation des formations supérieures en SSI SecNum*edu*.

En 2019, en étroite collaboration avec Syntec Numérique, un travail visant à la mettre à jour et à l'enrichir a été lancé et piloté par l'ANSSI.

Le périmètre des acteurs consultés tout au long du projet a en outre été très sensiblement élargi par rapport à la première étude : représentants des entreprises et des administrations, acteurs de l'enseignement supérieur délivrant des formations en sécurité du numérique (communauté SecNum*edu*), communautés professionnelles sectorielles (y compris TPE / PME), administrations utilisatrices et grands comptes privés. Cette consultation a permis de collecter les besoins, les tendances observées et les différentes réalités et pratiques du marché de l'emploi.

PRINCIPES D'ÉLABORATION ET MODE D'EMPLOI

Élaborer une liste de métiers dans un secteur aussi changeant est un exercice délicat. Qui plus est, certains métiers ont parfois des contours mal définis et leur dénomination peut varier d'une organisation à l'autre. L'objet de ce Panorama n'est pas de figer les acceptions et les pratiques, mais d'élaborer un état des lieux partagé au moment de sa publication, dans l'idée de proposer un outil à ceux qui voudront s'en saisir et non une norme. Les principes et partis-pris méthodologiques qui ont présidé à l'élaboration de ce Panorama des métiers sont décrits en annexe.

L'ANSSI propose une nomenclature de métiers de la sécurité dans le numérique qui a vocation à être déclinée par chaque organisation selon ses spécificités.
Chaque fiche métier est autoporteuse et peut être utilisée indépendamment des autres fiches métiers proposées dans le document, ce qui explique certains recoupements d'activités entre plusieurs métiers.

STRUCTURE DU DOCUMENT

Le présent document comprend deux parties. **La partie principale, consacrée aux métiers dédiés à la cybersécurité, est organisée en quatre grandes familles :**

▶ **Gestion de la sécurité et pilotage des projets de sécurité**
Cette famille regroupe les métiers contribuant au pilotage de la démarche de sécurité, ainsi que les métiers visant à mettre en œuvre les projets de sécurité des SI.
▶ **Conception et maintien d'un SI sécurisé**
Cette famille regroupe les métiers qui assurent la prise en compte de la sécurité dans la conception des SI, l'expertise sur la sécurité d'un domaine particulier, l'administration des solutions de sécurité, ainsi que l'audit de la sécurité des SI.
▶ **Gestion des incidents et des crises de sécurité**
Cette famille regroupe les métiers qui assurent la détection et le traitement des incidents de sécurité, ainsi que les métiers qui gèrent les crises de sécurité.
▶ **Conseil, services et recherche**
Cette famille regroupe les métiers que l'on peut rencontrer au sein des entreprises spécialisées en cybersécurité : entreprises de conseil, entreprises de formation, laboratoires d'évaluation, éditeurs de produits de sécurité, intégrateurs de produits de sécurité, laboratoires et instituts de recherche.

La seconde partie est consacrée aux métiers connexes :

▶ Une première sous-partie présente les métiers avec lesquels la filière cybersécurité est amenée à interagir et qui contribuent à la démarche globale de sécurité des SI. Les métiers sont présentés au sein de ce Panorama pour permettre d'en appréhender la cohérence et les interactions existantes avec les métiers de la liste principale.
▶ Une seconde sous-partie présente quelques métiers qui peuvent se spécialiser en cybersécurité, notamment dans les grandes organisations.

Les document comprend également deux annexes :

▶ Des précisions sur la méthodologie adoptée ;
▶ Un glossaire.

REMERCIEMENTS

L'ANSSI remercie Syntec Numérique pour son appui dans le co-pilotage de cette étude. Elle remercie également, pour leur participation aux travaux, l'ACN, le Cesin, le Cigref, le Cinov-IT (pour la CPME), le Clusif, le Crédit Agricole (et plus largement le Forum des Compétences), le Ministère des Armées (et plus particulièrement la DGA), le Ministère de l'Economie et des Finances, Orange Cyberdéfense, Sanofi et l'UIMM.

NOTE

Le vocable « cybersécurité » présente certaines variantes : sécurité des systèmes d'information, sécurité numérique, sécurité du numérique. Dans le document, ces notions ont un sens équivalent.

MÉTIERS DE LA CYBERSÉCURITÉ

GESTION DE LA SÉCURITÉ ET PILOTAGE DES PROJETS DE SÉCURITÉ

Directeur Cybersécurité

Equivalence en anglais :
Executive security director

Autres titres équivalents :
▶ **FR :** Directeur de la sécurité des systèmes d'information (DSSI)
▶ **EN :** *Group Chief Security Officer, Group Chief Information Security Officer, Vice-President (VP) Cyber security*

MISSION ESSENTIELLE

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.

ACTIVITÉS ET TÂCHES

PLANIFIER
Définir les axes et les objectifs stratégiques en matière de cybersécurité et les faire valider par la Direction générale
Identifier les enjeux de sécurité, les risques majeurs de sécurité pesant sur l'organisation et les exigences de conformité légale et réglementaire
Définir et maintenir la politique de sécurité des SI en collaboration avec les parties prenantes
Définir la stratégie de mise en conformité au cadre législatif et réglementaire ; assurer les relations avec les acteurs de son secteur d'activité autour de la cybersécurité
Définir un plan d'actions annuel ou pluriannuel
Définir une politique d'investissement au regard des objectifs de sécurité
Définir l'organisation de la cybersécurité au sein de l'organisation et l'animer
Définir les mesures organisationnelles et techniques à mettre en œuvre pour atteindre les objectifs de sécurité
Piloter la réalisation de la charte de sécurité informatique de l'organisation et la promouvoir auprès de tous les utilisateurs
Contribuer à répondre aux sollicitations des clients et partenaires de l'organisation sur les aspects sécurité

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

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

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

FORMATION / EXPÉRIENCE PROFESSIONNELLE

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

COMPÉTENCES

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

COMPÉTENCES COMPORTEMENTALES
Leadership
Capacité d'influence
Sens de l'intérêt général
Management d'équipe
Capacité à travailler en transverse au sein de l'organisation
Capacité d'appropriation des enjeux métiers

TENDANCES ET FACTEURS D'ÉVOLUTION DU MÉTIER

Compte-tenu des enjeux actuels liés à la cybersécurité, le Directeur Cybersécurité occupe un poste de cadre dirigeant et est appelé à siéger dans les instances de direction de son organisation. Un rattachement à un membre du Comité exécutif est recommandé. Il doit avoir une compréhension globale de l'évolution de la cybersécurité pour maintenir à jour la stratégie de sécurité de l'organisation.

RESPONSABLE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION (RSSI)

Equivalence en anglais : *Chief Information Security Officer (CISO), Director of Information Security.*

Autres titres équivalents :

- **FR :** Officier de Sécurité des Systèmes d'Information (OSSI), Fonctionnaire de Sécurité des Systèmes d'Information (FSSI), Responsable de la Confiance Numérique (RCN)
- **EN :** *Information System Security Manager (ISSM), Information Security Manager*

MISSION ESSENTIELLE

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.

ACTIVITÉS ET TÂCHES

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

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

DÉTECTER
Prendre les mesures techniques et/ou organisationnelles permettant la surveillance des événements de sécurité, l'appréciation des incidents de sécurité et la réaction face aux attaques, assurer la mise en place d'un SOC (*Security Operation Center*)

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

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

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

FORMATION / EXPÉRIENCE PROFESSIONNELLE

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

COMPÉTENCES

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

COMPÉTENCES COMPORTEMENTALES
Capacité d'influence
Sens de l'intérêt général

Management d'équipe
Capacité de restitution au management
Capacité à travailler en transverse au sein de l'organisation
Capacité à résister à la pression
Capacité d'appropriation des enjeux métiers

TENDANCES ET FACTEURS D'ÉVOLUTION DU MÉTIER

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

Dans les grandes entreprises ou administrations, les activités et tâches peuvent être réparties entre un Directeur Cybersécurité ou un RSSI Groupe qui porte la responsabilité globale et des Responsables de la Sécurité des SI (RSSI) qui déclinent les actions sur leurs périmètres respectifs.

