Commission paritaire nationale de l'emploi et de la formation professionnelle de la métallurgie

Qualification : **2020 0302**

Catégorie : **D**

Niveau : **7**

Dernière modification : **07/10/ 2021**

REFERENTIELS DU CQPM

Titre du CQPM : Préventeur en cybersécurité des systèmes d'information

1. REFERENTIEL D'ACTIVITES DU CQPM

1.1. Missions et activités visées par la certification professionnelle

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 »).

Ses activités 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.

La finalité de cette activité vise à traduire les besoins de l'entreprise ou de l'organisation en matière de sécurité du système d'information.

- **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.

La finalité de cette activité vise à réaliser des audits d'un SI et de répertorier ses points forts et ses vulnérabilités, de réaliser un diagnostic à la suite de sa compromission et d'en réaliser un rapport contenant les preuves numériques.

- **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.

La finalité de cette activité vise à surveiller les SI et leurs processus, et de déployer la politique sécurité de l'entreprise ou de l'organisation à l'ensemble des utilisateurs.

1.2. Environnement de travail

Selon la taille et la nature de l'entreprise la fonction peut prendre des orientations différentes, mais dans tous les cas de figure, la maîtrise des techniques et la capacité à assumer des responsabilités sont indispensables à l'exercice du métier de préventeur en 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.

Son environnement de travail est principalement composé de serveurs, ordinateurs de développement, matériels réseau et cartes électroniques de scrutation. Il travaille dans son bureau et/ou en « *open space* » dans son organisation ou chez le client.

Les préventeurs en cybersécurité des systèmes d'informations sont principalement des hommes ou femmes ingénieurs système et réseau, ingénieurs sécurité informatique, chefs de projet SSI, Responsable Sécurité des SI, architectes sécurité, Pentesteurs (tests de pénétration), ou encore analyste FORENSIC, … qui constituent leur propre environnement de travail lorsqu'ils évoluent en équipe projet.

1.3. Interactions dans l'environnement de travail

Les actions menées par le préventeur en cybersécurité auront un impact direct sur la sécurisation du patrimoine informationnel de l'entreprise ou de l'organisation. De même, ces actions vont avoir un impact sur le comportement des collaborateurs de l'entreprise, via la politique de sécurité élaborée.

Le préventeur en cybersécurité est au cœur de nombreux échanges d'informations avec les autres. Cela peut se traduire par des réunions avec le client final afin de recueillir son besoin, par des interviews d'opérationnels de l'entreprise afin de déterminer les applications critiques du SI, mais également par le passage de consignes, par des formations et sensibilisations des collaborateurs dans le cadre de conduite de changement lors de la mise en place de la politique de sécurité. Il va également travailler en groupe afin de mener, par exemple, des audits du SI, ou encore afin de réaliser une analyse dite « médico-légale » après une cyber-attaque.

Enfin, la pratique de l'anglais (écrire, parler, comprendre) est nécessaire pour assurer les fonctions de préventeur en cybersécurité des systèmes d'information et se situe à partir du niveau B1 du Cadre Européen de Référence pour les langues (CERL).

2. REFERENTIEL DE COMPETENCES

Compétences et connaissances afférentes au CQPM visé :

Pour cela, il (elle) doit être capable de :

