Observatoire paritaire, prospectif et analytique des métiers et qualifications de la Métallurgie

CERTIFICATIONS

CQPM • Préventeur en cybersécurité des systèmes d'information

Gérer - Administrer

Informatique - Réseaux

MISSION(S) VISÉE(S) PAR LA QUALIFICATION

Le vocable cybersécurité est employé fréquemment dans les entreprises et les organisations, il peut présenter certaines variantes : sécurité des systèmes d'information ou encore sécurité du numérique. Ces notions ont un sens équivalent. La cybersécurité englobe plus largement les aspects juridiques, techniques et administratifs liés à la sécurité dans le monde de l'informatique, des réseaux et des Systèmes d'Information (SI). La cybersécurité consiste à garantir la sécurité informatique des infrastructures techniques du SI de l'entreprise ou de l'organisation.

Le préventeur en cybersécurité des systèmes d'Information occupe une grande variété d'emplois liés à la sécurité des SI. Le préventeur en cybersécurité exerce dans toute structure, entreprise ou organisation sujettes aux menaces d'éventuels incidents de sécurité informatique ou de cyber-attaques, comme expert en test d'intrusion ou de compromission du SI, comme responsable de la sécurité informatique, ou encore comme consultant en organisation de la Sécurité des Systèmes d'Information (SSI).

Le périmètre d'intervention du préventeur en cybersécurité des systèmes d'information comprend notamment :

- L'architecture technique sécurité, afin de structurer les choix techniques, technologiques et méthodologiques d'un système ou d'un logiciel répondant à des exigences de sécurité ;
- L'audit, qui permet de mettre en avant les éventuelles failles de sécurité tant d'un point de vue utilisation que déploiement ou paramétrage, et ainsi de préconiser des solutions de contournement ou de correction des failles mises en exergue ;
- Le droit des technologies de l'information et de la communication ainsi que des données personnelles ;

- Le hacking social, afin de permettre l'identification des divers chemins d'intrusions et de tracer le profil des attaquants ainsi que leurs méthodes de travail.

Les postes occupés peuvent être classés en trois grands domaines :

- L'exploitation des infrastructures techniques de sécurité, avec un engagement sur la qualité des services délivrés. Il assure dans ce cas la responsabilité de l'exploitation en menant un ensemble d'actions visant à offrir une qualité de service en termes de sécurité. Les activités de nature technique et celles liées au management sont menées seul ou au sein d'un groupe ou d'un service ;
- L'évolution de ces infrastructures en termes technologiques. Il participe alors à l'évolution de l'infrastructure sécurité de l'entreprise dans un souci d'amélioration de la sécurité. Il réalise, en totalité ou partiellement, l'étude et la conception des évolutions des solutions techniques répondant aux besoins nouveaux exprimés. Les activités sont essentiellement de nature technique et celles liées à l'évolution du système sont menées la plupart du temps dans un mode projet.
- L'expertise technique, réglementaire et de jurisprudence, ou organisationnelle et des processus de gestion lié à la cybersécurité.

Les activités menées s'inscrivent dans le cycle de vie des opérations de l'exploitation des infrastructures informatiques et dans l'évolution de celles-ci. Dans ce cadre, elles couvrent toutes les phases depuis l'analyse du cahier des charges à la conception du système sécurité, jusqu'à la mise en production, puis son exploitation.

A partir de directives précises, le préventeur en cybersécurité doit réaliser diverses opérations telles que :

- La traduction des besoins des entreprises à partir du cahier des charges et élaborer l'architecture sécurité du SI correspondant ;
- Le maquettage du SI sécurisé à partir des exigences de l'entreprise ou de l'organisation ;
- Le déploiement du SI sécurité au sein de l'entreprise en prenant en compte la Politique de Sécurité des Systèmes d'Information (PSSI) ;
- L'élaboration des scénarios d'optimisation à partir de procédures, d'instruction, de patch de sécurité ;
- L'administration et l'exploitation de la sécurité du SI à partir des procédures et des instructions ;
- L'audit d'un SI afin de décliner des scénarios argumentés de mise à niveau et de sécurisation de celui-ci.