Déclinaison pour le Responsable de sécurité des SI au sein d'une PME / TPE

Au sein d'une PME / TPE, la fonction de Responsable de la sécurité des systèmes d'information n'est pas un poste dédié et les missions et activités peuvent être portées par le DSI, le responsable informatique, un administrateur, un exploitant ou bien un responsable de projet informatique.

Les activités et tâches essentielles qui doivent être prises en charge par une ou plusieurs personnes de l'organisation sont décrites ci-dessous.

ACTIVITÉS ET TÂCHES

IDENTIFICATION
Identifier les risques de sécurité sur son périmètre
Définir et maintenir la politique de sécurité des SI

PROTECTION
Définir les mesures organisationnelles et techniques de sécurité, les déployer, en assurer le fonctionnement opérationnel et les maintenir à l'état de l'art
S'assurer que les projets sont conçus et menés de manière sécurisée
S'assurer que les politiques et règles de sécurité sont appliquées dans l'organisation, piloter les audits de sécurité sur le SI de l'organisation, suivre les actions de remédiation
Réaliser le paramétrage et l'administration des outils de sécurité
Diffuser une culture SSI à destination des utilisateurs et sensibiliser les décideurs aux problématiques de sécurité

DÉTECTION ET RÉPONSE
Contribuer à la détection et au pilotage de la gestion des incidents et des crises de sécurité
Préparer et mettre en œuvre un plan de continuité informatique

REPORTING
Produire des états des actions de sécurité au sein de l'organisation
Mobiliser des expertises extérieures si besoin

Coordinateur sécurité

Équivalence en anglais :
Security coordinator

Autres titres équivalents :
- **FR :** relais cybersécurité
- **EN :** *Security Officer*

MISSION ESSENTIELLE

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.

ACTIVITÉS ET TÂCHES

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

FORMATION / EXPÉRIENCE PROFESSIONNELLE

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

COMPÉTENCES

COMPÉTENCES CŒUR DE MÉTIER
Connaissance du système d'information et des principes d'architecture
Connaissance des technologies de sécurité et des outils associés
Gestion des risques, politique de cybersécurité et SMSI
Connaissance des méthodologies d'analyse des risques de sécurité
Maîtrise des fondamentaux dans les principaux domaines de la SSI

COMPÉTENCES COMPORTEMENTALES
Capacité de travail en équipe
Pédagogie sur les sujets de cybersécurité

Directeur de programme de sécurité

Équivalence en anglais :
Cyber security Program Manager

Autres titres équivalents :
- **FR :** Directeur de projet sécurité
- **EN :** *IT program manager*

MISSION ESSENTIELLE

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).

ACTIVITÉS ET TÂCHES

DIRECTION DE PROJET
Définir une trajectoire de sécurité répondant à des objectifs métiers et IT stratégiques ainsi qu'à l'augmentation de la cybermenace
Définir et organiser le portefeuille de projets cybersécurité
Assurer le déploiement du programme et des initiatives cybersécurité dans l'ensemble des entités tout en assurant la cohérence globale et la coordination entre ces différentes entités
Réorienter les actions pour tenir compte de l'évolution des cybermenaces

GESTION DES RESSOURCES
Mettre en œuvre la gouvernance et le mode de pilotage du programme nécessaires à sa réussite
Suivre les plannings, assurer le pilotage du budget des projets de sécurité, des risques et des plans de remédiation associés

COMMUNICATION
Assurer le reporting pour informer le commanditaire et le management de l'avancement et de la couverture des risques de sécurité apportée par le programme
Formaliser des tableaux de bord explicites et clairs à destination du top management

FORMATION / EXPÉRIENCE PROFESSIONNELLE

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

COMPÉTENCES

COMPÉTENCES CŒUR DE MÉTIER
Bonne connaissance des enjeux et des métiers de l'organisation
Maîtrise des fondamentaux dans les principaux domaines de la SSI
Capacité de compréhension des menaces cybersécurité
Connaissance des technologies de sécurité et des outils associés
Gestion de projets et de portefeuille de projets

COMPÉTENCES COMPORTEMENTALES
Pilotage d'équipe
Capacité de restitution au management
Capacité à coordonner de nombreuses équipes
Capacité d'appropriation des enjeux métiers

TENDANCES ET FACTEURS D'ÉVOLUTION DU MÉTIER

Le Directeur de programme de sécurité peut être une évolution d'un métier de Direction de programme informatique. Il doit acquérir une solide connaissance des enjeux de cybersécurité et de la stratégie de cybersécurité de son organisation.

Responsable de projet de sécurité

Équivalence en anglais :
IT security project leader

Autres titres équivalents :
- **FR :** Chef de projet sécurité IT
- **EN :** *Security project Manager*

MISSION ESSENTIELLE

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.

ACTIVITÉS ET TÂCHES

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

CONDUITE DU PROJET
Assurer le suivi des phases d'appel d'offres, réaliser l'évaluation et le choix des solutions, suivre la contractualisation
Analyser les risques de sécurité liés au projet, proposer des mesures de sécurité si nécessaire
Définir et superviser la réalisation des prototypes et de preuves de concept (POC) et des tests fonctionnels de la solution ou de l'infrastructure de sécurité choisie
Prendre en main les solutions de sécurité étudiées (fonctionnellement et techniquement) lors des phases d'études (maquettes, etc.)
Effectuer la recette des solutions de sécurité et apprécier leur conformité au cahier des charges
Contribuer à la conception et à l'intégration des solutions de sécurité adoptées (incluant notamment les aspects d'architecture, de gestion des identités et des accès et de contribution à la stratégie de surveillance et de détection) et assurer leur suivi

FORMATION / EXPÉRIENCE PROFESSIONNELLE

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

COMPÉTENCES

COMPÉTENCES CŒUR DE MÉTIER
Connaissance du système d'information et des principes d'architecture
Maîtrise des fondamentaux dans les principaux domaines de la SSI
Connaissances des solutions de sécurité du marché
Sécurité des systèmes d'exploitation
Sécurité des réseaux et protocoles
Gestion de projets et de portefeuille de projets

COMPÉTENCES COMPORTEMENTALES
Capacité à travailler en transverse au sein de l'organisation

TENDANCES ET FACTEURS D'ÉVOLUTION DU MÉTIER

Capacité à prendre en compte les nouvelles méthodes de gestion de projet (méthode agile notamment).

CONCEPTION ET MAINTIEN D'UN SI SÉCURISÉ

Chef sécurité de projet

Équivalence en anglais :
Project security leader

Autres titres équivalents :
- **FR :** Responsable de l'intégration de la sécurité dans les projets
- **EN :** *Project security Manager*

MISSION ESSENTIELLE

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.

