CYBERSÉCURITÉ : QUELLES COMPÉTENCES POUR RÉPONDRE AUX ENJEUX DE LA TRANSFORMATION NUMÉRIQUE ?

__L'association Talents du Numérique,__ qui associe établissements d'enseignement supérieur et entreprises du Numérique, a réalisé un travail important sur le développement des compétences des professionnels niveau Bac+5 du secteur du Numérique.
__La commission e-compétences__ de Talents du Numérique a pour objectif de préparer l'avenir des entreprises et des établissements de formation afin que le secteur soit en mesure de réagir à l'évolution des compétences recherchées, alors que de nouvelles technologies arrivent et se déploient. Dans le cadre de cette note, nous tenons tout particulièrement à remercier l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) d'avoir participé à nos échanges et alimenté le débat.

ÉLÉMENTS DE CONTEXTE[1]

La révolution numérique que nous vivons dépasse largement le cadre purement technologique. Elle bouscule les équilibres économiques et transforme les usages à une vitesse jamais atteinte jusque-là. Elle touche tout autant les clients des entreprises numériques dans leurs activités, leurs chaînes de valeur et leurs organisations, que les individus dans leur vie quotidienne et la société en général, dans ses règles et ses équilibres. Il s'ensuit pour les utilisateurs - individuels ou collectifs, publics ou privés – des risques potentiels engendrés par l'exploitation extensive des données et par la virtualisation des échanges et des processus qui renforcent le besoin de cybersécurité.

En tant qu'opérateurs de transformations numériques, les professionnels du numérique sont confrontés à de nouvelles responsabilités et exigences, face aux risques digitaux (cyberattaques, dévoiement de l'usage des données, etc.).

- Ils sont tenus de garantir la conformité au cadre législatif et réglementaire des systèmes et outils qu'ils conçoivent et utilisent
- Ils doivent s'assurer que ces mêmes dispositifs se déploient dans des environnements de confiance, avec des partenaires et des systèmes respectueux d'un cadre éthique et de sécurité
- Ils doivent tenir les objectifs de la cybersécurité qui sont la confidentialité, l'intégrité, la disponibilité, la traçabilité, la non-répudiation et la conformité.

De nombreux exemples de fuite de données ces dernières années ont montré les limites de la sécurité informatique : Affaires Snowden et Wikileaks, piratages de l'Élysée en 2012 et de Yahoo en 2014 (…). Rappelons que 21 incidents de sécurité sont identifiés chaque jour en France et que 75% des failles sont d'origine humaine. Le cabinet PwC, dans son étude mondiale 2017, estimait les pertes financières subies par les entreprises françaises en raison de problèmes de cybersécurité à 2,25 millions d'euros en moyenne, un chiffre en hausse de 50% par rapport à l'année précédente. La nécessité de poursuivre la recherche en ce domaine, la diffusion des différentes technologies disponibles, l'évangélisation et la formation des usagers et des citoyens sont primordiales. C'est un enjeu clé pour l'ensemble des entreprises : aucun secteur d'activité ne sera épargné.

[1] https://syntec-numerique.fr/system/files/Documents/Livre-Blanc-Guide-pratique-pour-reussir-sa-transformation-par-linnovation.pdf

C'est aussi un enjeu clé en matière de compétences pour l'ensemble des professionnels. La cybersécurité concerne tout le monde, et l'ensemble de la population devrait maîtriser les fondamentaux dans ce domaine. Les attaques informatiques peuvent par ailleurs paralyser des usines ou des entreprises, parfois dans des secteurs critiques comme l'énergie, la santé : wannacry, mirai, etc.
Au-delà, les besoins de notre économie en professionnels de la cybersécurité sont immenses. La cybersécurité fait partie intégrante de l'ensemble des domaines informatiques et des projets numériques. Le recrutement est perçu comme une difficulté majeure par les entreprises de ce secteur qui devrait générer en France en 2018, selon les prévisions, un CA de 2,5 Mds €, en croissance de 17%. Dans une étude réalisée par l'OPIIEC en 2017, la cybersécurité représentait 24 000 emplois de la branche des métiers de l'ingénierie, du numérique, des études, du conseil et des métiers de l'événement. Les entreprises de la branche anticipaient une croissance des effectifs en cybersécurité de 6%, soit 1400 créations nettes d'emplois.[2]

