Le Répertoire National des Certifications Professionnelles (RNCP)

Résumé descriptif de la certification **Code RNCP : 28248**

Intitulé

CQP : Certificat de qualification professionnelle Préventeur(trice) en cybersécurité des systèmes d'informations (CQPM)

AUTORITÉ RESPONSABLE DE LA CERTIFICATION	QUALITÉ DU(ES) SIGNATAIRE(S) DE LA CERTIFICATION
Commission paritaire nationale de l'emploi (CPNE) de la métallurgie – Union des industries et métiers de la métallurgie (UIMM)	Directeur emploi formation de l'UIMM

Niveau et/ou domaine d'activité

Convention(s) :

3109 - Métallurgie

Code(s) NSF :

326m Informatique, traitement de l'information

Formacode(s) :

Résumé du référentiel d'emploi ou éléments de compétence acquis

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 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.

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

A1 la définition de l'architecture sécurisée d'un système d'information ;

A2 la prévention et l'intervention en cas d'incident de sécurité informatique ;

A3 le management et la supervision d'un système d'information.

Les capacités attestées :

CP1 Analyser un cahier des charges d'un système d'information

CP2 Élaborer la maquette du dossier d'architecture technique

CP3 Élaborer l'architecture d'un système d'information sécurisé

CP4 Définir un plan de reprise d'activités informatique

CP5 Auditer la sécurité du système d'information

CP6 Gérer un système d'information après compromission

CP7 Superviser le système d'information

CP8 Sensibiliser les utilisateurs du système d'information à l'hygiène informatique et aux risques liés à la cybersécurité

Secteurs d'activité ou types d'emplois accessibles par le détenteur de ce diplôme, ce titre ou ce certificat

Le (la) titulaire du CQPM 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).

Analyste en vulnérabilité de code logiciel

Expert ou experte en cybersécurité

Expert ou experte en sécurité des systèmes d'information

Expert ou experte en tests d'intrusion – sécurité des systèmes d'information

Expert ou experte en sécurité informatique

Codes des fiches ROME les plus proches :

M1802 : Expertise et support en systèmes d'information

Modalités d'accès à cette certification

Descriptif des composantes de la certification :

Les CQPM sont accessibles soit à l'issue de parcours de formation professionnelle, soit à l'issue d'actions de validation des acquis de l'expérience (VAE). Le référentiel du CQPM est constitué de plusieurs capacités professionnelles indépendantes les unes des autres. Toutes les capacités professionnelles doivent être validées pour que le CQPM soit délivré.

Dans le cadre d'un parcours de formation professionnelle, l'accès à la certification est constitué des étapes suivantes :

•- En amont, une phase d'inscription préalable, par l'intermédiaire d'une entreprise ou d'un organisme.

•- Une phase constitutive de l'évaluation.

L'UIMM territoriale centre d'examen définit les modalités d'évaluation en concertation avec l'entreprise et les acteurs concernés (organismes, candidats…). Les capacités professionnelles mentionnées dans le référentiel du CQPM sont évaluées par la commission d'évaluation à l'aide des critères, niveaux d'exigence et conditions d'évaluation définis par ce même référentiel. Une phase de jury paritaire de délibération qui vérifie que l'organisation des actions d'évaluation est conforme au dispositif paritaire et au référentiel du CQPM visé, examine le récapitulatif des évaluations mis à disposition par la commission d'évaluation et déclare admissibles ou non admissibles les candidats.

Dans le cadre d'une validation des acquis de l'expérience (VAE), l'accès à la certification est constitué des étapes suivantes :

•- En amont, une phase de recevabilité de la demande.

•- Une phase constitutive de la commission de validation : un entretien de validation, à l'appui d'un dossier de preuves préalablement constitué décrivant une ou plusieurs situations professionnelles succinctes en rapport avec les capacités professionnelles du CQPM visé.

