Métiers de la SSI

18 avril 2018

Sommaire

Liste des métiers

Métiers de la SSI

18 avril 2018

Origine

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 (ou sécurité des systèmes d'information, ou Cybersécurité, etc.). Cette liste a été publiée sur le site de l'ANSSI.

La liste actualisée présentée ci-après prend en compte les évolutions du domaine ainsi que le résultat de nouvelles études sur ce sujet et en particulier :

- la liste des métiers élaborée par l'OPIIEC en 2017 suite à une étude sur étude sur « les formations et les compétences en France sur la cybersécurité » ;
- le document du NIST SP800-181 de novembre 2016.

Principes d'élaboration

Élaborer une liste de métiers dans un domaine aussi changeant est un exercice délicat. Qui plus est, certains métiers ont parfois des contours mal définis et leur dénomination peut varier d'une entreprise à l'autre.

Avant de prendre connaissance de cette liste, il est donc utile d'exposer les principes et les partis-pris à l'origine son élaboration :

- **Nombre de métiers** : la première liste publiée sur le site de l'ANSSI identifiait 16 profils métiers. Ce nombre est similaire dans la liste actuelle. Il aurait été possible d'ajouter d'autres métiers en en raffinant certains qui sont très « génériques » (typiquement, « consultants ») en fonction des spécialités mais cela n'a pas été souhaité par certains des acteurs impliqués dans la réalisation de cette liste. Cette position pourrait évoluer dans le futur.
- **Niveau d'abstraction** : il est souhaitable de conserver un niveau d'abstraction homogène dans la typologie. En pratique, cela n'a pas été possible. On trouvera donc quelques métiers très spécialisés (évaluateurs, cryptologues) côtoyant des métiers aux contours très flous (consultants) et ce choix est assumé.
- **Dédiés :** certains métiers sont propres au domaine de la sécurité (par exemple, « RSSI ») alors que d'autres sont des métiers dont l'objet principal n'est pas la sécurité mais dont la composante sécurité est significative (par exemple, « administrateur systèmes et réseaux »). Ces derniers sont pris en compte dans la présente liste.
- **Effets conjoncturels** : les métiers comme « délégué à la protection des données » ou « responsable du plan de continuité d'activité » sont de plus en plus souvent associés à la rubrique « sécurité » (des systèmes d'information) par les employeurs. Même s'il s'agit d'une vision très extensive de ce qui est normalement rattaché à la sécurité, ces métiers ont été conservés dans la présente liste.
- **Compétences** : cette version ne comporte pas de liste de compétences associée aux métiers. On notera que le document du NIST SP800-181 propose une liste de 614 compétences, 359 expertises, 119 capacités et 928 tâches associée aux différents *work-roles* que l'on peut

souvent associer à des métiers. Le lecteur intéressé pourra donc se référer utilement à cette liste.

- **Métiers et rôles** : la pratique d'un métier peut varier en fonction de l'entreprise et en particulier, de sa taille. Ainsi, dans une entreprise de petite taille, le RSSI peut être directement en charge de toutes les activités et rôles associés à son métier alors que dans une grande entreprise, les différentes activités et rôles pourront être gérés par une équipe, le RSSI ayant alors essentiellement un rôle de manager. Les compétences demandées à l'un ou à l'autre peuvent donc être très différentes…

Interpréter le tableau des métiers

Le tableau ci-après est organisé de la façon suivante :