Blocs de compétences	*Compétences professionnelles*	*Connaissances associées*
BDC 1 : La définition de l'architecture sécurisée d'un système d'information	1. Analyser un cahier des charges d'un système d'information 2. Élaborer la maquette du dossier d'architecture technique 3. Élaborer l'architecture d'un système d'information sécurisé	*<u>Dans le domaine des réseaux :</u>* *- Savoir ce qu'est un LAN, un MAN, un WAN ;* *- Connaissance de la terminologie des réseaux ;* *- Connaissance de l'architecture TCP/IP ;* *<u>Dans le domaine des systèmes :</u>* *- Connaissances approfondies sur les architectures Windows et LINUX ;* *- Savoir mettre en place une stratégie GPO ;* *- Connaître les concepts essentiels d'une PKI ;* *- Savoir mettre en place une IAM (Identity Access Management)* *<u>Dans le domaine du développement :</u>* *- Avoir des notions de base en algorithmie (construction, optimisation d'un algorithme) ;* *- Langages C et Python (Connaissance de la syntaxe de base, savoir réaliser un programme simple, savoir faire des fonctions et passer des arguments, connaitre les bibliothèques standards)* *- Savoir reverser un programme* *<u>Dans le domaine des Systèmes d'informations :</u>* *- Connaissance des Proxy ;* *- Connaissance du principe de fonctionnement des VPN.*
BDC 2 : La prévention et intervention en cas d'incident de sécurité informatique	1. Définir un plan de reprise d'activités informatique 2. Auditer la sécurité du système d'information 3. Gérer un système d'information après compromission	*<u>Dans le domaine des réseaux :</u>* *- Connaissance des adressages publics et privés ;* *- Connaissance des mécanismes de translations d'adresses.* *<u>Dans le domaine des systèmes :</u>* *- Connaissance de la gestion des packages et des installations ;* *<u>Dans le domaine du développement :</u>* *- savoir réaliser du fuzzing sur un composant logiciel* *- Connaitre la méthodologie OWASP de sécurisation du code* *<u>Dans le domaine de la sécurité :</u>* *- Connaissance des différentes failles matérielles, des différentes menaces et des malwares* *- Connaissance sur l'analyse médico-légale d'un crime informatique* *<u>Dans le domaine des Systèmes d'informations :</u>* *- Connaissance des différents dispositifs de protection usuels : anti-virus, Firewall.*
BDC 3 : Le management et la supervision d'un système d'information	1. Superviser le système d'information *2.* Sensibiliser les utilisateurs du système d'information à l'hygiène informatique et aux risques liés à la cybersécurité	*<u>Dans le domaine des réseaux :</u>* *- Connaissances des protocoles réseaux filaires et Wireless* *<u>Dans le domaine des systèmes :</u>* *- Connaissance de la configuration d'un réseau* *- Savoir sécuriser un DNS* *- Connaître l'architecture AD multi-forêts et savoir la sécuriser ;* *<u>Dans le domaine de la sécurité :</u>* *- Connaissance approfondie des architectures sécurisées ;* *- Connaissance sur les techniques d'attaque : attaques réseau, système, de code, des mots de passe, des adressages IP, du déni de service, des types Man in the Middle, des attaques par ingénierie sociale ;* *- Connaissance de base de la cryptologie quantique* *<u>Dans le domaine des Systèmes d'informations :</u>* *- Connaissance des principes de fonctionnement unifié au sein d'un SI.*

3. REFERENTIEL D'EVALUATIONS

3.1. Conditions de réalisation et d'évaluation des compétences professionnelles selon les critères mesurables, observables et les résultats attendus

Compétences professionnelles	Conditions de réalisation	Critères mesurables et observables	Résultats attendus
1 Analyser un cahier des charges d'un système d'information	L'analyse se fait à partir : - Du cahier des charges client, décrivant les fonctionnalités et contraintes auxquelles doit répondre le système d'information ; - Des comptes rendus des réunions préparatoires avec le client ; - Des textes législatifs de sécurité, tels que : ○ RGS V2 ; ○ Loi informatique et liberté ; ○ Loi de programmation militaire, …	**<u>En matière de méthodes utilisées :</u>** Les différents livrables du cahier des charges sont identifiés. La matrice de traçabilité des exigences est définie. L'analyse des risques et des opportunités est faite. La liste des attendus client est définie. Elle précise tout élément que le client doit impérativement mettre à disposition pour assurer correctement la mission de prévention en cybersécurité, c'est-à-dire, et de manière non exhaustive : - la mise à disposition d'un accès au système d'information existant ; - la mise à disposition de la charte utilisateur ; - tout autre attendu client, stipulé dans le cahier des charges. **<u>En matière de moyens utilisés :</u>** L'analyse des risques et des opportunités est formalisée dans un document recensant tous les liens existants du cahier des charges. La liste des attendus client est définie principalement dans des documents Word et Excel. Elle est formalisée sous la forme d'une matrice Excel de traçabilité. **<u>En matière de liens professionnels / relationnels :</u>** L'analyse de la demande formalisée traduit bien les exigences et besoins réels du client, elle permet de cadrer le projet voire de le réadapter, elle est exploitable et partageable avec un tiers. Toute information nécessaire à la conduite du futur projet est recherchée auprès des interlocuteurs (parties prenantes du projet). **<u>En matière de contraintes liées au milieu et environnement de travail :</u>** Le besoin du client tient compte de l'ensemble des éléments antérieurs et/ou en interaction avec d'autres projets. La demande prend en considération les éléments réglementaires (sécurité, environnement), ainsi que les exigences en termes de qualité, coût et délais.	La matrice de traçabilité des exigences permet de confectionner différentes vues du système d'information à partir de l'ensemble des exigences. L'analyse des risques et des opportunités permet d'évaluer les menaces pouvant être considérées comme envisageables avec une certaine opportunité. Les différents livrables identifiés du cahier des charges permettent l'élaboration : - Du dossier d'architecture technique général ; - Du dossier d'architecture technique spécifique sécurité ; - Du dossier de justificatifs des écarts.