•- Une phase de jury paritaire de délibération qui vérifie que l'organisation des actions d'évaluation est conforme au dispositif paritaire et au référentiel du CQPM visé, examine le récapitulatif des évaluations mis à disposition par la commission d'évaluation et déclare admissibles ou non admissibles les candidats.

Pour que le candidat soit déclaré admissible au CQPM par le jury paritaire de délibération l'ensemble des blocs de compétences doit être acquis.

Bloc de compétence :

INTITULÉ	DESCRIPTIF ET MODALITÉS D'ÉVALUATION
Bloc de compétence n°1 de la fiche n° 28248 - La définition de l'architecture sécurisée d'un système d'information	**Descriptif :** Ce bloc de compétences reprend les capacités professionnelles suivantes : CP1 Analyser un cahier des charges d'un système d'information CP2 Élaborer la maquette du dossier d'architecture technique CP3 Élaborer l'architecture d'un système d'information sécurisé **Modalités d'évaluation :** ***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. ***Ou*** ***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 de 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. ***Ou*** ***Evaluation à partir d'une situation professionnelle reconstituée :*** Si nécessaire, la commission d'évaluation pourra mettre en œuvre une évaluation en 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 restitution écrite et/ou orale par le candidat. ***Et*** ***Avis de l'entreprise :*** L'entreprise (tuteur, responsable fonctionnel ou hiérarchique...) donne un avis au regard du référentiel de certification (capacités professionnelles et/ou critères) sur les éléments mis en œuvre par le candidat lors de la réalisation de projets ou activités professionnels. **Attestation :** Chaque bloc est certifié, il donne lieu à une évaluation et une validation

INTITULÉ	DESCRIPTIF ET MODALITÉS D'ÉVALUATION
Bloc de compétence n°2 de la fiche n° 28248 - La prévention et intervention en cas d'incident de sécurité informatique	**Descriptif :** Ce bloc de compétences reprend les capacités professionnelles suivantes : CP4 Définir un plan de reprise d'activités informatique CP5 Auditer la sécurité du système d'information CP6 Gérer un système d'information après compromission **Modalités d'évaluation :** ***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. ***Ou*** ***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 de 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. ***Ou*** ***Evaluation à partir d'une situation professionnelle reconstituée :*** Si nécessaire, la commission d'évaluation pourra mettre en œuvre une évaluation en 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 restitution écrite et/ou orale par le candidat. ***Et*** ***Avis de l'entreprise :*** L'entreprise (tuteur, responsable fonctionnel ou hiérarchique...) donne un avis au regard du référentiel de certification (capacités professionnelles et/ou critères) sur les éléments mis en œuvre par le candidat lors de la réalisation de projets ou activités professionnels. **Attestation :** Chaque bloc est certifié, il donne lieu à une évaluation et une validation

INTITULÉ	DESCRIPTIF ET MODALITÉS D'ÉVALUATION
Bloc de compétence n°3 de la fiche n° 28248 - Le management et la supervision d'un système d'information	**Descriptif :** Ce bloc de compétences reprend la capacité professionnelle suivante : CP7 Superviser le système d'information CP8 Sensibiliser les utilisateurs du système d'information à l'hygiène informatique et aux risques liés à la cybersécurité **Modalités d'évaluation :** ***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. ***Ou*** ***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 de 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. ***Ou*** ***Evaluation à partir d'une situation professionnelle reconstituée :*** Si nécessaire, la commission d'évaluation pourra mettre en œuvre une évaluation en 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 restitution écrite et/ou orale par le candidat. ***Et*** ***Avis de l'entreprise :*** L'entreprise (tuteur, responsable fonctionnel ou hiérarchique...) donne un avis au regard du référentiel de certification (capacités professionnelles et/ou critères) sur les éléments mis en œuvre par le candidat lors de la réalisation de projets ou activités professionnels. **Attestation :** Chaque bloc est certifié, il donne lieu à une évaluation et une validation

Validité des composantes acquises : illimitée

CONDITIONS D'INSCRIPTION À LA CERTIFICATION	OUI	NON	COMPOSITION DES JURYS
Après un parcours de formation sous statut d'élève ou d'étudiant		X	
En contrat d'apprentissage		X	