UN SUJET TRANSVERSAL, À CONCEVOIR COMME UN ENSEMBLE

La cybersécurité est un sujet transversal qui doit être partie intégrante de tout projet numérique et donc de toute démarche de transformation numérique, dès sa conception. La cybersécurité est, de plus, un processus qui intervient tout au long du cycle de vie d'un produit ou d'un service pour identifier les risques techniques et organisationnels, définir les techniques et processus de protection, mettre en place des mesures de détection et de réponse aux cyber-attaques, et revenir à un mode de fonctionnement normal.

La sécurité d'un service numérique se conçoit comme une chaîne qui doit couvrir le service de bout en bout, en considérant toutes ses composantes - le réseau, les contrôles d'accès, les applicatifs, etc. - et prévoir la gouvernance de l'ensemble.
À chaque niveau, des normes existent permettant de cadrer la mise en œuvre de la démarche de cybersécurité.

Au-delà, les thématiques usuelles de la cybersécurité sont :

- Sécurité, contrôle d'accès et sécurité du développement logiciel
- Planification et cryptographie de la continuité des activités et reprise après sinistre
- Gouvernance de la sécurité de l'information, gestion des risques et juridiques, règlements, enquêtes et conformité
- Sécurité des opérations, sécurité physique et environnementale
- Architecture et design de sécurité, télécommunications et sécurité des réseaux

À noter : la cybersécurité ne doit pas rester l'apanage de quelques experts. Développer une culture de la sécurité numérique est essentiel afin de se protéger de catastrophes économiques et industrielles.
L'effort pédagogique à réaliser doit être impulsé par les directions générales afin d'être concluant et opérant.

[2] Étude OPIIEC *Les formations et les compétences en France sur la cybersécurité*, 21-05-2017 – Synthèse : https://bit.ly/2nEl1Ta et Rapport complet : https://bit.ly/2u5Hsmm

CYBERSÉCURITE, MÉTIERS ET COMPÉTENCES[3]

Nous reprendrons ici les travaux réalisés par l'ANSSI et le monde industriel, notamment Syntec Numérique, réalisés entre 2015 et 2017, et encore largement opérants.

I. Pilotage, organisation et gestion des risques (POG)

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

Expérience : 5 à 10 ans

Ayant généralement une expérience professionnelle de plusieurs années, le/la RSSI définit la politique de sécurité du système d'information et veille à sa mise en application. Il/elle 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/elle 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/elle propose à l'autorité compétente la politique de sécurité du SI et veille à son application. Il/elle 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/elle effectue un travail de veille technologique et réglementaire sur son domaine et propose les évolutions qu'il/elle juge nécessaires pour garantir la sécurité du système d'information dans son ensemble. Il/elle est l'interface reconnue des exploitants et des chefs de projets, mais aussi des experts et des intervenants.

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

☐ Correspondant.e sécurité

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

Il/elle assure un rôle d'intermédiaire ou de relais entre le RSSI, à qui il/elle 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/elle 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/elle est en mesure de faire converger les objectifs de sécurité et de sûreté de fonctionnement. Il/elle conduit des analyses de risques et propose des solutions résilientes afin de minimiser sans concession les impacts « métiers ». Il/elle peut être amené.e à conseiller les directions métiers, contribuer à l'expression de besoins, globale et technique, de sécurité en conception, en intégration et en gestion de la sécurité. À ce titre, il/elle dispose d'une compétence et d'une expérience dans son domaine métier et d'une compétence dans le domaine de la sécurité, souvent acquise à travers la formation continue (courte ou longue).