- **Familles de métiers** : les différents métiers sont regroupés en familles :
  - Pilotage, organisation et gestion des risques (POG)
  - Management de projets et cycle de vie (MPC)
  - Opération et maintien en condition opérationnelle (OMCO)
  - Support et gestion des incidents (SGI)
  - Conseil, audit et expertise (CAE)
- **Colonne « métier »** : on y trouve en tête, la dénomination principale retenue par le groupe de travail. Suivent d'autres dénominations possibles, sachant que parfois, ces dénominations ne se recouvrent pas complètement (en particulier, entre certaines dénominations anglo-saxonnes et certaines dénominations françaises).
- **Colonne « dédié »** : « OUI » dans cette colonne signifie que le métier est dédié à la sécurité. « NON » signifie que la sécurité est une composante indispensable et significative au métier cité qui n'est lui-même pas dédié à la sécurité.
- **Principales fonction** : cette colonne décrit les principales activités associées au métier. Plusieurs sources sont possibles :
  - GT : groupe de travail à l'origine de cette liste
  - OPIIEC : liste de l'OPIIEC
  - NIST : NIST SP800-181
- **Études ou expérience** : indique lorsque cela à un sens le niveau d'études généralement requis (BAC+3 à BAC+5) associé éventuellement à un nombre d'années d'expérience.

PILOTAGE, ORGANISATION ET GESTION DES RISQUES (POG)				
Famille	**Métier**	**Dédié sécurité**	**Principales fonctions**	**Formation Expérience**
POG-1	**Responsable de la Sécurité des Systèmes d'Information (RSSI)** OSSI : Officier de la sécurité des systèmes d'information ISSM : *Information Systems Security Manager* CISO : *Chief Information Security Officer* CSO : *Chief Security Officer*	OUI	Ayant généralement une expérience professionnelle de plusieurs années, le RSSI définit la politique de sécurité du système d'information et veille à sa mise en application. Il joue un rôle de conseil, d'assistance, d'information, de formation et d'alerte auprès de la direction. Selon la taille de l'entité, il joue un rôle opérationnel dans la mise en œuvre de la politique de sécurité ou encadre une équipe composée d'experts techniques et de consultants. Il propose à l'autorité compétente la politique de sécurité du SI et veille à son application. Le RSSI assure un rôle de conseil, d'assistance, d'information, de formation et d'alerte. Il peut intervenir en matière de SSI sur tout ou partie des systèmes informatiques et télécoms de son entité, tant au niveau technique qu'organisationnel. Il effectue un travail de veille technologique et réglementaire sur son domaine et propose les évolutions qu'il juge nécessaires pour garantir la sécurité du système d'information dans son ensemble. Il est l'interface reconnue des exploitants et des chefs de projets, mais aussi des experts et des intervenants extérieurs pour les problématiques de sécurité de tout ou partie du SI.	5 à 10 ans d'expérience

			--- *NIST : Senior official or executive with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation (CNSSI 4009).*	
POG-2	**Correspondant sécurité** CSSI : Correspondant Sécurité du Système d'Information Gestionnaire de Risques cyber Expert connexe CRO : Correspondant risques opérationnels Assistant RSSI	NON	Assure un rôle d'intermédiaire ou de relai entre le RSSI, à qui il remonte des tableaux de bord, et les lignes métiers. Selon les organisations, il s'agit d'une fonction à temps partiel ou à temps plein. Sa forte proximité avec le métier lui permet d'intervenir sur des thématiques de gestion des risques, de gouvernance et de sensibilisation auprès des utilisateurs. En particulier, il a pour rôle d'analyser, de concevoir, d'intégrer ou de mettre en œuvre les techniques de sécurisation dans le cadre de son domaine « métier ». Maitrisant les référentiels des domaines « métier », il est en mesure de faire converger les objectifs de sécurité et de sûreté de fonctionnement. Il conduit des analyses de risques et propose des solutions résilientes, afin de minimiser sans concession les impacts « métiers ». Il peut être amené à conseiller les directions métiers, contribuer à l'expression de besoin globale et technique de sécurité en conception, en intégration et en gestion de la sécurité. À ce titre, il dispose d'une compétence et d'une expérience dans son domaine métier et d'une compétence dans le domaine de la sécurité, souvent acquise initialement à travers la formation continue (courte ou longue).	Expérience dans un ou plusieurs domaines « métier » plus formation continue en sécurité.
POG-3	**Spécialiste en gestion de crise cyber**	OUI	Le spécialiste en gestion de crise cyber conseille l'organisme pour lui permettre de disposer d'une capacité de gestion de crise majeure dédiée aux systèmes	Bac+4/5 plus expérience