Compétences professionnelles	Conditions de réalisation	Critères mesurables et observables	Résultats attendus
2 Élaborer la maquette du dossier d'architecture technique	La maquette (ou Proof Of Concept (POC)) est élaborée à partir : - de l'analyse de tout ou partie du cahier des charges client ; - des machines représentatives du système d'information (serveurs, PC client, matériels réseau (switch, routeur, firewall, etc.)).	**En matière de méthodes utilisées :** Les grandes étapes du dossier d'architecture technique (général et spécifique sécurité) sont rédigées. L'organisation des différents éléments du système est identifiable par un tiers. Les relations entre les éléments (logiciels, matériels, ressources humaines, informations, …) sont schématisées. Les fonctionnalités non réalisables de la maquette sont identifiées. **En matière de moyens utilisés :** La réalisation de la maquette se fait à partir d'un ensemble de serveurs, PC, matériels réseau (Routeurs, Switch, Firewall, etc.). **En matière de liens professionnels / relationnels :** La réalisation du POC est un travail d'équipe qui implique, bien sur le préventeur, mais également plusieurs autres personnes de l'équipe projet : le responsable intégration, le responsable qualité, et parfois certains développeurs. Le préventeur remonte à sa hiérarchie les résultats du POC, que ceux-ci soient positifs ou non. **En matière de contraintes liées au milieu et environnement de travail :** La contrainte principale est le respect de la traçabilité des dysfonctionnements notés (ceci se faisant par des outils comme JIRA par exemple).	Les grandes étapes du dossier d'architecture technique permettent d'identifier l'architecture générale inhérente au système d'information. La maquette répond aux exigences de tout ou partie du cahier des charges et est validée par le chef de projet ou le responsable de lot.

Compétences professionnelles	Conditions de réalisation	Critères mesurables et observables	Résultats attendus
3 Élaborer l'architecture d'un système d'information sécurisé	L'architecture est élaborée à partir : - du cahier des charges client ; - des réunions préparatoires ; - des dossiers d'architecture technique existants, le cas échéant ; - des textes législatifs de sécurité ; - de la FEROS (Fiches d'Expression Rationnelle des Objectifs de Sécurité) du système d'information ; - des machines du système d'information (serveurs, PC client, matériels réseau (switch, routeur, firewall, etc.)).	**En matière de méthodes utilisées :** Les dossiers d'architecture technique générale et d'architecture technique spécifique sécurité sont rédigés en tenant compte de la norme ISO 27002 (qui donne des lignes directrices en matière de normes organisationnelles relatives à la sécurité de l'information et des bonnes pratiques de management de la sécurité de l'information, incluant la sélection, la mise en œuvre et la gestion de mesures de sécurité prenant en compte le ou les environnement(s) de risques de sécurité de l'information de l'organisation), ainsi que la norme ISO 27004 (qui définit des lignes directrices pour surveiller, mesurer, analyser et évaluer un Système de Management de la Sécurité de l'Information) Le dossier d'analyse des impacts sécurité est réalisé. La plateforme représentative de l'architecture technique est réalisée et est fonctionnelle en regard de la matrice de traçabilité des exigences. Les fiches de recette des fonctionnalités du système d'information sont rédigées. **En matière de moyens utilisés :** La liste des attendus client définie précédemment (on la retrouve dans la matrice de traçabilité réalisée précédemment) est prise en compte, respectée et complétée le cas échéant. Les fiches de recette des fonctionnalités du système d'information sont rédigées le plus souvent sous Word, et Excel. Les fonctionnalités du système d'information sont testées à partir des fiches de recette définies précédemment. Chaque fiche de recette donne lieu à une fiche d'évaluation soumise au responsable qualité du projet. **En matière de liens professionnels / relationnels :** Pour cette compétence, et suivant l'importance du projet, le préventeur peut travailler en collaboration avec d'autres préventeurs. Il (elle) travaille également en étroite collaboration avec le responsable qualité du projet. **En matière de contraintes liées au milieu et environnement de travail :** Il n'existe pas de contraintes spécifiques liées au milieu ou à l'environnement de travail.	L'architecture du système d'information permet d'identifier le système d'information sécurisé. L'ensemble des fiches de recette déroulées ont un statut « test OK ». Les fiches de recette des fonctionnalités sont validées par le chef de projet, le responsable de lot, ou le responsable intégration vérification validation qualité (IVVQ).