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

[3] https://www.ssi.gouv.fr/particulier/formations/profils-metiers-de-la-cybersecurite/

☐ Spécialiste en gestion de crise cyber

Expérience / niveau de diplôme : Bac+5

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

***Métiers associés** : Cyber Defense Infrastructure Support Specialist*

☐ Responsable du plan de continuité d'activité (RPCA)

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

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

II. Management de projets et cycle de vie (MPC)

☐ Chef.fe de projet sécurité

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

S'assure de la bonne prise en compte des aspects sécurité liés au développement d'un projet. En général, le/la chef.fe de projet sécurité assiste le/la chef.fe de projet sur ces aspects.

Les tâches associées à ce métier peuvent être :

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

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

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

☐ Développeur/Développeuse sécurité

Expérience / niveau de diplôme : Bac+5

Le développeur ou la développeuse 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, 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/de la développeuse 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/elle développe de façon méthodique, en appliquant des règles de conception / codage / tests (qu'il définit au besoin ou qu'il contribue à définir) et s'assure que les composants qu'il produit sont testables en termes de conformité fonctionnelle, de robustesse (tests aux limites et hors limites), de sécurité (résistance aux attaques identifiées en entrée de la conception) et de performance. Ses compétences lui permettent également de faire des revues, audits ou évaluations de code (Secure Software Assessor, Source Code Auditor).

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

☐ Architecte sécurité

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

L'architecte de sécurité structure les choix techniques, technologiques et méthodologiques d'un ensemble [système, logiciel] répondant à des exigences de sécurité. Il/elle s'assure de la déclinaison des exigences techniques (fonctionnalités à offrir, contraintes de performance, d'interopérabilité, d'interchangeabilité, de robustesse, d'intégration de solutions sur étagère, d'exportabilité) selon des critères de coût, d'efficacité, de stabilité, de maîtrise, de niveau de risque, de respect des standards, d'aptitude à la production, au déploiement et à la maintenance MCO (Maintien en Condition Opérationnelle) et MCS (Maintien en Condition de Sécurité). Il/elle valide la cartographie du système d'information et s'assure notamment que les hypothèses de sécurité relatives à l'environnement de son architecture sont clairement énoncées et prises en compte dans sa conception. Il/elle 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/elle prépare les dossiers de conception et de justification sur les aspects sécurité. Il/elle participe à la conception de l'architecture et de l'implémentation du produit ou système à développer en s'assurant que les différentes briques disposent du niveau de sécurité adapté aux contextes du projet sur les aspects techniques, usages, métiers…

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

☐ Intégrateur/Intégratrice de sécurité

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

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

III. Opération et maintien en condition opérationnelle (OMCO)

☐ Administrateur / Administratrice sécurité

Expérience / niveau de diplôme : Bac+3

Met en œuvre la politique de sécurité de l'entreprise et administre des solutions de sécurité de type antivirus, antispam, IPS, la gestion des habilitations (départ, arrivée, mobilité) et les dérogations. En général, la fonction d'administration de la sécurité est une des fonctions de l'administrateur ou administratrice système/réseaux. Mais certaines organisations peuvent dédier des personnes à ce seul métier. Ces personnes agissent alors en complément des administrateurs/trices réseaux et systèmes.