	Cyber Defense Infrastructure Support Specialist		d'information, ou avec un volet cyber prépondérant. Il organise la gestion de crise pour : • agir et résoudre la crise ; • communiquer l'état de la crise aux personnes et aux organismes concernés ; • coordonner l'action des différentes parties en présence. Il limite les volets organisationnels, l'entraînement et la simulation aux acteurs susceptibles d'intervenir en cas de crise majeure liée aux systèmes d'information et à leurs interlocuteurs métiers ou support concernés à contacter (gestionnaire de crise, RSSI, responsables de l'ingénierie, administrateurs systèmes / données). À un niveau plus opérationnel et sous la pression d'une attaque en cours, le profil de gestionnaire de crise peut être également identifié dans la catégorie « maintien en condition opérationnelle ».	
POG-4	**Responsable du plan de continuité d'activité (RPCA)**	NON	Élabore et met en œuvre dans son entreprise un Plan de Continuité d'Activité (PCA)	BAC+4/5 3 ans d'expérience
MANAGEMENT DE PROJETS ET CYCLE DE VIE (MPC)				
Famille	**Métier**	**Dédié sécurité**	**Principales fonctions**	**Formation Expérience**
MPC-1	**Chef de projet sécurité**	OUI	S'assure de la bonne prise en compte des aspects sécurité liés au développement d'un projet. En général, le chef de projet sécurité assiste le chef de projet sur ces	BAC+5 3 à 5 ans

	Chef de projet sécurité informatique Chef de projet sécurité des systèmes d'information *Security Project Manager Officer (PMO)* *Program Manager* *IT program manager*		aspects. Les tâches associées à ce métier peuvent être : - analyse des besoins de la sécurité (analyse de risque, cible de sécurité), - sécurité du développement, - prise en compte des aspects liés aux évaluations/audits de la sécurité, - tests liés à la sécurité, - formation des utilisateurs, - … À ce titre, le métier peut être considéré comme spécifique à la sécurité. Tous les projets ne nécessitant pas la présence d'un chef de projet sécurité, la responsabilité de ces aspects peut être prise en charge par le chef de projet qui s'appuie ponctuellement sur des experts du domaine.	d'expérience
MPC-2	**Développeur sécurité**	OUI	Le développeur de sécurité assure le sous-ensemble des activités d'ingénierie nécessaire au développement de logiciels (spécifications, conception, codage, production de binaire, assemblage, tests, préparation à l'intégration de niveau solution, gestion des sources, gestion de configuration, gestion des faits techniques, archivage, documentation) répondant à des exigences de sécurité. En plus de sa connaissance des fondamentaux de la SSI qui lui permet de comprendre les problématiques à traiter et de ses compétences en développement, on attend du développeur sécurité des connaissances dans les domaines des vulnérabilités, des contre-mesures logicielles et/ou matérielles, des règles de développement sûr (au sens de la sécurité), des langages et de leurs propriétés, des chaînes de développement et de leur paramétrage, du test (de sécurité) et éventuellement, des méthodes formelles. Il développe de façon méthodique, en appliquant des règles de conception / codage	BAC+5