ACTIVITÉS ET TÂCHES

EXPRESSION DES BESOINS DE SÉCURITÉ
Analyser les besoins de sécurité et réaliser l'analyse des risques de sécurité du projet
Vérifier que les solutions techniques et fonctionnelles proposées répondent aux exigences de sécurité identifiées
Définir des mesures de sécurité complémentaires pour traiter les risques

SUIVI DE LA CONCEPTION
Suivre la sécurité des développements le cas échéant
Suivre la sécurité des architectures et des paramétrages initiaux avec l'aide éventuelle d'experts
Évaluer les fournisseurs et les tiers lors de la souscription des contrats et s'assurer de la mise en œuvre d'un plan d'assurance sécurité, selon la nature des solutions et des prestations fournies
Lancer les évaluations, tests ou audits liés à la sécurité des SI
Contribuer à mener des démarches d'homologation des systèmes qui le nécessitent
Contribuer à qualifier les risques de sécurité résiduels avant le passage en production
S'assurer de la formation des utilisateurs aux aspects de sécurité des SI le cas échéant

FORMATION / EXPÉRIENCE PROFESSIONNELLE

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

COMPÉTENCES CŒUR DE MÉTIER
Prise en compte de la sécurité dans les projets
Gestion de projets et de portefeuille de projets
Maîtrise du système d'information, de l'urbanisation et de l'architecture du SI
Maîtrise des fondamentaux dans les principaux domaines de la SSI
Connaissance juridique en matière de droit informatique lié à la sécurité et à la protection des données

Connaissance des technologies de sécurité et des outils associés
Connaissance des méthodologies d'analyse de risques de sécurité

COMPÉTENCES COMPORTEMENTALES
Travail en équipe
Pédagogie sur les sujets de cybersécurité
Capacité à travailler en transverse au sein de l'organisation
Capacité d'appropriation des enjeux métiers

Architecte sécurité

Équivalence en anglais :
Security Architect

Autres titres équivalents :
▶ **FR :** Architecte Sécurité Informatique

MISSION ESSENTIELLE

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.

ACTIVITÉS ET TÂCHES

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

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

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

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

FORMATION / EXPÉRIENCE PROFESSIONNELLE

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

COMPÉTENCES

COMPÉTENCES CŒUR DE MÉTIER
Maîtrise du système d'information, de l'urbanisation et de l'architecture du SI
Sécurité des systèmes d'exploitation
Sécurité des réseaux et protocoles
Contribution des architectures à la sécurité : conception et modèles
Contribution des architectures à la sécurité : intégration des systèmes
Connaissances des solutions de sécurité du marché
Veille technologique cybersécurité et étude des tendances
Innovation cybersécurité
Capacité de compréhension des menaces cybersécurité

COMPÉTENCES COMPORTEMENTALES
Capacité à travailler en transverse au sein de l'organisation
Capacité à s'intégrer dans des réseaux pour pratiquer une veille technologique

TENDANCES ET FACTEURS D'ÉVOLUTION DU MÉTIER

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

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

Spécialiste sécurité d'un domaine technique

Équivalence en anglais :
Technical security expert

Autres titres équivalents :
- **FR :** Expert cybersécurité
- **EN :** *Cyber security expert*

MISSION ESSENTIELLE

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.

ACTIVITÉS ET TÂCHES

PARTICIPATION AUX ÉTUDES DANS SON DOMAINE D'EXPERTISE
Conduire des études pour la sécurisation de son domaine d'expertise
Participer à l'élaboration des standards techniques de sécurité et de la documentation technique
Intervenir dans le choix des fournisseurs
Analyser, recommander et valider les choix d'implémentation

SOUTIEN AUPRÈS DES ÉQUIPES DE SON DOMAINE D'EXPERTISE
Assister et conseiller sur la mise en œuvre de systèmes et de produits respectant l'état de l'art de la sécurité en la matière
Diagnostiquer les dysfonctionnements et contribuer à la remédiation lors d'incidents ou de crises de sécurité
Contribuer au paramétrage efficace des solutions de sécurité
Proposer des techniques de contrôle du respect des politiques de sécurité dans son domaine d'expertise, aider la constitution de tableaux de bord de contrôle

PARTAGE DE CONNAISSANCES ET VEILLE TECHNOLOGIQUE DANS SON DOMAINE D'EXPERTISE
Être l'interface reconnue des experts extérieurs et de la communauté
Maintenir des relations avec les fournisseurs pour analyser les évolutions techniques des solutions de sécurité et des tendances et innovations du marché sur son périmètre d'expertise
Proposer des solutions pour améliorer la sécurité sur son périmètre d'expertise

FORMATION / EXPÉRIENCE PROFESSIONNELLE

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

COMPÉTENCES

COMPÉTENCES CŒUR DE MÉTIER
Maîtrise du système d'information, de l'urbanisation et de l'architecture du SI
Contribution des architectures à la sécurité : conception et modèles

Contribution des architectures à la sécurité : intégration des systèmes
Connaissances des solutions de sécurité du marché
Veille technologique cybersécurité et étude des tendances
Innovation cybersécurité
Configuration des outils liés à la sécurité
Capacité de compréhension des menaces cybersécurité
Cyberdéfense : connaissance des vulnérabilités des environnements

COMPÉTENCES COMPORTEMENTALES
Pédagogie sur les sujets de cybersécurité
Capacité à définir des procédures
Rédaction de rapports adaptés à différents niveaux d'interlocuteurs
Capacité à s'intégrer dans des réseaux pour pratiquer une veille technologique
Capacité d'influence

TENDANCES ET FACTEURS D'ÉVOLUTION DU MÉTIER

Le spécialiste est issu d'un autre métier (architecte, auditeur, administrateur, etc.).

Spécialiste en développement sécurisé

Équivalence en anglais :
Application security expert

Autres titres équivalents :
▶ **FR :** spécialiste en sécurité applicative, spécialiste en sécurité logicielle, expert en sécurité applicative, expert en développement sécurisé
▶ **EN :** *Security in development expert, DevSecOps*

MISSION ESSENTIELLE

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.

ACTIVITÉS ET TÂCHES

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

SOUTIEN AUPRÈS DES ÉQUIPES DE DÉVELOPPEMENT
Participer à la rédaction des exigences de sécurité applicative
Faire respecter les bonnes pratiques de sécurité du développement sur les projets et, en phase d'intégration, contribuer aux sprints pour suivre les revues sécurité pour les développements en méthode agile
Assurer la formation des développeurs aux techniques de développement sécurisé et aux risques de sécurité sur la base de *frameworks* de développement sécurisé du marché ; les former aux outils de revue de code
Évaluer la bonne implémentation des exigences de sécurité à travers des audits applicatifs et des revues de code
Prioriser les vulnérabilités rencontrées et accompagner les développeurs dans la bonne prise en compte des mesures de remédiation

PARTAGE DE CONNAISSANCES ET VEILLE TECHNOLOGIQUE
Assurer une veille technologique sur les techniques de développement sécurisé
Proposer des solutions pour améliorer la sécurité sur son périmètre d'expertise

FORMATION / EXPÉRIENCE PROFESSIONNELLE

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

COMPÉTENCES

COMPÉTENCES CŒUR DE MÉTIER
Développement logiciel et ingénierie logicielle (sous l'angle de la sécurité) : conception et développement des applications

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

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

TENDANCES ET FACTEURS D'ÉVOLUTION DU MÉTIER

Dans le cadre d'une démarche agile, le spécialiste en développement sécurisé intervient au sein des équipes pour définir les users stories et les abusers stories et suivre la prise en compte des anomalies (démarche DevSecOps). En sus des compétences en sécurité applicative, le métier nécessitera une compétence en gestion opérationnelle de la sécurité de systèmes et en sécurité des middlewares.

Cryptologue

Équivalence en anglais :
Cryptologist

Autres titres équivalents :
▶ **FR :** Expert en cryptographie, Cryptographe

MISSION ESSENTIELLE

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.