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

☐ Technicien.ne sécurité

Expérience / niveau de diplôme : Bac+2/3

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

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

IV. Support et gestion des incidents (SGI)

☐ Analyste SOC

Expérience / niveau de diplôme : Bac+3

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

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

☐ Expert.e réponse à incident

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

Analyse et traite les incidents de sécurité au sein d'une structure ou d'une équipe de réponse à incident. Communique et fournit des recommandations de sécurité aux services clients de la cellule de réponse à incident. L'expert.e 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/elle doit interagir avec les experts en investigation numérique afin d'appréhender rapidement le contexte, et les architectes qui maîtrisent le système d'information. Il/elle formule des recommandations de mesures de contournement et de mesures d'urgence et d'amélioration des capacités de détection (journalisation notamment).
Métiers associés : *Spécialiste en investigation numérique - Analyste traitement d'incident - Cyber Crime Investigator - Forensics Analyst - Cyber Defense Forensics Analyst*

V. Conseil, Audit et Expertise (CAE)

☐ Consultant.e sécurité « organisationnel »

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

« Consultant.e » 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 consultant.e.s intervenant plutôt sur les aspects organisationnels ou non techniques de la sécurité de ceux/celles qui interviennent dans les domaines techniques.
Typiquement, le/la consultant.e organisationnel.le 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

Ses compétences peuvent l'amener à réaliser des prestations d'audit dans tout ou partie des domaines précédemment cités.
Métiers associés : *Consultant.e sécurité – Consultant.e gouvernance, risques et conformité – Consultant.e en SSI – Auditeur organisationnel – Lead auditor – Lead implementer – Systems auditor -Information security auditor*

☐ Consultant.e sécurité « technique »

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

« Consultant.e » 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/la consultant.e technique effectuera des prestations dans les domaines suivants :

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

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

☐ Cryptologue

Expérience / niveau de diplôme : Bac+5 à doctorat

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

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

Exceptionnellement, il/elle peut être amené à concevoir des algorithmes cryptographiques.
Métiers associés : *Expert.e crypto – Cryptographer – Cryptanalyst*

☐ Juriste spécialisé en cybersécurité

Expérience / niveau de diplôme : Bac+5/6

Le/la juriste spécialisé.e en cybersécurité est un.e expert.e du droit des technologies de l'information et de la communication qui est spécialiste des thèmes et des corpus concernés par la cybersécurité, la cybercriminalité et la protection des données à caractère personnel.

Il/elle peut 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/elle se tient informé des évolutions de la réglementation internationale, européenne et nationale. Il/elle 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 les décisions qui sont des cas d'espèce de celles qui, au contraire, amènent à des réflexions plus générales sur la pratique du droit.

Métiers associés : *Consultant.e juridique en cyberdéfense – Cyber Legal Advisor*

☐ Évaluateur / Évaluatrice sécurité

Expérience / niveau de diplôme : Bac+5

Le métier concerne les laboratoires qui réalisent les évaluations de sécurité des technologies de l'information et les développeurs/développeuses de produits devant être évalué.e.s :

- Côté évaluateur/évaluatrice : L'évaluateur/l'évaluatrice sécurité vérifie la conformité d'un produit, voire d'un système, par rapport à sa spécification de sécurité (cible de sécurité…) selon des critères et une méthode normalisée ou réglementaire (CC, CSPN…) ou privée (PCI, EMVCo…). Le résultat de cette évaluation peut donner lieu à une certification (ou assimilée).
- Côté développeur/développeuse : Les mêmes compétences peuvent être utilisées chez les développeurs/développeuses de produits ou de systèmes qui doivent subir une évaluation sécurité. En termes de titre, on parlera plutôt de « responsable évaluation » ou de « responsable certification ». Son rôle est de gérer la relation avec les laboratoires qui réalisent les évaluations, de s'assurer que toutes les fournitures attendues sont disponibles etc.

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

☐ Analyste de la menace

Expérience / niveau de diplôme : Bac+3/5

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

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

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

Métiers associés *: Threat Intelligence*

- ☐ **Délégué.e à la Protection des Données (DPD)**
  Expérience / niveau de diplôme : Bac+5 – 10 ans d'expérience

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

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

CONNAISSANCES REQUISES

La cybersécurité nécessite des compétences dans tous les domaines scientifiques, techniques, organisationnels et juridiques concernés par les systèmes d'information et de communication ce qui rend le sujet particulièrement excitant mais en contrepartie, particulièrement complexe à appréhender. Elle aborde ces domaines sous un angle particulier visant à en rechercher des faiblesses pour en rechercher les vulnérabilités et les corriger, le tout, dans un environnement socioéconomique et légal contraint.