			/ tests (qu'il définit au besoin ou qu'il contribue à définir) et s'assure que les composants qu'il produit sont testables en termes de conformité fonctionnelle, de robustesse (tests aux limites et hors limites), de sécurité (résistance aux attaques identifiées en entrée de la conception), et de performances. Ses compétences lui permettent également de faire des revues, audits ou évaluations de code (*Secure Software Assessor, Source Code Auditor*). **Note** : toute personne faisant du développement devrait avoir été initiée à la prise en compte des bonnes pratiques et des méthodes pour limiter l'introduction de vulnérabilités de construction. Cette initiation est typiquement ce que propose une formation labellisée CyberEdu. Le métier décrit ici correspond à une spécialité (d'où son classement en « dédié ») qui va au-delà de ce que l'on attend d'un développeur formé.	
MPC-3	**Architecte sécurité** Architecte Sécurité Informatique Architecte Réseaux et Télécom *System architect* *Information Security Architect* *Security architect*	OUI	L'architecte de sécurité structure les choix techniques, technologiques et méthodologiques d'un ensemble [système, logiciel] répondant à des exigences de sécurité. Il s'assure de la déclinaison des exigences techniques (fonctionnalités à offrir, contraintes de performance, d'interopérabilité, d'interchangeabilité, de robustesse, d'intégration de solutions sur étagère, d'exportabilité), selon des critères de coût, d'efficacité, de stabilité, de maîtrise, de niveau de risque, de respect des standards, d'aptitude à la production, au déploiement et à la maintenance MCO (Maintien en Conditions Opérationnelles) et MCS (Maintien en Conditions de Sécurité). Il valide la cartographie du système d'information et notamment s'assure que les hypothèses de sécurité relatives à l'environnement de son architecture sont clairement énoncées et prises en compte dans sa conception.	BAC+3 à BAC+5 5 à 10 ans d'expérience

			Il veille à ce que les exigences de sécurisation applicables aux différents constituants de son architecture ou aux outils permettant de la produire soient effectivement mises en œuvre. Il prépare les dossiers de conception et de justification sur les aspects sécurité. Il participe à la conception de l'architecture et de l'implémentation du produit ou système à développer en s'assurant que les différentes briques disposent du niveau de sécurité adapté aux contextes du projet sur les aspects techniques, usages, métiers… --- *NIST : Designs enterprise and systems security throughout the development life cycle; translates technology and environmental conditions (e.g., law and regulation) into security designs and processes.*	
MPC-4	**Intégrateur de sécurité**	OUI	De niveau licence à master, l'intégrateur de sécurité système analyse et prend en charge les volets sécurité (objectifs, niveau de criticité et attentes en termes de résilience) en liaison avec l'architecte des projets informatiques et programmes dans l'infrastructure. Il définit et met en œuvre des plates-formes nécessaires à l'intégration des solutions (services ou produits de sécurité) dans les nouvelles applications. Il planifie, coordonne, en relation avec les autres secteurs concernés (systèmes, réseaux, système de gestion base de données, etc.), les besoins d'intégration exprimés. Il installe des composants matériels, des composants logiciels ou des sous-systèmes supplémentaires dans un système existant ou en cours de développement, respecte	BAC+3 à BAC+5

			les processus et procédures établis (i.e. gestion de configuration), en tenant compte de la spécification, de la capacité et de la compatibilité des modules existants et des nouveaux modules afin de garantir intégrité et interopérabilité. Il contribue à la qualification technique et à l'intégration dans l'environnement de production. Il documente les processus de mise en œuvre, de mise à jour et d'exploitation des composants de sécurité et organise les conditions de mise en œuvre du maintien en condition de sécurité.	
OPERATION ET MAINTIEN EN CONDITION OPERATIONNELLE (OMCO)				
Famille	**Métier**	**Dédié sécurité**	**Principales fonctions**	**Formation Expérience**
OMCO-1	**Administrateur sécurité** Administrateur Sécurité Informatique Opérateur en sécurité des systèmes d'information *System Administrator* *Cyber Defense Infrastructure Support Specialist*	NON	Met en œuvre la politique de sécurité de l'entreprise et administre des solutions de sécurité de type antivirus, antispam, IPS, la gestion des habilitations (départ, arrivée, mobilité) et les dérogations. En général, la fonction d'administration de la sécurité est une des fonctions de l'administrateur système/réseaux (d'où son placement en métier non dédié à la sécurité). Mais certaines organisations peuvent dédier des personnes à ce seul métier. Elles agissent en complément des administrateurs réseaux et systèmes. --- *NIST : Responsible for the analysis and development of the integration, testing, operations, and maintenance of systems security.*	BAC+3

