26/10/2018

KIT DE PRESSE

PANORAMA DES MÉTIERS DE LA SÉCURITÉ DU NUMÉRIQUE

PAR L'AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION

SOMMAIRE

LES MÉTIERS DE LA SÉCURITÉ DU NUMÉRIQUE

Un groupe de travail composé de représentants de l'enseignement supérieur, du monde industriel, notamment de Syntec Numérique et de l'Agence nationale de la sécurité des systèmes d'information (ANSSI) a élaboré un panorama de « profils métiers » dans le domaine de la sécurité du numérique.

Cette démarche inédite, développée dans le cadre de label SecNumedu*, présente de façon simple et concrète les grands métiers de la sécurité des systèmes d'information (SSI).

« *Dans un monde où les technologies, les menaces et les usages sont en perpétuelle évolution, le marché de la cybersécurité offre de nombreuses opportunités de carrière. Ces nouveaux métiers vont permettre de répondre aux besoins d'aujourd'hui et d'anticiper ceux de demain* », résume Guillaume Poupard, Directeur général de l'ANSSI.

Ce panorama 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 « les formations et les compétences en France sur la cybersécurité »
- le document du NIST SP800-181 de novembre 2016

Cinq catégories de métiers ont été définies par le groupe de travail dans le cadre du label SecNum*edu**:

- Pilotage, organisation et gestion des risques
- Management de projets et cycle de vie
- Opération et maintien en condition opérationnelle
- Support et gestion des incidents
- Conseil, audit et expertise

Dans un domaine aussi mouvant et dynamique que la sécurité du numérique, ce panorama de métiers sera évidemment amené à évoluer très régulièrement.

*** LE LABEL SECNUMEDU**

SecNumedu est un programme qui vise à labelliser des formations supérieures en sécurité du numérique qui sont conformes à une charte et des critères publics (publiés sur le site Web de l'ANSSI). Pour plus d'informations sur SecNum*edu*, rendez-vous sur :
https://www.ssi.gouv.fr/entreprise/formations/secnumedu/

PILOTAGE, ORGANISATION ET GESTION DES RISQUES

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

EXPÉRIENCE : 5 à 10 ans

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 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.

MÉTIERS ASSOCIÉS

- OSSI : Officier de la sécurité des systèmes d'information
- SSM : Information Systems Security Manager
- CISO : Chief Information Security Officer
- CSO : Chief Security Officer

CORRESPONDANT SÉCURITÉ

EXPÉRIENCE : quelques années dans un ou plusieurs domaines « métier » et formation continue en sécurité

Assure un rôle d'intermédiaire ou de relais 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 à travers la formation continue (courte ou longue).

MÉTIERS ASSOCIÉS

- CSSI : Correspondant Sécurité du Système d'Information
- Gestionnaire de Risques cyber
- Expert connexe
- CRO : Correspondant risques opérationnels
- Assistant RSSI

SPÉCIALISTE EN GESTION DE CRISE CYBER

NIVEAU DE DIPLÔME : Bac+5

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 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 (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 ».

MÉTIER ASSOCIÉ

- Cyber Defense Infrastructure Support Specialist

RESPONSABLE DU PLAN DE CONTINUITÉ D'ACTIVITÉ (RPCA)

NIVEAU DE DIPLÔME : Bac+5

EXPÉRIENCE : 3 ans d'expérience

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

MANAGEMENT DE PROJETS ET CYCLE DE VIE

CHEF DE PROJET SÉCURITÉ

NIVEAU DE DIPLÔME : Bac+5

EXPÉRIENCE : 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 chef de projet sécurité assiste le chef 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 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.

MÉTIERS ASSOCIÉS

- Chef de projet sécurité informatique
- Chef de projet sécurité des systèmes d'information
- Security Project Manager Officer (PMO)
- Program Manager
- IT program manager

DÉVELOPPEUR SÉCURITÉ

NIVEAU DE DIPLÔME : Bac+5

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, 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 / 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 développeur formé.

ARCHITECTE SÉCURITÉ

NIVEAU DE DIPLÔME : Bac+3 à Bac+5

EXPÉRIENCE : 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 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 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.

L'architecte de sécurité 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…

MÉTIERS ASSOCIÉS

- Architecte Sécurité Informatique
- Architecte Réseaux et Télécom
- System architect
- Information Security Architect
- Security architect

INTÉGRATEUR DE SÉCURITÉ

NIVEAU DE DIPLÔME : Bac+3 à Bac+5

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 informatique et/ou l'architecte sécurité 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.

L'intégrateur de sécurité 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 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.

OPÉRATION ET MAINTIEN EN CONDITION OPÉRATIONNELLE

ADMINISTRATEUR SÉCURITÉ

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 système/réseaux. Mais certaines organisations peuvent dédier des personnes à ce seul métier. Ces personnes agissent alors en complément des administrateurs réseaux et systèmes.