ACTIVITÉS ET TÂCHES

Concevoir et analyser la sécurité des algorithmes cryptographiques et leurs modes opératoires
Concevoir et analyser la sécurité des protocoles cryptographiques
Assurer la connaissance sur l'utilisation de produits cryptographiques (bibliothèques logicielles, équipements matériels)
Réaliser l'implémentation sécurisée d'algorithmes cryptographiques
Réaliser une évaluation sécuritaire de la mise en œuvre de la cryptographie dans un contexte donné
Assurer un travail de veille scientifique et technique sur le sujet

FORMATION / EXPÉRIENCE PROFESSIONNELLE

Formation : Bac+5 à doctorat

COMPÉTENCES

COMPÉTENCES CŒUR DE MÉTIER
Maîtrise de la cryptographie
Veille technologique cybersécurité et étude des tendances

COMPÉTENCES COMPORTEMENTALES
Rigueur
Capacité à définir des procédures
Capacité à s'intégrer dans des réseaux pour pratiquer une veille technologique

TENDANCES ET FACTEURS D'ÉVOLUTION DU MÉTIER

La cryptologie est utilisée dans de nombreux secteurs d'activité : les systèmes bancaires, l'industrie des cartes à puce, les télécommunications et la téléphonie mobile, les équipements réseaux, la protection de documents et de données, etc. L'évolution des dernières avancées sur la question de la faisabilité des ordinateurs quantiques soulève une menace non clairement identifiée sur les algorithmes cryptographiques utilisés actuellement. Le cryptologue se doit donc, de plus en plus, de se tenir informé des évolutions en cours dans le domaine de la cryptographie post-quantique.

Administrateur de solutions de sécurité

Équivalence en anglais :
Security solution administrator

Autres titres équivalents :
▶ **FR :** Administrateur de sécurité informatique

MISSION ESSENTIELLE

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.

ACTIVITÉS ET TÂCHES

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

MAINTENANCE
Maintenir et faire évoluer les solutions de sécurité de son périmètre, dans un objectif de qualité, de productivité et de sécurité globale
Assurer le suivi et la remédiation des vulnérabilités identifiées

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

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

FORMATION / EXPÉRIENCE PROFESSIONNELLE

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

COMPÉTENCES

COMPÉTENCES CŒUR DE MÉTIER
Maîtrise du système d'information, de l'urbanisation et de l'architecture du SI

Maîtrise des processus de production
Sécurité des systèmes d'exploitation
Sécurité des réseaux et protocoles
Configuration des outils liés à la sécurité

COMPÉTENCES COMPORTEMENTALES
Rigueur
Capacité à définir des procédures

TENDANCES ET FACTEURS D'ÉVOLUTION DU MÉTIER

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.

Auditeur de sécurité organisationnelle

Équivalence en anglais : *Cyber security organisational auditor*

Autres titres équivalents :
- **FR :** Expert audit sécurité organisationnelle
- **EN :** *Security control assessor*

MISSION ESSENTIELLE

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.

ACTIVITÉS ET TÂCHES

RÉALISATION DES AUDITS
Adopter une vision globale du système d'information à auditer
Définir les plans d'audits et de contrôles au sein de l'organisation
Mener des contrôles permanents et/ou périodiques de sécurité, notamment sur la base de revues documentaires, de collecte de preuves, d'accès aux consoles et aux rapports des outils de sécurité ou de l'utilisation d'outils automatisés de contrôle de conformité
Mener et documenter des audits des processus de sécurité, analyser la documentation et les preuves, procéder à des interviews des équipes
Évaluer la bonne application, l'efficacité et la conformité des politiques et procédures de sécurité de l'entreprise
Évaluer la conformité à une norme ou à un référentiel, établir l'éligibilité à une certification
Rédiger des rapports intégrant une analyse des vulnérabilités et écarts constatés et mettre en évidence et évaluer les risques de sécurité et leurs impacts sur les métiers
Définir les recommandations permettant de remédier aux risques découlant des vulnérabilités découvertes
Collaborer avec les équipes informatiques pour mettre en œuvre les recommandations
Produire des tableaux de bord du niveau de sécurité et de conformité

FORMATION / EXPÉRIENCE PROFESSIONNELLE

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

COMPÉTENCES

COMPÉTENCES CŒUR DE MÉTIER
Connaissance de la gouvernance, des normes et des standards : maîtrise des méthodologies d'audits
Connaissance du système d'information et des principes d'architecture
Maîtrise des fondamentaux dans les principaux domaines de la SSI
Connaissance de la gouvernance, des normes et des standards dans le domaine de la sécurité : normes ISO (2700X), normes sectorielles (PCI-DSS…)

COMPÉTENCES COMPORTEMENTALES
Capacité de synthèse et de vulgarisation pour des publics non techniques
Rédaction de rapports adaptés à différents niveaux d'interlocuteurs
Rigueur

Auditeur de sécurité technique

Équivalence en anglais :
Cyber security technical auditor

Autres titres équivalents :
▶ **FR :** Expert technique en audit sécurité, auditeur informatique, expert en tests d'intrusions
▶ **EN :** *Ethical Hacker, Vulnerability assessor, Pentester, Information Security Auditor, Penetration tester, Vulnerability assessment analyst*

MISSION ESSENTIELLE

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.).

ACTIVITÉS ET TÂCHES

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

RÉALISER OU PILOTER LA MISE EN ŒUVRE DE SCANS DE VULNÉRABILITÉS ET DE CONTRÔLES TECHNIQUES, EN CONTINU ET DE MANIÈRE AUTOMATISÉE
Procéder à des interviews des équipes pour évaluer les impacts pour l'organisation des vulnérabilités détectées
Rédiger des rapports intégrant une analyse des vulnérabilités rencontrées et une identification des causes ; mettre en évidence et évaluer les risques de sécurité et les impacts pour les métiers
Définir les recommandations permettant de remédier aux risques découlant des vulnérabilités découvertes
Collaborer avec les équipes informatiques pour mettre en œuvre les recommandations techniques
Produire des tableaux de bord du niveau de sécurité et de conformité

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

FORMATION / EXPÉRIENCE PROFESSIONNELLE

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

COMPÉTENCES

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

COMPÉTENCES COMPORTEMENTALES
Capacité de synthèse et de vulgarisation pour des publics non techniques
Rédaction de rapports adaptés à différents niveaux d'interlocuteurs
Sens éthique
Capacité de travail en équipe
Rigueur

TENDANCES ET FACTEURS D'ÉVOLUTION DU MÉTIER

L'auditeur sécurité technique peut être amené à réaliser des audits de type red team qui visent à simuler des attaques en grandeur réelle dans le but de tester les défenses de l'organisation. Il peut également être amené à réaliser des audits dans une approche purple team afin d'entrainer les équipes de détection des incidents de cybersécurité.

GESTION DES INCIDENTS ET DES CRISES DE SÉCURITÉ

Responsable du SOC (*Security Operation Center*)

Équivalence en anglais :
SOC Manager

Autres titres équivalents :
▶ **FR :** Responsable du centre opérationnel de sécurité, responsable du centre de Cyberdéfense, responsable du service de détection des incidents de sécurité
▶ **EN :** *Security Operation Center manager, Operational security manager*

MISSION ESSENTIELLE

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.