Compétences professionnelles	Conditions de réalisation	Critères mesurables et observables	Résultats attendus
4 Définir un plan de reprise d'activités informatique	Le plan de reprise est défini à partir : - des méthodologies standardisées, ou normes (ISO 22301) ; - des interviews utilisateurs ; - du dossier d'architecture technique (général, spécifique) ; - du dossier d'analyse des impacts sécurité.	**En matière de méthodes utilisées :** Les fiches d'interview des différents acteurs du système d'information (utilisateurs, administrateurs, ...) sont élaborées. Le rapport d'interviews est rédigé et donne lieu à une synthèse éliminant les redondances. Le listing des applications/services critiques est défini. A partir des éléments ci-dessus, des contraintes de temps de rétablissement des services imposées par le client et conformément à l'ISO 22301, le préventeur rédige des procédures de rétablissement en cas d'interruption mineure (Plan de Continuité de l'Activité) ou en cas de sinistre majeur (Plan de Reprise de l'Activité).	Les fiches d'interview sont validées par le chef de projet ou le responsable de lot. Le plan de reprise d'activité répond au bon fonctionnement du système d'information en mode dégradé.
		En matière de moyens utilisés : Les fiches d'interview sont élaborées sous Word ou Excel. Le listing des applications/services est fait sous Excel. La norme ISO9 22301 est appliquée à la définition du PCA et du PRA ou les normes utilisées sont adaptées.	
		En matière de liens professionnels / relationnels : Les interviews sont réalisées auprès des différents acteurs du système d'information (utilisateurs, administrateurs, ...). Ces interviews sont faites par le préventeur qui, connaissant parfaitement la norme ISO 22301, sait, en tant que de besoin, recentrer son interlocuteur.	
		En matière de contraintes liées au milieu et environnement de travail : Les contraintes liées à cette compétence sont issues du fait que le préventeur, faisant ses interviews en transversale, doit faire preuve de beaucoup de pédagogie et de diplomatie lors de celles-ci.	