			Installs, configures, troubleshoots, and maintains hardware and software, and administers system accounts. *Tests, implements, deploys, maintains, and administers the infrastructure hardware and software.*	
OMCO-2	**Technicien sécurité** Technicien support SSI Télé-assistant *Technical Support Specialist*	NON	Le technicien support est responsable d'activités de support, de gestion ou d'administration de la sécurité aux plans techniques ou administratifs : conception, production, conditionnement et gestion des réseaux de chiffrement et des éléments secrets. Selon le profil d'emploi et la formation reçue, il est en mesure de déployer et d'administrer des solutions de gestion de la sécurité, ainsi que de paramétrer les éléments de sécurité des équipements serveurs et des terminaux traitants. Il est en capacité d'effectuer des tâches de contrôles administratifs de conformité dans le domaine des habilitations du personnel, du suivi comptable et des inventaires réglementaires, de l'application des procédures d'exploitation de sécurité, apportant ainsi son soutien aux opérations d'audit et de contrôle. Il contribue aux séances de sensibilisation pour l'usage des ressources par les utilisateurs finaux.	Bac+2/3
SUPPORT ET GESTION DES INCIDENTS (SGI)				
Famille	**Métier**	**Dédié sécurité**	**Principales fonctions**	**Formation Expérience**

SGI-1	**Analyste SOC** Analyste Cyber SOC Analyste détection d'incident Veilleur-Analyste *Cyber Defense Analyst*	OUI	Paramètre les systèmes de supervision de la sécurité (SIEM, sondes, *honeypots*, équipements filtrants). Catégorise, analyse et traite les alertes de sécurité de façon régulière pour en améliorer l'efficacité. Assure la détection, l'investigation et la réponse aux incidents de sécurité. Dans le domaine de la cybersécurité, l'analyste SOC analyse et interprète les alertes, les événements corrélés et recherche les vulnérabilités. --- *Uses data collected from a variety of cyber defense tools (e.g., IDS alerts, firewalls, network traffic logs) to analyze events that occur within their environments for the purposes of mitigating threats.* *Develops unique cyber indicators to maintain constant awareness of the status of the highly dynamic operating environment. Collects, processes, analyzes, and disseminates cyber warning assessments.* *Collaborates to identify access and collection gaps that can be satisfied through cyber collection and/or preparation activities. Leverages all authorized resources and analytic techniques to penetrate targeted networks.*	BAC+3
SGI-2	**Expert réponse à incident** Spécialiste en investigation numérique Analyste traitement d'incident *Cyber Crime Investigator*	OUI	Analyse et traite les incidents de sécurité au sein d'une structure ou d'une équipe de réponse à incident. Communique et fournis des recommandations de sécurité aux services clients de la cellule de réponse à incident. L'expert en réponse à incident travaille sous forte contrainte pour reprendre la main lors d'attaques/compromissions de systèmes d'information. Disposant de la cartographie du système d'information, il doit interagir avec de nombreuses personnes dont les experts en investigation numérique afin d'appréhender	BAC+3 à BAC+5