ACTIVITÉS ET TÂCHES

PILOTAGE DES OPÉRATIONS
Planifier et organiser les opérations quotidiennes du SOC
Assurer un appui opérationnel à la gestion de crise de sécurité en cas d'incidents de sécurité majeurs
Assurer les relations avec les équipes de réponse à incidents CERT (*Computer Emergency Response Team*) ou CSIRT (*Computer Security Incident Response Team*), notamment en situation de crise pour coordonner les différentes équipes de sécurité opérationnelle

STRATÉGIE DE PRÉVENTION ET DE DÉTECTION
Définir la stratégie du SOC, assurer la cohérence technique, prendre en compte les exigences réglementaires
Définir et mettre en œuvre les outils du SOC pour la collecte des évènements, l'accès aux plateformes de sécurité, la recherche d'évènements suspects, la gestion des alertes, les workflows de suivi d'incidents de sécurité
Alimenter la stratégie de détection à partir d'une vision globale de la nature et du niveau de vulnérabilité du SI
Définir les cas d'usages de détection et les intégrer dans les outils de détection
Définir et mettre en place les processus de notification et d'escalade
Évaluer et valider l'efficacité des outils déployés dans le SOC et conduire les plans d'action correctifs nécessaires le cas échéant
Créer des synergies avec les autres équipes de sécurité en partageant les informations sur les menaces identifiées (en interne comme en externe)

FORMATION / EXPÉRIENCE PROFESSIONNELLE

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

COMPÉTENCES

COMPÉTENCES CŒUR DE MÉTIER
Sécurité des systèmes d'exploitation

Sécurité des réseaux et protocoles
Cyberdéfense : connaissance en gestion de crise
Cyberdéfense : pratique de l'analyse de journaux (systèmes ou applicatifs)
Cyberdéfense : pratique de l'analyse de flux réseaux
Cyberdéfense : connaissance d'outils et de méthodes de corrélation de journaux d'évènements (SIEM)
Cyberdéfense : connaissance des solutions de supervision sécurité
Cyberdéfense : connaissance des techniques d'attaques et d'intrusions
Cyberdéfense : connaissance des vulnérabilités des environnements
Scripting

COMPÉTENCES COMPORTEMENTALES
Management d'équipe
Capacité à travailler en transverse dans l'organisation
Capacité à travailler en équipe
Capacité à résister à la pression
Capacité de restitution et de vulgarisation pour des publics non techniques
Sens éthique

TENDANCES ET FACTEURS D'ÉVOLUTION DU MÉTIER

Le responsable du SOC doit acquérir une bonne compréhension des besoins de supervision pour les activités métiers critiques afin d'assurer le développement des cas d'usages applicatifs et spécifiques (e.g. surveillance des SI industriels). De plus, le responsable du SOC doit gérer de plus en plus d'incidents de sécurité et doit par conséquent développer une bonne compréhension des menaces qui pèsent sur son périmètre. Cette compréhension fine des menaces lui permet de concevoir au mieux les actions de prévention et de détection et d'être efficace dans la réponse apportée. Pour suivre l'évolution des tendances, il pourra être amené à développer des compétences en *machine learning* et en *threat intelligence* afin de renforcer les capacités de détection.

Opérateur analyste SOC (*Security Operation Center*)

Équivalence en anglais :
SOC analyst

Autres titres équivalents :
- FR : Analyste CyberSOC, Analyste détection d'incident, Veilleur-Analyste, Opérateur analyste SOC
- EN : *Cyber Defense Analyst*

MISSION ESSENTIELLE

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.

ACTIVITÉS ET TÂCHES

DÉTECTION
Identifier les évènements de sécurité en temps réel, les analyser et les qualifier
Évaluer la gravité des incidents de sécurité
Notifier les incidents de sécurité, escalader le cas échéant

RÉACTION
Transmettre les plans d'action aux entités en charge du traitement et apporter un support concernant les correctifs ou palliatifs à mettre en œuvre
Faire des recommandations sur les mesures immédiates
Accompagner le traitement des incidents par les équipes d'investigation

MISE EN PLACE DES D'USAGES ET DES OUTILS
Contribuer à la mise en place du service de détection (SIEM, etc.)
Contribuer à la définition de la stratégie de collecte des journaux d'évènements
Participer au développement et au maintien des règles de corrélation d'évènements

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

REPORTING ET DOCUMENTATION
Renseigner les tableaux de bord rendant compte de l'activité opérationnelle
Maintenir à jour la documentation
Atívités de recherche de compromissions (*threat hunting*)

FORMATION / EXPÉRIENCE PROFESSIONNELLE

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

COMPÉTENCES

COMPÉTENCES CŒUR DE MÉTIER
Sécurité des systèmes d'exploitation
Sécurité des réseaux et protocoles
Cyberdéfense : pratique de l'analyse de journaux (systèmes ou applicatifs)
Cyberdéfense : pratique de l'analyse de flux réseaux
Cyberdéfense : connaissance d'outils et de méthodes de corrélation de journaux d'évènements (SIEM)
Cyberdéfense : connaissances des solutions de supervision sécurité
Cyberdéfense : connaissance des techniques d'attaques et d'intrusions
Cyberdéfense : connaissances des vulnérabilités des environnements
Scripting

COMPÉTENCES COMPORTEMENTALES
Capacité à travailler en équipe
Capacité à définir des procédures

TENDANCES ET FACTEURS D'ÉVOLUTION DU MÉTIER

L'opérateur du SOC pourra être amené à développer des compétences en *machine learning* afin de renforcer les capacités de détection.

Responsable du CSIRT (*Computer Security Incident Response Team*)

Équivalence en anglais :
CERT (Computer Emergency Response Team) Manager

Autres titres équivalents :
- **FR :** Pilote du CERT, Responsable d'un service de réponse aux incidents de sécurité
- **EN :** *Computer Emergency Response Team Manager, Computer Security Incident Response Team Manager*

MISSION ESSENTIELLE

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.

ACTIVITÉS ET TÂCHES

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

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

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

FORMATION / EXPÉRIENCE PROFESSIONNELLE

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

COMPÉTENCES

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

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

TENDANCES ET FACTEURS D'ÉVOLUTION DU MÉTIER

Le 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.

Analyste réponse aux incidents de sécurité

Équivalence en anglais :
Forensic analyst

Autres titres équivalents :
▶ **FR :** Analyste CERT, analyste CSIRT, spécialiste en investigation numérique, analyste traitement d'incidents
▶ **EN :** *Incident Responder, First Incident Responder, Digital Forensics Analyst, Cyber Defense Forensics Analyst*

MISSION ESSENTIELLE

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.

ACTIVITÉS ET TÂCHES

ANTICIPATION
Réaliser une veille sur les nouvelles vulnérabilités, sur les nouvelles technologies et sur les méthodes des attaques relatives aux différents composants du système d'information
Alimenter les bases de renseignement sur les menaces (*threat intelligence*)
Maintenir et développer des outils d'investigation

ANALYSE DES INCIDENTS
Collecter les informations techniques d'un large ensemble de systèmes d'information, réaliser la recherche d'indicateurs de compromission
Analyser les relevés techniques réalisés afin d'identifier le mode opératoire et l'objectif de l'attaquant et de qualifier l'étendue de la compromission
Rédiger des rapports d'investigation

CONSEIL
Préconiser des mesures de contournement et de remédiation de l'incident (assainissement et durcissement)
Préconiser des mesures d'amélioration des capacités d'analyse (extraction des indicateurs de compromission)
Préparer des rapports

FORMATION / EXPÉRIENCE PROFESSIONNELLE

Formation Bac +5, dont spécialisation en cybersécurité

COMPÉTENCES

COMPÉTENCES CŒUR DE MÉTIER
Maîtrise du système d'information, de l'urbanisation et de l'architecture du SI
Analyse post-mortem (forensic) : connaissance des outils d'analyse

Analyse post-mortem (forensic) : connaissance des procédures légales
Cyberdéfense : pratique de l'analyse de flux réseaux
Cyberdéfense : connaissance des techniques d'attaques et d'intrusions
Cyberdéfense : connaissance des vulnérabilités des environnements
Scripting

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

TENDANCES ET FACTEURS D'ÉVOLUTION DU MÉTIER

L'analyste réponse aux incidents de sécurité peut être spécialisé en tant qu'analyste système, analyste réseau, analyste de codes malveillants.

Gestionnaire de crise de cybersécurité

Équivalence en anglais :
Cyber security crisis manager

Autres titres équivalents :
▶ **FR :** Organisateur de la gestion de crise de cybersécurité

MISSION ESSENTIELLE

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.