Compétences professionnelles	Conditions de réalisation	Critères mesurables et observables	Résultats attendus
5 Auditer la sécurité du système d'information	L'audit est réalisé à partir : - De la PSSI (Politique de Sécurité du Système d'informations) - Du dossier d'architecture technique ; - De la liste des applicatifs présents sur le système d'information ; - De la liste des failles connues pour chaque applicatif présent ; - Des Fiches d'Expression Rationnelle des Objectifs de Sécurité (FEROS) du système d'information ; - Du système d'information ; - De la charte utilisateur ; - De la Politique de Sécurité du Système d'Information (PSSI).	**<u>En matière de méthodes utilisées :</u>** L'audit est réalisé dans les règles de la PSSI et fait l'objet d'un rapport que rédige le préventeur. Le rapport d'audit du système d'information fait apparaitre l'ensemble des failles identifiées, ainsi que les méthodes techniques et/ou organisationnelles nécessaires à mettre en place pour les remédier. Le rapport d'audit est synthétisé de manière à éliminer les redondances et à mettre en évidence les éléments critiques (failles/risques identifiés) présents dans le système d'information. **<u>En matière de moyens utilisés :</u>** L'audit technique va être réalisé à partir d'outils de pentest appelés des Profileurs (exemple : Wappalyzer, BuiltWith, …), ainsi que d'autres outils techniques type Dnsdumpster, nmmapper, etc. Il est à noter que les failles informatiques recensées évoluant très régulièrement, les outils d'audit et pentest évoluent également très rapidement, nécessitant ainsi de la part du préventeur (trice) une veille technologique régulière sur ces outils. Une fois les analyses techniques réalisées, le rapport d'audit est rédigé sous Word. Les failles techniques sont recensées par le CERT qui sont le centre gouvernemental de veille, d'alerte et de réponse aux attaques informatiques. **<u>En matière de liens professionnels / relationnels :</u>** L'audit est fait en équipe et se déroule par phases : - La VAPT : Évaluation de la vulnérabilité et test de pénétration - L'analyse statique et dynamique du code (non systématique) - L'analyse de la configuration des périphériques réseau - Les tests de manipulation des paiements (le cas échéant) - Les tests de l'infrastructure des serveurs et DevOps - Les tests de la logique d'entreprise, les préconisations de remédiation Un compte-rendu est réalisé au client final et/ou au chef de projet ou au responsable de lot. **<u>En matière de contraintes liées au milieu et environnement de travail :</u>** La contrainte principale est la phase rédactionnelle du rapport d'audit. Effectivement, les préventeurs sont des collaborateurs extrêmement pointus techniquement, mais ils doivent aussi avoir la capacité de vulgariser les conclusions de leur audit afin de le rendre compréhensible à des non-initiés et tout particulièrement aux VIP de leur entreprise cliente.	Les préconisations de sécurisation du système d'information sont établies et priorisées. Le rapport d'audit synthétisé met en évidence les éléments critiques présents dans le système d'information.

Compétences professionnelles	Conditions de réalisation	Critères mesurables et observables	Résultats attendus
6 Gérer un système d'information après compromission	Le système d'information est géré en conséquence : - D'une cyber-attaque ayant eu lieu ; Et à partir : - Du système d'information ; - Des mesures conservatoires validées par le chef de projet ou le responsable de lot ; - Des moyens de gestion de crise mis en œuvre	**<u>En matière de méthodes utilisées :</u>** L'enquête « médico-légale » du système d'information ayant subi une cyber-attaque est réalisée, et nécessite notamment : - La collecte et l'analyse de la « Random Access Memory » (RAM) et d'artéfacts ; - La copie des disques ; - L'analyse de journaux d'équipement réseaux, l'analyse de systèmes UNIX ; - L'analyse de systèmes Windows (ruches système et utilisateurs, journaux et quarantaine antivirus, etc.…) ; - Les analyses Active Directory ; - La sécurisation des preuves recueillies afin de les rendre admissibles lors d'un éventuel procès. - La préconisation de remédiations à partir des failles recensées par le CERT. Ces remédiations permettront ensuite d'éviter une nouvelle attaque utilisant les mêmes vecteurs de pénétration.	Le rapport de l'enquête « médico-légale » de l'attaque est rédigé, ainsi que la synthèse des moyens de compromission et de camouflage.
		<u>En matière de moyens utilisés :</u> Pour la réalisation de l'analyse médico-légale après un crime informatique, le préventeur s'appuie sur de solides compétences techniques sur les différentes possibilités d'hacker un système, mais également sur certains outils type LACE CARVER (permet d'extraire efficacement les fichiers de preuves), BlueBear LACE (permet de catégoriser efficacement de grandes quantités de données d'images et de données vidéo), Digital Forensic Framework (capable d'extraire, analyser et mettre en corrélation des traces suspectes et des données de différents fichiers) ou encore Regripper (permet de faire l'analyse des registres du système). Le rapport est rédigé sous une application de traitement de texte.	
		<u>En matière de liens professionnels / relationnels :</u> Le préventeur s'appuie sur l'équipe de spécialistes techniques et le chef de projet, il les sollicite autant que possible pour assurer son analyse médico-légale après compromission du système d'information.	
		<u>En matière de contraintes liées au milieu et environnement de travail :</u> La contrainte majeure de cette compétence est liée au fait que l'entreprise dans laquelle le préventeur intervient, vient de subir un crime informatique avec souvent des conséquences graves. Dans ce contexte, tous les intervenants de l'entreprise ont parfois des réactions disproportionnées que le préventeur doit aussi gérer. De même, un crime informatique est souvent corrélé avec une gestion de crise et ses aspects communication vers l'extérieur, aspects qui peuvent aussi être délégués au préventeur pour les parties techniques.	