	Forensics Analyst *Cyber Defense Forensics Analyst*		rapidement le contexte et les architectes qui maîtrisent le système d'information. Il formule des recommandations de mesures de contournement et de mesures d'urgence et d'amélioration des capacités de détection (journalisation notamment). --- *NIST : Identifies, collects, examines, and preserves evidence using controlled and documented analytical and investigative techniques (Cyber Crime Investigator)* *NIST : Conducts deep-dive investigations on computer-based crimes establishing documentary or physical evidence, to include digital media and logs associated with cyber intrusion incidents.* *NIST : Analyzes digital evidence and investigates computer security incidents to derive useful information in support of system/network vulnerability mitigation.*	
CONSEIL, AUDIT, EXPERTISE (CAE)				
Famille	**Métier**	**Dédié sécurité**	**Principales fonctions**	**Formation Expérience**
CAE-1	**Consultant sécurité « organisationnel »** Consultant sécurité Consultant gouvernance, risques et conformité.	OUI	« Consultant » est un terme générique souvent utilisé par les sociétés de services pour désigner toute personne en mesure de prodiguer des conseils à un client. Dans le domaine de la sécurité, on peut distinguer les consultants intervenant plutôt sur les aspects organisationnels ou non techniques de la sécurité de ceux qui interviennent dans les domaines techniques.	BAC+4/5 Qualification ANSSI possible : PASSI

	Consultant en SSI Auditeur organisationnel *Lead auditor,* *Lead implementer,* *Systems auditor* *Information security auditor*		Typiquement, le consultant organisationnel effectuera des prestations dans tout ou partie des domaines suivants : - travaux méthodologiques ; - analyses de risques ; - activités d'analyse de risques, d'audit, de gestion de projet sécurité ; - définition et mise en place de politiques de sécurité ou de systèmes de management de la sécurité ; - entraînement au management de la sécurité ; - etc. Ses compétences peuvent l'amener à réaliser des prestations d'audit dans tout ou partie des domaines précédemment cités. --- *NIST : Conducts evaluations of an IT program or its individual components, to determine compliance with published standards.*	
CAE-2	**Consultant sécurité « technique »** Auditeur technique sécurité et test d'intrusion Pen testeur Expert audit sécurité et intrusion Spécialiste cybersécurité Expert technique	OUI	« Consultant » est un terme générique souvent utilisé par les sociétés de services pour désigner toute personne en mesure de prodiguer des conseils à un client. Dans le domaine de la sécurité, on peut distinguer les consultants intervenant plutôt sur les aspects organisationnels ou non techniques de la sécurité de ceux qui interviennent dans les domaines techniques. Selon son domaine d'expertise, le consultant technique effectuera des prestations dans les domaines suivants : - les travaux en lien avec les applications et les services sécurisés (mise en œuvre et configuration, analyse de la sécurité…) ; - les travaux en lien avec les systèmes d'exploitation (mise en œuvre et	BAC+4/5 Qualification ANSSI possible : PASSI

	Consultant sécurité *Security Control Assessor* *Vulnerability Assessment Analyst* *Ethical Hacker* *Penetration tester* *Vulnerability assessor*		configuration, audit de configuration, test de pénétration…) ; - les travaux en lien avec les réseaux (mise en œuvre et configurations d'équipements sécurité, test de pénétration…) ; - les travaux en liens avec du matériel (mesures de signaux compromettants, analyse logique, conception de produits matériels sécurisés…) : - la rétro ingénierie (logicielle ou matérielle) ; - la cryptographie (implémentation sûres… Pour ce thème voir « Cryptologue ») ; - l'analyse post-mortem (investigation numérique, forensique) ; - et de manière générale, les activités à caractère technique ou scientifique. Ses compétences peuvent l'amener à réaliser des prestations d'audit dans tout ou partie des domaines précédemment cités.	
CAE-3	**Cryptologue** Expert crypto *Cryptographer* *Cryptanalyst*	OUI	Il apporte son expertise dans tout ou partie des domaines suivants (selon la finalité de l'organisation dans laquelle il travaille ou le projet pour lequel il intervient) : - utilisation d'algorithmes cryptographiques, - utilisation / conception de protocoles cryptographique, - gestion des clés, - implémentation sécurisée d'algorithmes cryptographiques, - utilisation de bibliothèques cryptographiques, - évaluation de l'utilisation et de l'implémentation d'algorithmes cryptographiques, - analyse cryptographique, - … Exceptionnellement, il peut être amené à concevoir des algorithmes cryptographiques.	BAC+5 à doctorat