ACTIVITÉS ET TÂCHES

ANTICIPATION
Conseiller l'organisation pour lui permettre de disposer d'une capacité de gestion de crises de cybersécurité majeures
Définir les moyens nécessaires à la gestion de crise : plans, procédure, ressources, etc.
Vérifier que tous les éléments de préparation des crises sont présents
Assurer la formation et l'entraînement des acteurs métiers ou support susceptibles d'intervenir en cas de crise de cybersécurité ; tester et valider la capacité de l'organisation à réagir à une attaque

RÉACTION
Organiser la gestion de crise pour agir et traiter la crise de cybersécurité
Animer la cellule de crise décisionnelle et contribuer aux cellules de crise opérationnelles
Coordonner l'action des différentes parties en présence et la diffusion des informations vers les parties prenantes
Suivre et coordonner les plans d'actions en matière d'investigation et de remédiation
Assurer les relations avec les autorités, les assurances et des experts externes éventuels
S'assurer de la cohérence de la stratégie de communication de crise vis-à-vis des parties prenantes
Organiser les revues post-mortem et la prise en compte des retours d'expérience pour donner suite aux incidents et proposer l'amélioration des dispositifs de prévention, détection et réaction

FORMATION / EXPÉRIENCE PROFESSIONNELLE

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

COMPÉTENCES

COMPÉTENCES CŒUR DE MÉTIER
Bonne connaissance des enjeux et des métiers de l'organisation
Connaissance des technologies de sécurité et des outils associés
Maîtrise des fondamentaux dans les principaux domaines de la SSI
Cyberdéfense : connaissance en gestion de crise
Connaissance juridique en matière de droit informatique lié à la sécurité et à la protection des données
Cyberdéfense : connaissance des types d'attaques et d'intrusions
Cyberdéfense : connaissance des vulnérabilités des environnements

COMPÉTENCES COMPORTEMENTALES
Sens de l'intérêt général
Capacité à gérer des situations de crise
Capacité d'appropriation des enjeux métiers
Capacité de restitution et de vulgarisation à des publics non techniques
Capacité à coordonner de nombreuses équipes
Capacité à résister à la pression
Capacité à communiquer en interne et en externe

TENDANCES ET FACTEURS D'ÉVOLUTION DU MÉTIER

Au sein des organisations qui ne disposent pas d'une structure de réponse à incidents spécifique, 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.

Analyste de la menace cybersécurité

Équivalence en anglais :
Cyber threat intelligence analyst

Autres titres équivalents :
- **FR :** Analyste cyber *threat intelligence*
- **EN :** *Threat hunter*

MISSION ESSENTIELLE

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.

ACTIVITÉS ET TÂCHES

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

ACTIVITÉS DE RENSEIGNEMENT (*THREAT INTELLIGENCE*) SUR LE CONTEXTE DES MENACES CYBERSÉCURITÉ
Comprendre les enjeux et le contexte de la cybermenace, réaliser une veille sur les menaces émergentes
Qualifier les menaces pouvant viser un type d'organisation, étudier le niveau d'exposition aux risques
Apporter un support dans la compréhension des incidents rencontrés

SUPPORT À L'AMÉLIORATION DES MOYENS DE DÉTECTION
Analyser les techniques d'attaques et les modes opératoires connus
Améliorer les capacités de détection

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

FORMATION / EXPÉRIENCE PROFESSIONNELLE

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

COMPÉTENCES

COMPÉTENCES CŒUR DE MÉTIER
Bonne connaissance des enjeux et des métiers de l'organisation
Capacité de compréhension des menaces cybersécurité
Capacité à exploiter des sources ouvertes de manière sécurisée
Mise en place de plans de veille sur un ou plusieurs secteurs déterminés
Détection, qualification et analyse d'informations pertinentes
Veille géopolitique et géostratégique

COMPÉTENCES COMPORTEMENTALES
Capacité de synthèse des éléments analysés
Rigueur
Capacité à s'intégrer dans des réseaux pour pratiquer une veille technologique

TENDANCES ET FACTEURS D'ÉVOLUTION DU MÉTIER

Ce métier est en développement au sein des organisations qui possèdent une structure de type SOC.

CONSEIL, SERVICES ET RECHERCHE

Consultant en cybersécurité

Équivalence en anglais :
Cybersecurity consultant

Autres titres équivalents :
▶ **FR :** Consultant sécurité, consultant en SSI

MISSION ESSENTIELLE

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.

ACTIVITÉS ET TÂCHES

CONSEIL SUR LA STRATÉGIE DE SÉCURITÉ
Contribuer à définir la stratégie de cybersécurité et de conformité (à une réglementation, à des référentiels d'exigences) de l'organisation du client, évaluer l'engagement budgétaire nécessaire
Réaliser des évaluations du niveau de sécurité de l'organisation du client, le comparer à l'état de l'art du marché
Effectuer des préconisations et des recommandations sur l'amélioration du niveau de sécurité
Informer et sensibiliser les directions générales et les directions métiers sur les enjeux de cybersécurité et l'état de la menace

ASSISTANCE AUX ÉQUIPES SÉCURITÉ
Mettre en place des méthodologies et des processus de sécurité, réaliser des analyses de risques de sécurité
Intervenir dans l'intégration des normes de sécurité et apporter une expertise lors de la mise en œuvre des projets de sécurité
Assister dans le choix et l'utilisation des outils de sécurité, informer sur les évolutions des outils
Apporter son expertise pour analyser des incidents de sécurité et établir des plans correctifs et d'amélioration de la sécurité des SI (sur les plans technique et organisationnel)
Former les utilisateurs, intervenants techniques et autres relais opérationnels aux technologies et systèmes de sécurité

APPORT D'EXPERTISE TECHNIQUE
Assurer une veille sur les menaces existantes et émergentes et définir les mesures de protection à mettre en place
Apporter une expertise sur les incidents de sécurité sur le système d'information, sur les techniques utilisées et le profil des attaquants le cas échéant
Apporter une expertise sur la sécurité dans un domaine technique (état de l'art)

FORMATION / EXPÉRIENCE PROFESSIONNELLE

Formation : Bac +5, dont une spécialisation en cybersécurité

COMPÉTENCES

COMPÉTENCES CŒUR DE MÉTIER
Maîtrise des fondamentaux dans les principaux domaines de la SSI
Connaissance des technologies de sécurité et des outils associés
Gestion des risques, politique de cybersécurité et SMSI
Connaissance de la gouvernance, des normes et des standards dans le domaine de la sécurité : normes ISO (2700X), normes sectorielles (PCI-DSS…)
Cyberdéfense : connaissance des vulnérabilités des environnements
Veille technologique cybersécurité et étude des tendances

COMPÉTENCES COMPORTEMENTALES
Capacité à réaliser un diagnostic et à proposer des solutions adaptées au contexte
Sens de l'écoute des besoins des clients
Capacité de synthèse des éléments analysés
Rigueur
Capacité de restitution au management
Capacité à travailler en transverse au sein de l'organisation
Rédaction de rapports adaptés à différents niveaux d'interlocuteurs
Pédagogie sur les sujets de cybersécurité
Capacité de travail en équipe

TENDANCES ET FACTEURS D'ÉVOLUTION DU MÉTIER

Le consultant sécurité est souvent spécialisé dans un ou plusieurs domaines de cybersécurité : sécurité organisationnelle, sécurité technique, IAM, etc.

Formateur en cybersécurité

Équivalence en anglais :
Cyber security trainer

Autres titres équivalents :
▶ **FR :** chargé de formation en sécurité des SI

MISSION ESSENTIELLE

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.

ACTIVITÉS ET TÂCHES

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

FORMATION / EXPÉRIENCE PROFESSIONNELLE

Formation : Bac +5, dont une spécialisation en informatique

COMPÉTENCES

COMPÉTENCES CŒUR DE MÉTIER
Maîtrise des outils et plateformes spécifiques à la formation en SSI
Connaissance du système d'information et des principes d'architecture
Connaissance des technologies de sécurité et des outils associés
Gestion des risques, politique de cybersécurité et SMSI
Maîtrise des fondamentaux dans les principaux domaines de la SSI
Veille technologique cybersécurité et étude des tendances

COMPÉTENCES COMPORTEMENTALES
Capacité de travail en équipe
Pédagogie sur les sujets de cybersécurité

Évaluateur de la sécurité des technologies de l'information

Equivalence en anglais :
IT Security Evaluation Facility (ITSEF) Specialist

Autres titres équivalents :
▶ **FR :** Responsable évaluation

MISSION ESSENTIELLE

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*).