Le programme de labellisation SecNum*edu de l'ANSSI* liste un certain nombre de thèmes qui devraient au moins être abordés dans toutes formations dédiées à la sécurité.
On ne citera que quelques exemples ci-après :

☐ Programmation et cryptographie

- Mathématiques discrètes (éléments d'arithmétique, probabilités, algèbre…)
- Développement logiciel et ingénierie logicielle
- Service de sécurité et mécanisme de cryptographie
- Méthodes, pratiques et Hacking
- Programmation (Par exemple : Java et Javacard)
- PKI, stéganographie et tatouage

☐ Infrastructure et réseaux

- Infrastructure internet ;
- Principes, méthodes architecture et protocole, contrôle d'accès et gestion des identités
- Application réseaux et transport de données
- Infrastructure de confiance et mise en œuvre
- Communication sans fil et réseaux autonomes
- Analyse post-mortem, forensique des systèmes et des réseaux

☐ Gestion et sécurité

- Sécurité des réseaux, des infrastructures, des systèmes informatiques :
  - Sécurité des adresses IP (Metasploit, Kali Linux…)
- Sécurité des systèmes spécifiques et émergents
- Sécurité des développements, des applis web
- Sécurité des bases de données
- Gestion et organisation de la sécurité d'un système d'information : SOC (Security Operation Center), monitoring et pilotage du risque
- Sécurité des systèmes embarqués ; Audit de sécurité et de vulnérabilité
- Sécurité physique
- Sécurité des services externalisés
- Sécurité des cartes à puce (Smart cards) et moyens de paiement
- Test d'intrusion
- (…)

À cela, il convient d'ajouter :

- ☐ **La physique**
  Tous les produits que nous utilisons s'appuient sur des phénomènes physiques (électricité, électromagnétisme…) qui peuvent être mis à profit par les attaquants
- ☐ **Les sciences humaines et sociales**
  Beaucoup d'attaques commencent par cibler les personnes…
- ☐ **Les normes organisationnelles**
  … qui varient en fonction des métiers
- ☐ **L'encadrement légal et juridique**
  des activités liées à la cybersécurité
- ☐ **Les méthodes d'analyse de risques**
- ☐ **Les techniques d'audits**
  (organisationnelles, techniques)
- ☐ **La rétro ingénierie**
- ☐ **Les techniques d'évaluation de la sécurité des produits**
- ☐ **Les aspects économiques de la sécurité**
- ☐ **(…)**

Ainsi le domaine de la cybersécurité n'apparaît pas nouveau. **Il bénéficie néanmoins de récentes innovations impactantes, qu'il convient de connaître, voire de maîtriser.**
Citons notamment :

- Solutions de gestion des identités et des accès (Iam), de gouvernance des accès aux données non structurées (dag) et de gestion des comptes à privilèges (Pam)
- Nouveaux paradigmes développés autour de l'adoption croissante du cloud computing : Casb (Cloud access security brokers)
- Solutions de type SIEM (Security information and event management)
- Normes certifiantes imposées par les États et organisations internationales : directives européennes, ...
- Perfectionnement des solutions de protection périmétrique et instauration de dispositifs de type SoC (Security operations Center)
- Solutions d'analyse d'impact du déploiement de solutions de cloud computing, notamment publiques, en termes de risque d'accès à des actifs immatériels de grande valeur.
- (…)

Les membres de la Commission e-Compétences de Talents du Numérique insistent sur six aspects fondamentaux :

- Savoir mettre en place une veille permanente, à dimension internationale. Être curieux
- Disposer de solides connaissances juridiques (au-delà du simple RGPD : Loi de programmation militaire, technologie duale…). Les professionnels ont pu constater le niveau lacunaire de nombre d'étudiants en ce domaine. Connaître la gouvernance, les normes et les standards dans le domaine de la sécurité
- Acquérir une solide culture générale en matière de géopolitique et d'intelligence économique
- Acquérir des connaissances et savoir analyser les cyberattaquants, leurs méthodes et motivations, afin de générer des défenses adaptées
- Ne pas sous-estimer la dimension (inter)culturelle de la cybersécurité. La pratique courante de l'anglais est une nécessité
- Développer la capacité d'analyse, d'anticipation et de mise en situation.