Après un parcours de formation continue	X		Jury paritaire: 50% de représentants des salariés / 50% de représentants des employeurs. Délégation patronale : maximum de cinq membres qualifiés relevant de la branche de la métallurgie et, en tant que de besoin, un membre supplémentaire de la branche du travail temporaire. Délégation syndicale : chaque organisation syndicale représentative de salariés au niveau national dans la branche de la métallurgie désigne un ou plusieurs représentants qualifiés et, en tant que de besoin, un membre supplémentaire de la branche du travail temporaire. Seul un représentant par organisation syndicale siège dans le jury avec droit de vote. En cas de partage des voix, celle du président du jury est prépondérante.
En contrat de professionnalisation	X		Jury paritaire: 50% de représentants des salariés / 50% de représentants des employeurs. Délégation patronale : maximum de cinq membres qualifiés relevant de la branche de la métallurgie et, en tant que de besoin, un membre supplémentaire de la branche du travail temporaire. Délégation syndicale : chaque organisation syndicale représentative de salariés au niveau national dans la branche de la métallurgie désigne un ou plusieurs représentants qualifiés et, en tant que de besoin, un membre supplémentaire de la branche du travail temporaire. Seul un représentant par organisation syndicale siège dans le jury avec droit de vote. En cas de partage des voix, celle du président du jury est prépondérante.
Par candidature individuelle		X	
Par expérience dispositif VAE prévu en 2007	X		Jury paritaire: 50% de représentants des salariés / 50% de représentants des employeurs. Délégation patronale : maximum de cinq membres qualifiés relevant de la branche de la métallurgie et, en tant que de besoin, un membre supplémentaire de la branche du travail temporaire. Délégation syndicale : chaque organisation syndicale représentative de salariés au niveau national dans la branche de la métallurgie désigne un ou plusieurs représentants qualifiés et, en tant que de besoin, un membre supplémentaire de la branche du travail temporaire. Seul un représentant par organisation syndicale siège dans le jury avec droit de vote. En cas de partage des voix, celle du président du jury est prépondérante.

	OUI	NON
Accessible en Nouvelle Calédonie		X
Accessible en Polynésie Française		X

LIENS AVEC D'AUTRES CERTIFICATIONS **ACCORDS EUROPÉENS OU INTERNATIONAUX**

Base légale

Référence du décret général :

Référence arrêté création (ou date 1er arrêté enregistrement) :

Arrêté du 07 avril 2017 publié au Journal Officiel du 21 avril 2017 portant enregistrement au répertoire national des certifications

professionnelles. Enregistrement pour cinq ans, sous l'intitulé "Certificat de qualification professionnelle Préventeur(trice) en cybersécurité des systèmes d'informations (CQPM)" avec effet au 21 avril 2017, jusqu'au 21 avril 2022.

Référence du décret et/ou arrêté VAE :

Références autres :

Pour plus d'informations

Statistiques :

Ce CQPM vient d'être créé, il n'y a donc pas de statistique.

Autres sources d'information :

http://cqpm.fr

https://uimm.fr/

Le site de la CPNE métallurgie sur les CQPM

Lieu(x) de certification :

Union des industries et métiers de la métallurgie (UIMM) - 56, avenue de Wagram - 75017 Paris

Lieu(x) de préparation à la certification déclarés par l'organisme certificateur :

Se renseigner auprès des UIMM territoriales : annuaire des Chambres syndicales territoriales : https://uimm.fr/adherer/annuaire-chambres-syndicales-territoriales/

Historique de la certification :

La création du CQPM Préventeur en cybersécurité des systèmes d'informations a été validée le 02/04/2015. C'est sur la base d'une analyse du besoin des entreprises de son territoire que le Groupe des Industries Métallurgiques de la Région Parisienne à procéder à l'étude d'opportunité de création d'une qualification répondant à ce besoin de certification.