Compétences professionnelles	Conditions de réalisation	Critères mesurables et observables	Résultats attendus
7 Superviser le système d'information	Le système d'information est supervisé à partir : - Des matériels hardwares et softwares du système d'information ; - Du cahier des charges client ; - Des logiciels de supervision et de création de requêtes à disposition.	**<u>En matière de méthodes utilisées :</u>** Les logiciels de supervision « Security Information and Event Management » (SIEM), exemple : SPLUNK, …) et de requêtes corrélées (exemple : Elastic Search, …) sont identifiés à partir des exigences du cahier des charges client.	Les requêtes d'analyse sont établies, validées par le chef de projet ou le responsable de lot, et sont fonctionnelles. Ces requêtes vont permettre d'associer entre eux divers événements qui, pris indépendamment ne laisseraient rien présager, mais qui pris conjointement signalent le début d'une attaque informatique.
		<u>En matière de moyens utilisés :</u> Les logiciels de supervision et de création de requêtes corrélées sont installés, configurés et permettent de récupérer correctement l'ensemble des informations nécessaires à la surveillance des systèmes d'informations.	
		<u>En matière de liens professionnels / relationnels :</u> En règle générale, le préventeur est autonome pour la supervision d'un système d'information. Cela pouvant naturellement être modulable en fonction de la taille, de la complexité du SI, et donc de l'organisation en place.	
		<u>En matière de contraintes liées au milieu et environnement de travail :</u> Les contraintes principales sont liées à l'extrême niveau de concentration nécessaire pour surveiller l'ensemble des indicateurs remontés et pour ne pas laisser passer une corrélation d'événements qui pourraient être le signal du début d'une attaque informatique.	

Compétences professionnelles	Conditions de réalisation	Critères mesurables et observables	Résultats attendus
8 Sensibiliser les utilisateurs du système d'information à l'hygiène informatique et aux risques liés à la cybersécurité	Les personnels de l'entreprise ou de l'organisation sont sensibilisés à partir : - De la politique sécurité de l'entreprise (PSSI) ; - De la charte utilisateur ; - Des préconisations de l'Agence National de la Sécurité des Systèmes d'Information (ANSSI) ; - De la production de supports rédigés reprenant des termes techniques en anglais.	**<u>En matière de méthodes utilisées :</u>** Les réunions de sensibilisation sont planifiées et organisées avec l'ensemble des chefs de service qui libèrent leurs personnels afin de suivre cette sensibilisation. Les supports de sensibilisation à l'hygiène informatique sont réalisés et comportent : - Les risques utilisateurs en fonction du poste occupé ; - Les mesures mises en place par l'entreprise ou l'organisation ; - Les mesures à mettre en place par l'utilisateur en fonction du poste occupé. **<u>En matière de moyens utilisés :</u>** Le préventeur définit ses objectifs pédagogiques, réalise son déroulé pédagogique et prépare des supports de cours (textes, textes réglementaires, animations, vidéos…) avec les moyens bureautiques à disposition dans son organisation. **<u>En matière de liens professionnels / relationnels :</u>** Le préventeur sollicite les chefs de service de l'entreprise, ainsi que la Direction des Ressources Humaines afin de planifier l'ensemble des sessions de sensibilisation, et d'être certain que tous les personnels ont bien suivi celle-ci. **<u>En matière de contraintes liées au milieu et environnement de travail :</u>** La principale contrainte est de faire comprendre aux auditeurs que cette sensibilisation n'est pas seulement là pour faire passer le temps, mais qu'elle a une réelle plu value pour l'entreprise. Néanmoins, il n'est pas du ressort du préventeur de garantir la probité des personnels ayant suivis cette sensibilisation.	Les réunions de sensibilisation ainsi que les supports de formation sont validées par le chef de projet. Les sessions de sensibilisation sont réalisées : - Systématiquement pour les nouveaux arrivants au sein de l'entreprise ou de l'organisation ; - Tiennent compte de la planification élaborée en amont. La maîtrise de l'anglais est caractérisée au minimum : - Par la compréhension des termes et notions essentiels liés à l'informatique et des systèmes d'information ; - En prenant part sans préparation à une conversation technique et en articulant des expressions techniques de manière simple en donnant des raisons et des opinions sur les risques liés à la cybersécurité ; - En écrivant un texte simple et cohérent sur un sujet relatif à la cybersécurité.