A partir de directives générales, le préventeur en cybersécurité doit également décliner la PSSI de l'entreprise, qu'elle soit stratégique, tactique, ou dite éthique (ou de « bonne conduite »).

ACTIVITÉS

En fonction des différents contextes et/ou organisations des entreprises, les missions ou activités du titulaire portent sur :

1. La définition de l'architecture sécurisée d'un système d'information

Cette activité consiste à étudier le cahier des charges du client afin d'en extraire l'ensemble des fonctionnalités souhaitées par ce dernier, ainsi que l'ensemble des contraintes de sécurité, contraintes réglementaires et/ou environnementales, etc. À partir de ces fonctionnalités et de ces contraintes, l'objectif va être de réaliser une preuve de concept (Proof of concept (POC), ou encore une démonstration de faisabilité) de manière à valider soit l'ensemble des fonctionnalités et des contraintes, soit les fonctionnalités qui sont le plus difficile à mettre en œuvre. À l'issue de la réalisation de cette maquette, l'ensemble des documentations techniques va être rédigé.

2. La prévention et intervention en cas d'incident de sécurité informatique

Cette activité consiste à s'assurer que le système d'information fonctionne correctement sur la durée. Pour cela il est nécessaire de définir un plan de continuité d'activité (PCA) ainsi qu'un plan de reprise d'activité (PRA). Ces 2 plans vont permettre de garantir la disponibilité du système d'information et ceci quel que soit l'événement qui puisse arriver. Il est également nécessaire d'auditer, d'un point de vue sécurité, le système d'information afin de garantir que l'ensemble des failles de sécurité est maîtrisé et lorsqu'il reste une faille de sécurité de permettre de rédiger des préconisations de remédiation sur celle-ci.

3. Le management et la supervision d'un système d'information

Cette activité consiste à monitorer (fait de maintenir un œil, de surveiller quelque chose) différents paramètres du système d'information au sein du Security Operation Center (SOC : désigne dans une entreprise l'équipe en charge d'assurer la sécurité de l'information). Ceci se fait au travers de requêtes corrélées qui permettent de mettre en relation différents événements qui pris indépendamment passeraient inaperçus. Dans cette activité, il est également nécessaire d'expliquer aux collaborateurs de l'entreprise les règles de base de la sécurité informatique afin de les sensibiliser aux risques qu'ils peuvent faire courir à leur entreprise.

COMPÉTENCES

- Analyser un cahier des charges d'un système d'information
- Élaborer la maquette du dossier d'architecture technique
- Élaborer l'architecture d'un système d'information sécurisé
- Définir un plan de reprise d'activités informatique
- Auditer la sécurité du système d'information
- Gérer un système d'information après compromission
- Superviser le système d'information

- Sensibiliser les utilisateurs du système d'information à l'hygiène informatique et aux risques liés à la cybersécurité

LES MÉTIERS LIÉS

- Responsable Sécurité Informatique

> Les interlocuteurs

- L'UIMM territoriale la plus proche
- Représentant des salariés
- Directement en entreprise
- Conseiller d'orientation
- Conseiller en évolution profesionnelle : Pôle emploi, APEC…

> Identification

Catégorie : D
Niveau : 7
N° Cert. : 2015 0302
État : Active

> Dispositif d'accès

Qui peut accéder à la certification ?

- Jeunes et adultes
- Salarié(e)s
- Intérimaires
- Demandeurs d'emploi

Comment accéder à la certification ?

Par la formation

- Plan de développement des compétences
- Pro A

Par la Validation des Acquis de l'Expérience

- Période de Professionnalisation
- Plan de formation
- CPF
- Congé VAE