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

Qualification : **MQ 2015 04 92 0302**

Catégorie : D

Dernière Modification : 02/04/2015

REFERENTIEL DU CQPM

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

1. REFERENTIEL D'ACTIVITES DU CQPM

1.1. Mission (s) et activités visées par la qualification

Le (la) Préventeur (trice) en cybersécurité des systèmes d'information occupe une grande variété d'emplois liés à la sécurité des systèmes d'information. Le (la) préventeur (trice) 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).

En fonction des différents contextes et/ou organisations des entreprises, les missions ou activités du titulaire peuvent porter à titre d'exemples sur :

- *la définition de l'architecture sécurisée d'un système d'information ;*
- *la prévention et l'intervention en cas d'incident de sécurité informatique ;*
- *le management et la supervision d'un système d'information.*

1.2. Environnement de travail

Le terme cybersécurité est employé fréquemment dans les entreprises et les organisations. 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 périmètre d'intervention du (de la) préventeur (trice) en cybersécurité des SI comprend notamment :

- *l'architecture technique sécurité afin de structurer les choix techniques, technologiques et méthodologiques d'un système ou 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.*

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 (trice) en cybersécurité.

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 terme technologique. 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 selon un mode projet la plupart du temps ;*
- *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 (la) préventeur (trice) en cybersécurité doit réaliser des opérations telles que :

- *traduire les besoins des entreprises à partir du cahier des charges et élaborer l'architecture sécurité du SI correspondant ;*
- *maquetter le SI sécurisé à partir des exigences de l'entreprise ou de l'organisation ;*
- *déployer le SI sécurité au sein de l'entreprise en prenant en compte la Politique de Sécurité des Systèmes d'Information (PSSI) ;*
- *élaborer des scénarios d'optimisation à partir de procédures, d'instruction, de patch de sécurité ;*
- *administrer et exploiter la sécurité du SI à partir des procédures et des instructions ;*
- *auditer un SI afin de décliner des scénarios argumentés de mise à niveau et de sécurisation du SI.*

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

1.3. Interactions dans l'environnement de travail

Les actions menées par le (la) préventeur (trice) 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 (la) préventeur (trice) 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 (elle) 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.

2. REFERENTIEL DE CERTIFICATION DU CQPM

2.1. Capacités professionnelles du CQPM

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

Capacités Professionnelles	*Intitulé des regroupements de capacités professionnelles en unités cohérentes [1]*
1- Analyser un cahier des charges d'un système d'information	*BDC 0077 : La définition de l'architecture sécurisée d'un système d'information*
2- Élaborer la maquette du dossier d'architecture technique	
3- Élaborer l'architecture d'un système d'information sécurisé	
4- Définir un plan de reprise d'activités informatique	*BDC 0078 : La prévention et intervention en cas d'incident de sécurité informatique*
5- Auditer la sécurité du système d'information	
6- Gérer un système d'information après compromission	
7- Superviser le système d'information	*BDC 0079 : Le management et la supervision d'un système d'information*
8- Sensibiliser les utilisateurs du système d'information à l'hygiène informatique et aux risques liés à la cybersécurité	

[1] Blocs de compétences pour les CQPM inscrits au RNCP

2.2. Conditions de réalisation et critères d'évaluation des capacités professionnelles du CQPM

Capacités professionnelles	Conditions de réalisation	Critères observables et ou mesurables avec niveau d'exigence
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, …	□ La matrice de traçabilité des exigences est définie et formalisée dans un document recensant tous les liens existants du cahier des charges. Elle permet de confectionner différentes vues du système d'information à partir de l'ensemble des exigences.
		□ L'analyse des risques et des opportunités est faite. Elle permet d'évaluer les menaces pouvant être considérées comme envisageables avec une certaine opportunité.
		□ Les différents livrables du cahier des charges sont identifiés, et permettent l'élaboration : • du dossier d'architecture technique général ; • du dossier d'architecture technique spécifique sécurité ; • du dossier de justificatifs des écarts.
		□ 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, ...
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.).	□ Les grandes étapes du dossier d'architecture technique (général et spécifique sécurité) sont rédigées. Elles permettent d'identifier l'architecture générale inhérente au système d'information.
		□ L'organisation des différents éléments du système est identifiable par un tiers. Les relations entre les éléments (logiciels, matériels, ressources humaines, informations,…) sont schématisées.
		□ 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.
		□ Les fonctionnalités non réalisables de la maquette sont identifiées.

Capacités professionnelles	Conditions de réalisation	Critères observables et ou mesurables avec niveau d'exigence
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.).	□ Les dossiers : • d'architecture technique générale ; • d'architecture technique spécifique sécurité ; sont rédigés et permettent d'identifier le système d'information sécurisé.
		□ Le dossier d'analyse des impacts sécurité est réalisé.
		□ La liste des attendus client définie précédemment est prise en compte et complétée le cas échéant.
		□ 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. Elles sont validées par le chef de projet, le responsable de lot, ou le responsable intégration vérification validation qualité (IVVQ).
		□ Les fonctionnalités du système d'information sont testées. L'ensemble des fiches de recette déroulées ont un statut « test OK ».
4-*Définir un plan de reprise d'activités informatique*	Le plan de reprise est défini à partir : • des méthodologies standardisées, ou normes (EBIOS®, ISO 27001 par exemple) ; • des interviews utilisateurs ; • du dossier d'architecture technique (général, spécifique) ; du dossier d'analyse des impacts sécurité.	□ Les fiches d'interview des différents acteurs du système d'information (utilisateurs, administrateurs, ...) sont élaborées. Elles sont validées par le chef de projet ou le responsable de lot.
		□ Les interviews sont réalisées auprès des différents acteurs du système d'information (utilisateurs, administrateurs, ...).
		□ Le rapport d'interviews est rédigé et donne lieu à une synthèse éliminant les redondances.
		□ Le listing des applications/services critiques est défini. Les méthodologies standardisées appliquées ou les normes utilisées sont adaptées. Le plan répond au bon fonctionnement du système d'information en mode dégradé.