CAE-4	**Juriste spécialisé en cybersécurité** Consultant juridique en cyberdéfense *Cyber Legal Advisor*	NON	Le juriste spécialisé en cybersécurité est un expert du droit des technologies de l'information et de la communication qui est spécialiste des thèmes et des corpus concernés par la cybersécurité, la cybercriminalité et la protection des données à caractère personnel. Il peut opportunément présenter une expérience d'avocat à même d'éclairer la direction sur les conséquences pénales ou civiles d'une cyberattaque, dès lors qu'une décision voire la gestion d'une crise avec une composante « cybersécurité» requiert son expertise. Conseil de la direction en matière de responsabilités civile et pénale, il se tient informé des évolutions de la réglementation internationale, européenne et nationale. Il effectue une veille juridique depuis le simple projet jusqu'à la publication et l'entrée en vigueur des textes régissant les conflits armés, le droit des affaires (notamment le secret des affaires), ainsi que la jurisprudence, en différenciant selon que la décision est un cas d'espèce ou au contraire amène des réflexions plus générales sur la pratique du droit. --- *NIST : Provides legally sound advice and recommendations to leadership and staff on a variety of relevant topics within the pertinent subject domain. Advocates legal and policy changes, and makes a case on behalf of client via a wide range of written and oral work products, including legal briefs and proceedings.*	BAC+5/6
CAE-5	**Évaluateur sécurité** Responsable évaluation	OUI	ANSSI : Le métier concerne les laboratoires qui réalisent les évaluations de la sécurité et les développeurs de produits devant être évalués : **Coté évaluateur :**	BAC+5

	Responsable certification *System Testing and Evaluation Specialist*		l'évaluateur sécurité vérifie la conformité d'un produit, voire, d'un système, par rapport à sa spécification de sécurité (Cible de sécurité…) selon des critères et une méthode normalisé ou réglementaire (CC, CSPN…) ou privé (PCI, EMVCo…). Le résultat de cette évaluation peut donner lieu à une certification (ou assimilée). **Coté développeur** Les mêmes compétences peuvent être utilisées chez les développeurs de produits ou de systèmes qui doivent subir une évaluation sécurité. En termes de titre, on parlera plutôt de « responsable évaluation » ou de « responsable certification ». Son rôle est de gérer la relation avec les laboratoires qui réalisent les évaluations, de s'assurer que toutes les fournitures attendues sont disponibles, etc. --- *NIST : Plans, prepares, and executes tests of systems to evaluate results against specifications and requirements as well as analyze/report test results.*	
CAE-6	**Analyste de la menace** *Threat Intelligence*	OUI	De niveau licence à master, l'analyste peut contribuer à plusieurs domaines d'activités de la cybersécurité, dans les domaines de : - l'anticipation technologique avec de la veille technique ; - l'anticipation dans le domaine du renseignement sur les menaces, avec de l'analyse d'impact des codes d'exploitation (activités CERT et intégrateur de solutions) ; - l'anticipation en conduite pour évaluer les dommages subis par un système compromis, participer à la conception de la solution technique visant à restituer le service et apporter ses compétences de spécialiste en matière de mise en œuvre des principes de sécurisation SSI et dans le domaine	BAC+3/5

			technique de la cyber sécurité. Il peut contribuer au schéma directeur et à l'urbanisation sécurisée des systèmes.	
CAE-6	**Délégué à la Protection des Données (DPD)** Correspondant informatique et libertés (CIL) Data protection officer (DPO) Privacy Compliance Manager Privacy officer Data protection officer	NON	S'assure que les données personnelles sont traitées par l'entreprise conformément aux règles internes et aux lois en vigueur. --- *NIST : Develops and oversees privacy compliance program and privacy program staff, supporting privacy compliance needs of privacy and security executives and their teams.*	BAC+5 10 ans d'expérience