MÉTIERS ASSOCIÉS

- Administrateur Sécurité Informatique
- Opérateur en sécurité des systèmes d'information
- System Administrator
- Cyber Defense Infrastructure Support Specialist

TECHNICIEN SÉCURITÉ

NIVEAU DE DIPLÔME : Bac+2/3

Le technicien sécurité est responsable d'activités de support, de gestion ou d'administration de la sécurité aux plans 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 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 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 contribue aux séances de sensibilisation pour l'usage des ressources par les utilisateurs finaux.

MÉTIERS ASSOCIÉS

- Technicien support SSI
- Télé-assistant
- Technical Support Specialist

SUPPORT ET GESTION DES INCIDENTS

ANALYSTE SOC

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 RÉPONSE À INCIDENT

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 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 les experts en investigation numérique afin d'appréhender 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).

MÉTIERS ASSOCIÉS

- Spécialiste en investigation numérique
- Analyste traitement d'incident
- Cyber Crime Investigator
- Forensics Analyst
- Cyber Defense Forensics Analyst

CONSEIL, AUDIT ET EXPERTISE

CONSULTANT SÉCURITÉ « ORGANISATIONNEL »

NIVEAU DE DIPLÔME : Bac+4/5

QUALIFICATION ANSSI POSSIBLE : PASSI* (plus de détails dans l'encadré ci-dessous)

« 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.

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

Ses compétences peuvent l'amener à réaliser des prestations d'audit dans tout ou partie des domaines précédemment cités.

MÉTIERS ASSOCIÉS

- Consultant sécurité
- Consultant gouvernance, risques et conformité
- Consultant en SSI
- Auditeur organisationnel
- Lead auditor
- Lead implementer
- Systems auditor
- Information security auditor

***PRESTATAIRES D'AUDIT DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION (PASSI) QUALIFIÉS**

A travers le processus de qualification des prestataires de service, l'ANSSI s'assure qu'un service est rendu en toute confiance, par des sociétés et des intervenants compétents dans leur domaine. La qualification PASSI a pour objectif d'accroître la qualité des audits de sécurité en imposant certains critères, qui sont garantis par la réalisation d'une prestation qualifiée conforme au référentiel PASSI.

CONSULTANT SÉCURITÉ « TECHNIQUE »

NIVEAU DE DIPLÔME : Bac+4/5

QUALIFICATION ANSSI POSSIBLE : PASSI* (plus de détails dans l'encadré page 5)

« 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 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.

MÉTIERS ASSOCIÉS

- Auditeur technique sécurité et test d'intrusion
- Pen testeur
- Expert audit sécurité et intrusion
- Spécialiste cybersécurité
- Expert technique
- Consultant sécurité
- Security Control Assessor
- Vulnerability Assessment Analyst
- Ethical Hacker
- Penetration tester
- Vulnerability assessor

CRYPTOLOGUE

NIVEAU DE DIPLÔME : Bac+5 à doctorat

Il 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 peut être amené à concevoir des algorithmes cryptographiques.

MÉTIERS ASSOCIÉS

- Expert crypto
- Cryptographer
- Cryptanalyst

JURISTE SPÉCIALISÉ EN CYBERSÉCURITÉ

NIVEAU DE DIPLÔME : Bac+5/6

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.

MÉTIERS ASSOCIÉS

- Consultant juridique en cyberdéfense
- Cyber Legal Advisor

ÉVALUATEUR SÉCURITÉ

NIVEAU DE DIPLÔME : Bac+5

Le métier concerne les laboratoires qui réalisent les évaluations de la sécurité des technologies de l'information et les développeurs de produits devant être évalués :

- Coté évaluateur :

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 normalisée ou réglementaire (CC, CSPN…) ou privée (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.

MÉTIERS ASSOCIÉS

- Responsable évaluation
- Responsable certification
- System Testing and Evaluation Specialist

ANALYSTE DE LA MENACE

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

MÉTIER ASSOCIÉ

- Threat Intelligence

DÉLÉGUÉ À LA PROTECTION DES DONNÉES (DPD)

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 informatique et libertés (CIL)
- Data protection officer (DPO)
- Privacy Compliance Manager
- Privacy officer
- Data protection officer

Retrouvez plus d'informations dans la rubrique formation du site de l'ANSSI :
https://www.ssi.gouv.fr/particulier/formations/

À PROPOS DE L'ANSSI

L'Agence nationale de la sécurité des systèmes d'information (ANSSI) a été créée par le décret
n° 2009-834 du 7 juillet 2009 sous la forme d'un service à compétence nationale.
L'agence assure la mission d'autorité nationale en matière de défense et sécurité des systèmes d'information. Elle est rattachée au secrétaire général de la défense et de la sécurité nationale, sous l'autorité du Premier ministre.

AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION
ANSSI — 51, boulevard de la Tour-Maubourg — 75 700 PARIS 07 SP

www.ssi.gouv.fr — communication@ssi.gouv.fr

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
Premier ministre
SGDSN

CONTACTS PRESSE

communication@ssi.gouv.fr

Margaux Vincent
margaux.vincent@ssi.gouv.fr
01 71 75 84 04