Capacités professionnelles	Conditions de réalisation	Critères observables et ou mesurables avec niveau d'exigence
5-*Auditer la sécurité du système d'information*	L'audit est réalisé à partir : • 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).	□ L'audit est réalisé dans les règles de la PSSI et fait l'objet d'un rapport.
		□ Le rapport d'audit du système d'information (machine, charte utilisateur, PSSI) est rédigé, faisant apparaitre l'ensemble des failles identifiées
		□ 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.
		□ Les préconisations de sécurisation du système d'information sont établies et priorisées.
		□ Un compte-rendu est réalisé au client final et/ou au chef de projet ou au responsable de lot.
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 ; • de tout autre moyen nécessaire.	□ 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 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 . • etc...
		□ Le rapport de l'enquête « médico-légale » de l'attaque est rédigé, ainsi que la synthèse des moyens de compromission et de camouflage.
		□ Les préconisations de sécurisation vis-à-vis des failles utilisées pour l'attaque sont rédigées et priorisées.
		□ La mise en place des mesures conservatoires (supervision de circonstance et remédiation) est adaptée.

Capacités professionnelles	Conditions de réalisation	Critères observables et ou mesurables avec niveau d'exigence
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.	□ Les logiciels de supervision SIEM (Security Information and Event Management, exemple : SPLUNK,…) et de requêtes corrélées (exemple : Elastic Search,…) sont identifiés à partir des exigences du cahier des charges client.
		□ Les logiciels de supervision et de création de requêtes corrélées sont installés, configurés et fonctionnels.
		□ Les requêtes d'analyse sont établies, validées par le chef de projet ou le responsable de lot, et sont fonctionnelles.
		□ Les critères d'alerte sont établis, validés par le chef de projet ou le responsable de lot, et sont fonctionnelles.
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.	□ Les réunions de sensibilisation sont planifiées et organisées avec les bons interlocuteurs, et validées par le chef de projet.
		□ Les supports de sensibilisation à l'hygiène informatique (Powerpoint, mémento, films, etc.) 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.
		□ Les sessions de sensibilisation sont réalisées : • systématiquement pour les nouveaux arrivants au sein de l'entreprise ou de l'organisation ; • et 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. CONDITIONS D'ADMISSIBILITE

Les CQPM, ou les blocs de compétences pour les CQPM inscrits au RNCP, sont attribués aux candidats[2] sous le contrôle du groupe technique paritaire « Qualifications », à l'issue des actions d'évaluation, et dès lors que toutes les capacités professionnelles ont été acquises et validées par le jury paritaire de délibération, au regard des critères observables et/ou mesurables d'évaluation.

4. MODALITES D'EVALUATION

4.1. 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 d'examen.

- L'UIMM territoriale centre d'examen et l'entreprise ou à défaut le candidat (VAE, demandeurs d'emploi…) définissent dans un dossier qui sera transmis à l'UIMM centre de ressources, 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. Dans les cas exceptionnels où il est impossible de mettre en œuvre cette modalité d'évaluation et lorsque cela est prévu dans le référentiel de certification, des évaluations en situation professionnelle reconstituée pourront être mises en œuvre.

4.2. Mise en œuvre des modalités d'évaluation

A) Validation des capacités professionnelles

L'évaluation des capacités professionnelles est assurée par la commission d'évaluation. Cette évaluation sera complétée par l'avis de l'entreprise (hors dispositif VAE).

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

B) Définition des différentes modalités d'évaluation

a) Evaluation en situation professionnelle réelle

L'évaluation des capacités professionnelles s'effectue dans le cadre d'activités professionnelles réelles. Cette évaluation s'appuie sur :

- une observation en situation de travail
- des questionnements avec apport d'éléments de preuve par le candidat

b) Présentation des projets ou activités réalisés en milieu professionnel

Le candidat transmet un rapport à l'UIMM territoriale centre d'examen, dans les délais et conditions préalablement fixés, afin de montrer que les capacités 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.

c) Evaluation à partir d'une situation professionnelle reconstituée

L'évaluation des capacités professionnelles s'effectue dans des conditions représentatives d'une situation réelle d'entreprise :

- par observation avec questionnements

Ou

- avec une restitution écrite et/ou orale par le candidat

d) Avis de l'entreprise

L'entreprise (tuteur, responsable hiérarchique ou fonctionnel…) donne un avis en regard des capacités professionnelles du référentiel de certification sur les éléments mis en œuvre par le candidat lors de la réalisation de projets ou activités professionnels.