Enfin, la Commission estime que l'offre de formation actuelle pourrait heureusement être complétée par des formations plus centrées sur les aspects liés au management de la sécurité.

CYBERSÉCURITÉ ET CONDUITE DE PROJETS

La gestion de la composante « Cybersécurité » des projets numériques sont l'affaire de personnes et profils très divers (scientifiques et techniques, experts en sciences humaines, méthode, policy, certification et normes, juriste (…). Il est ainsi particulièrement difficile d'identifier et de recruter la ou les personnes disposant des qualités scientifiques, mais aussi humaines, pour mener ces projets exigeants. Aussi, leur réussite dépendra-t-elle de la capacité à réunir une équipe associant toutes les compétences du numérique attendues.
Il convient ainsi de mobiliser certes des professionnels niveau Bac+5 de spécialité, mais également des généralistes, à même d'avoir une vision globale, d'embrasser toute la chaîne de valeur, les dimensions métiers et l'ensemble de l'architecture.

La **démarche globale** passe par :

- la sensibilisation et la formation des collaborateurs
- la mise en place de dispositifs de protection passive : filtres d'écrans, caches prises usB, ...
- la mise en place de dispositifs de protection active : chiffrement des données sur les équipements des collaborateurs
- (…)

Au niveau de **la gouvernance,** il convient de :

- Définir et exécuter la démarche globale de sécurité du SI
- Systématiser les analyses de risques pour définir les besoins
- Impliquer le management
- Décliner la démarche et responsabiliser les parties prenantes
- Communiquer
- Assurer la couverture de bout en bout (OT et IT)

Au niveau **du réseau,** il convient de :

- Sécuriser les réseaux dès leur conception
- Optimiser et rationaliser les mesures existantes
- Mesurer le niveau effectif de vulnérabilité et de protection
- Déployer les architectures sécurisées
- Accompagner les équipes d'administration technique

Au niveau **des applicatifs,** il convient de :

- Comprendre l'exposition aux risques
- Vérifier la réalité de l'application de la sécurité et l'efficacité de la gestion des vulnérabilités (tests d'intrusion …)
- Éduquer les équipes de développement à prendre en compte la sécurité
- Comprendre les événements de sécurité (analyse de logs & SIEM)
- Garantir l'intégrité et l'origine d'un document ou d'un flux de données

Enfin, la conduite ou la participation à ce type de projet nécessite, comme pour l'ensemble des projets de transformation numérique, des qualités humaines importantes, des **softskills** que les établissements de formation doivent contribuer à développer chez leurs étudiants.
Les membres de la Commission insistent notamment sur la nécessité de développer les capacités **d'analyse critique**, **d'adaptabilité** et de **réactivité.**

CONCLUSION - RECOMMANDATIONS

Les besoins en compétences dans le domaine de la cybersécurité sont très importants, chiffrés à **plusieurs dizaines de milliers d'emplois en France d'ici 2022.** Les établissements de formation se sont mobilisés pour y répondre et ont ouvert des cursus, en formation initiale ou continue, qui devraient permettre de satisfaire la demande. Deux difficultés sont cependant relevées : l'**attractivité** de ces formations et le **manque d'enseignants.**