3.2 MODALITES D'EVALUATION

3.2.1 Conditions de mise en œuvre des évaluations en vue de la certification

- L'accès au CQPM ou blocs de compétences implique une inscription préalable du candidat à la certification auprès de l'UIMM territoriale centre de certification.

- L'UIMM territoriale centre de certification et l'entreprise ou à défaut le candidat (Salariés ; VAE ; Demandeurs d'emploi…) définissent dans un dossier qui sera transmis à l'UIMM centre de certification, les modalités d'évaluation qui seront mises en œuvre en fonction du contexte parmi celles prévues dans le référentiel de certification.

- Les modalités d'évaluation reposant sur des activités/missions ou projets réalisés en milieu professionnel sont privilégiées.

3.2.2 Mise en œuvre des modalités d'évaluation

A) Validation des compétences professionnelles

Les compétences professionnelles mentionnées dans le référentiel de certification sont évaluées par la commission d'évaluation à l'aide des critères mesurables, observables et les résultats attendus selon les conditions d'évaluation précisées dans le référentiel de certification, ceux-ci sont complétés par l'avis de l'entreprise d'accueil du candidat à la certification professionnelle (hors dispositif VAE).

COMMISSION D'EVALUATION La commission d'évaluation est composée de plusieurs membres qualifiés ayant une expérience professionnelle leur permettant d'évaluer la maîtrise des compétences professionnelles du candidat identifiées dans le référentiel de la certification professionnelle sélectionnée.	**ENTREPRISE** (hors VAE)
Les différentes modalités d'évaluation sont les suivantes : **ÉVALUATION EN SITUATION PROFESSIONNELLE RÉELLE.** L'évaluation des compétences professionnelles s'effectue dans le cadre d'activités professionnelles réelles réalisées en entreprise	**AVIS DE L'ENTREPRISE.** L'entreprise (tuteur, responsable hiérarchique ou fonctionnel…) donne un avis au regard du référentiel d'activité.

ou en centre de formation habilité, ou tout autre lieu adapté. Celle-ci s'appuie sur : 1. une observation en situation de travail. 2. des questionnements avec apport d'éléments de preuve sur les activités professionnelles réalisées en entreprise par le candidat. **PRÉSENTATION DES PROJETS OU ACTIVITÉS RÉALISÉS EN MILIEU PROFESSIONNEL.** Le candidat transmet un rapport à l'UIMM territoriale centre de certification, dans les délais et conditions préalablement fixés, afin de montrer que les compétences professionnelles à évaluer selon cette modalité ont bien été mises en œuvre en entreprise à l'occasion d'un ou plusieurs projets ou activités. La présentation de ces projets ou activités devant une commission d'évaluation permettra au candidat de démontrer que les exigences du référentiel de certification sont satisfaites.	(hors VAE)

4 CONDITIONS D'ADMISSIBILITE

Les CQPM, ou les blocs de compétences pour les CQPM inscrits au RNCP, sont attribués aux candidats[1] par le jury paritaire de délibération sous le contrôle du groupe technique paritaire « Certifications », à l'issue des actions d'évaluation, et dès lors que toutes les compétences professionnelles ont été acquises et validées par le jury paritaire de délibération.

[1] Le terme générique « candidat » est utilisé pour désigner un candidat ou une candidate.