ACTIVITÉS ET TÂCHES

RÉALISATION DE L'ÉVALUATION
Respecter une procédure et une méthodologie d'évaluation selon des critères préalablement définis
Vérifier que la documentation fournie par le développeur est conforme
Réaliser des tests techniques afin de vérifier que les fonctions de sécurité atteignent le niveau requis de robustesse en adéquation avec la cible de sécurité et le niveau de certification visé
Évaluer la robustesse des mécanismes cryptologiques du produit
Rédiger le rapport d'évaluation à destination de l'autorité de certification
Participer à l'amélioration continue des moyens et des méthodes d'évaluation

ASSISTANCE À UN COMMANDITAIRE POUR LA PRÉPARATION D'UNE ÉVALUATION RÉALISÉE PAR UN AUTRE ÉVALUATEUR
Assister à la rédaction de la cible de sécurité et des fournitures nécessaires à l'évaluation
Conduire des tests de sécurité amont

FORMATION / EXPÉRIENCE PROFESSIONNELLE

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)

COMPÉTENCES

COMPÉTENCES CŒUR DE MÉTIER
Certifications et évaluations de produits : connaissance des processus d'évaluation sécuritaires (Critères Communs, CPSN, etc.)
Sécurité de l'électronique et des architectures matérielles

Tests d'intrusion : maîtrise des techniques d'audits techniques de sécurité
Cyberdéfense : connaissance des techniques d'attaques et d'intrusions
Cyberdéfense : connaissance des vulnérabilités des environnements
Connaissance en rétro-ingénierie de systèmes (ou *reverse engineering*)
Connaissance en développement (codes embarqués, langages de conception, *scripting*)

COMPÉTENCES COMPORTEMENTALES
Rigueur
Rédaction de rapports adaptés à différents niveaux d'interlocuteurs
Capacité à travailler en équipe

TENDANCES ET FACTEURS D'ÉVOLUTION DU MÉTIER

L'évaluateur devra prendre en compte les réglementations internationales, notamment celles liées à la certification des produits connectés.

Développeur de solutions de sécurité

Équivalence en anglais :
Security product developer

MISSION ESSENTIELLE

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.

ACTIVITÉS ET TÂCHES

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

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

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

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

FORMATION / EXPÉRIENCE PROFESSIONNELLE

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

COMPÉTENCES

COMPÉTENCES CŒUR DE MÉTIER
Développement logiciel et ingénierie logicielle (sous l'angle de la sécurité) : conception et développement des applications
Développement logiciel et ingénierie logicielle (sous l'angle de la sécurité) : connaissance des vulnérabilités logicielles
Maîtrise du système d'information, de l'urbanisation et de l'architecture du SI
Connaissance des couches applicatives
Connaissance en développement (codes embarqués, langages de conception)
Contribution des architectures à la sécurité : intégration des systèmes

Cyberdéfense : connaissance des techniques d'attaques et d'intrusions
Cyberdéfense : connaissance des vulnérabilités des environnements

COMPÉTENCES COMPORTEMENTALES
Rigueur
Capacité à produire des procédures

Intégrateur de solutions de sécurité

Equivalence en anglais :
Security product integrator

MISSION ESSENTIELLE

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.

ACTIVITÉS ET TÂCHES

CONCEPTION
Définir, sous la responsabilité du responsable de projet, l'architecture fonctionnelle et technique du système d'information
Assembler et intégrer les différents composants
Définir les interfaces et définir les composants à faire évoluer pour permettre leur intégration
Documenter la solution

INTÉGRATION DE LA SOLUTION DANS L'ENVIRONNEMENT DE PRODUCTION
Contribuer à la définition de l'architecture technique cible
Mettre en œuvre les phases de test et de maquettage
Mettre en œuvre la recette, l'industrialisation et la mise en production, en liaison avec le responsable du projet
Réaliser le paramétrage de la solution pour garantir la meilleure efficacité en termes de sécurité
Documenter les processus de mise en œuvre, de mise à jour et d'exploitation des composants de sécurité

MAINTENANCE ET INFOGÉRENCE
Assurer la supervision des services, assurer la métrologie, gérer les alertes et les incidents de production
Préconiser les montées de versions de la solution
Pratiquer une veille sur les vulnérabilités et gérer le patching des solutions

EXPERTISE ET CONSEIL
Conseiller sur le paramétrage de la solution
Délivrer des formations sur la nouvelle solution de sécurité

VEILLE TECHNOLOGIQUE
Assurer une veille technologique dans le domaine

FORMATION / EXPÉRIENCE PROFESSIONNELLE

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

COMPÉTENCES

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

COMPÉTENCES COMPORTEMENTALES
Capacité à travailler en transverse au sein de l'organisation
Capacité de travail en équipe
Rigueur
Capacité à définir des procédures

Chercheur en sécurité des systèmes d'information

Equivalence en anglais :
Cyber security researcher

MISSIONS ESSENTIELLES

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.

ACTIVITÉS ET TÂCHES

MENER UN PROJET DE RECEHRCHE
Concevoir, présenter et mener un projet de recherche en autonomie et/ou en partenariat avec des pairs au sein de son unité (laboratoire) mais aussi en lien avec des partenaires externes
Imaginer des solutions innovantes et créatrices de connaissances, de technologies et de valeur, proposer de nouvelles approches, de nouvelles méthodes, aborder les objets, procédés et champs de recherche de manière innovante et inédite
Assurer une veille scientifique et technologique et anticiper les problématiques opérationnelles et les défis à venir dans son domaine
S'insérer dans un écosystème de recherche
Documenter les travaux réalisés et participer à la valorisation et au transfert des résultats obtenus
Contribuer et participer à des événements en lien avec son champ de recherche (réunions scientifiques, démonstrations, groupes de travail…)
Répondre à des appels d'offre et s'insérer dans des projets multi-acteurs
Vulgariser, diffuser, enseigner

FORMATION / EXPÉRIENCE PROFESSIONNELLE

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

COMPÉTENCES

COMPÉTENCES CŒUR DE MÉTIER
Connaissance des méthodes de production et de valorisation du savoir scientifique
Maîtrise du socle scientifique et technique pertinent pour le domaine de la SSI concerné
Connaissance de l'écosystème de recherche du secteur
Capacité à déceler et décliner en axes de recherche les enjeux technologiques émergents
Connaissance des technologies de sécurité et des outils associés

COMPÉTENCES COMPORTEMENTALES
Capacité à travailler en transverse au sein de l'organisation
Capacités d'encadrement
Capacités à collaborer avec ses pairs au sein d'une communauté
Pédagogie

TENDANCES ET FACTEURS D'ÉVOLUTION DU MÉTIER

Le chercheur en sécurité des SI peut appartenir à une équipe de recherche et développement (R&D). Son activité est alors davantage pilotée par les perspectives d'opérationnalisation des avancées scientifiques et techniques attendues. Il mène une activité de veille technologique pointue et intègre dans sa démarche les attendus des produits et services du point de vue des usages.

Dans le domaine de la recherche publique, le chercheur en sécurité des SI peut collaborer avec une équipe de recherche dont les axes de travail ne sont pas strictement dédiés à la sécurité. Cette multidisciplinarité est souvent nécessaire pour appréhender la complexité du domaine.

L'intrication croissante des problématiques techniques et comportementales dans le champ de la cybersécurité conduira probablement les chercheurs et les équipes à collaborer de manière interdisciplinaire afin d'aborder des objets de recherche intégrant solutions techniques et réflexion sur les usages.