Nos membres se félicitent de la mobilisation des pouvoirs publics et de l'ANSSI en particulier pour structurer l'offre de formation, développer l'appétence pour cette thématique des futurs professionnels du numérique, des professionnels de notre économie et de l'ensemble de nos concitoyens. La sécurité (et la cybersécurité en particulier) est l'affaire de tous. Ils se réjouissent également de **l'agilité des établissements de formation** et du dynamisme de l'écosystème : de **nombreux cursus dédiés** ont été ouverts.
En termes de formation, les établissements et entreprises réunies au sein de Talents du Numérique insistent sur la nécessité de développer une **approche globale et systémique**. La cybersécurité est un sujet transversal qui doit être partie intégrante de tout projet numérique et donc de toute démarche de transformation numérique. Ainsi, une formation en cybersécurité doit couvrir l'ensemble de la chaîne, de la conception à la production.

Notre commission recommande :

- ⇨ en matière **d'attractivité,** de mener **des actions de communication avant le bac** et **pendant les cursus** auprès des **jeunes** et du **grand public** qui pourraient notamment consister en :
  - pour le jeune public, une sensibilisation aux bonnes pratiques dès le plus jeune âge (accompagnement dans l'acquisition d'un téléphone portable et/ou d'un compte sur un réseau social)
  - pour le grand public, l'inclusion des bonnes pratiques de cybersécurité dans la formation professionnelle de base, au même titre que l'hygiène, la sécurité incendie ou le secourisme.

- ⇨ **d'enseigner les concepts** et les **cas d'usages principaux de la cybersécurité** dans les **formations d'ingénieurs ne relevant pas spécifiquement du numérique** mais également **dans les écoles de commerce** (Management de SI), à l'instar de ce qui a pu être développé pour le Big Data. L'ensemble des étudiants devrait être en capacité de suivre durant son cursus une initiation / une formation aux concepts globaux de la cybersécurité.

- ⇨ d'intégrer **le sujet « cybersécurité »** dans **l'ensemble des cursus des étudiants ingénieurs du numérique** comme un élément nécessaire et spécifique de formation. **La sécurité n'est pas une option,** elle doit être intégrée **dans les tous** les cours et maitrisée par l'ensemble des fonctions relevant du numérique, du développeur/de la développeuse au/à la chef.fe de projet. Pour cela, nous recommandons notamment **le programme CyberEdu** de l'ANSSI qui vise à sensibiliser à la sécurité les étudiants des formations supérieures en informatique non dédiées à la sécurité. (Ressources en accès libre : modules de formation, fiches de cours ; guide pédagogique… https://www.ssi.gouv.fr/entreprise/formations/cyberedu/)

- ⇨ d'intégrer la cybersécurité comme **une spécialité à part entière.** Cette spécialisation doit inclure des **travaux pratiques** sur les **usages et/ou secteurs particuliers**.
  Nous invitons aussi nos établissements à s'intéresser et à **demander le label SecNum*edu*,** label de formations initiales en cybersécurité de l'enseignement supérieur mis en place par l'ANSSI (https://www.ssi.gouv.fr/entreprise/formations/secnumedu).

Enfin, les formations doivent insister sur la **maîtrise des fondamentaux** et des concepts, et développer cette **capacité à s'adapter** qui permettra au professionnel, tout au long de sa carrière, d'évoluer.
Au-delà, il convient d'agir au quotidien pour **évangéliser les particuliers et les entreprises** aux **nouvelles menaces** issues du déploiement des nouvelles technologies, mais aussi et surtout, pour développer des solutions en capacité de les anticiper et de les parer.

Talents du numérique porte en effet cette conviction forte : la transformation numérique de l'économie et de la société ne se fera pas de manière harmonieuse sans juste prise en compte de la dimension « sécurité ».

Suivez toute l'actualité de Talents du Numérique sur le site www.talentsdunumerique.com
et nos réseaux sociaux www.talentsdunumerique.com/communaute
Contact : Rémi Ferrand (délégué général) - remi.ferrand@talentsdunumerique.com