MÉTIERS CONNEXES

MÉTIERS CONTRIBUANT À LA DÉMARCHE DE CYBERSÉCURITÉ

Au sein des organisations, les acteurs de la cybersécurité interagissent avec d'autres acteurs qui contribuent également à la démarche globale de cybersécurité, en particulier les acteurs des filières « continuité d'activité », « protection des données à caractère personnel », « risk management », « sûreté », « assurance » et « contrôle interne ».

Les métiers sont présentés au sein de ce panorama pour permettre d'appréhender la cohérence et les interactions existantes.

MÉTIERS	PRINCIPALES FONCTIONS	PRINCIPALES INTERACTIONS ENTRE CES MÉTIERS ET LA CYBERSÉCURITÉ
Responsable du plan de continuité d'activité (RPCA) *Business Continuity Manager (BCM)*	Il élabore et met en œuvre 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 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.
Délégué à la protection des données (DPD) *Correspondant informatique et libertés (CIL)* *Data protection officer (DPO)* *Privacy compliance manager* *Privacy officer* *Data protection officer*	Il est chargé de mettre en œuvre 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 œuvre 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 mène des analyses de risques complémentaires dans les projets (*security & privacy by design*).
Manager de risques *Risk Manager*	Il s'assure que tout ou partie des risques de l'organisation sont bien identifiés et couverts : il présente à la Direction générale les risques de l'organisation, il propose des solutions de maîtrise des risques optimisées en termes de financement, afin de poser des limites acceptables à la prise de risques ; il 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.
Directeur sûreté *Safety Manager*	Il définit et organise les moyens, dispositifs et systèmes visant à la protection des installations et des personnes. Il est garant de la sûreté des moyens de production. Il met en œuvre 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.

Responsable des assurances	Il 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).
Responsable du contrôle interne	Il 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.

MÉTIERS POUVANT SE SPÉCIALISER EN CYBERSÉCURITÉ

Au sein de grandes organisations, des métiers non spécifiques à la cybersécurité peuvent se spécialiser en cybersécurité dans le cadre de leurs activités habituelles.

MÉTIERS	PRINCIPALES FONCTIONS
Juriste spécialisé en cybersécurité Consultant juridique en cyberdéfense *Cyber Legal Advisor*	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 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 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 de communication spécialisé en cybersécurité	Le chargé de communication spécialisé en cybersécurité assiste les équipes cybersécurité dans la mise en œuvre opérationnelle de la communication sur l'actualité cybersécurité. Il peut aussi contribuer à préparer la communication interne et externe dans un contexte de crise de cybersécurité.
Security service delivery Manager	Le *Security service delivery manager* pilote les services de sécurité dont il a la responsabilité, au sein d'un catalogue de services mis à disposition des métiers. Il définit les indicateurs et veille à garantir auprès de son client les niveaux de services contractualisés.

ANNEXES

ÉLÉMENTS DE MÉTHOLOGIE

Afin de mieux comprendre la manière dont sont organisés et décrits les métiers du présent Panorama, il peut être utile d'exposer les principes et les partis-pris méthodologiques à l'origine de son élaboration.

NOMBRE DE MÉTIERS

Il aurait été possible d'ajouter d'autres métiers en déclinant, parfois légitimement, certains métiers qui peuvent paraître « génériques » ou en multipliant les métiers de spécialités, ou encore en déclinant plus précisément les différents niveaux hiérarchiques dans certains domaines d'expertise. Ces raffinements sont toujours possibles, parfois souhaitables, en fonction des contextes. Toutefois, le choix a été fait d'essayer de conserver une liste de taille limitée, facile à utiliser par le plus grand nombre, tout en en gardant un niveau de détail suffisant pour couvrir l'ensemble des aspects de la filière. L'idée qui porte ces choix, contestables parfois, est d'essayer de respecter en même temps les pratiques observées et les évolutions qu'il est possible de percevoir.

NIVEAU D'ABSTRACTION

Il aurait été souhaitable, au niveau de l'épure d'un outil RH complet, d'appliquer un niveau d'abstraction strictement homogène dans la typologie. En pratique, cela n'a pas été possible. Cette liste voit se côtoyer des métiers très spécialisés et des métiers aux contours moins nets, voire parfois moins exclusivement propres à la SSI. Ce choix est assumé pour pouvoir rester fidèle à un secteur dont les niveaux de maturité sont variables en fonction des organisations concernées, de la spécialisation des acteurs et de la diversité des approches choisies.

MÉTIERS DÉDIÉS À LA CYBERSÉCURITÉ

Par rapport à la liste précédente, il a été décidé de ne décrire en détails que les métiers dont la composante principale est la cybersécurité, ce qui a conduit à écarter les métiers non dédiés (correspondant, développeur, intégrateur, technicien, administrateur) et les métiers appartenant aux filières continuité d'activité et protection des données à caractère personnel (RPCA, DPO), même si évidemment ils ne sont pas sans lien avec ceux qui constituent la liste principale. Symétriquement, certains métiers présents dans la liste actuelle peuvent n'être dédiés à la sécurité que temporairement ou partiellement, pendant la durée d'un projet par exemple (responsable de projet de sécurité, directeur de programme sécurité) ; néanmoins il a été décidé de les mentionner car ce sont des métiers très présents dans les filières cybersécurité des organisations à la date de la publication.

COMPÉTENCES

Des compétences cœur de métier et comportementales ont été ajoutées par rapport à la première version du panorama. Les référentiels de compétences existants sur le marché étant trop génériques (European-e-Competence-Framework-3.0_FR) ou bien trop spécifiques (document du NIST SP800-181), il a été décidé de proposer des compétences précises mais en nombre volontairement limité, permettant de caractériser chacun des métiers. Ce point pourra évoluer à l'avenir et faire l'objet d'enrichissements locaux en fonction des besoins des organisations qui se saisiront de cet outil.

ALIGNEMENT AVEC LES PRATIQUES RH

L'évolution du référentiel propose un document utile et accessible aux fonctions RH, y compris dans un objectif de gestion de carrière (du futur candidat qui souhaite se projeter au collaborateur qui souhaite avoir une meilleure visibilité sur son évolution professionnelle) avec des fiches métiers à l'état de l'art du marché dans leur structure.

PRISE EN COMPTE DES TENDANCES

Les facteurs d'évolutions des métiers et les tendances sont précisées dans une rubrique dédiée afin d'apporter des nuances dans la description et inscrire l'outil dans une dynamique de marché observable.

MÉTIERS ET RÔLES

La pratique d'un métier peut varier en fonction de l'entreprise et en particulier, de sa taille. Ainsi, dans des grandes structures, on pourra trouver un large sous-ensemble des métiers identifiés avec parfois plusieurs personnes dans chacun de ces métiers ou des subdivision de ces métiers, alors que dans des entreprises plus petites, plusieurs métiers pourront être occupés par une seule personne : cette liste ne préjuge pas de l'organisation mise en place au sein des organisations.

GLOSSAIRE

ACRONYMES	INTITULÉS
ANSSI	Agence Nationale de la Sécurité des Systèmes d'Information
CERT	*Computer Emergency Response Team*
CISO	*Chief Information Security Officer*
CSIRT	*Computer Security Incident Response Team*
IAM	*Identity and Access Management*
PCA	Plan de Continuité d'Activité
PCI/DSS	*Payment Card Industry Data Security Standard*
PME	Petite et Moyenne Entreprise
PRA	Plan de Reprise d'Activité
RGPD	Règlement Général sur la Protection des Données
RSSI	Responsable de la Sécurité du Système d'Information
SMSI	Système de management de la sécurité de l'information
SOC	*Security Operation Center*
SSI	Sécurité des Systèmes d'Information
TPE	Très Petite Entreprise