

CQP Préventeur(trice) en cybersécurité des systèmes d'informations (CQPM)

RNCP28248 · RNCP · Publiée

L'essentiel

Niveau de qualification	Sans niveau – le positionnement dans le cadre de national des certifications professionnelles est non déterminé
Code(s) NSF	326m
Formacode(s)	31006
Code(s) ROME	M1802
Type d'enregistrement	Enregistrement sur demande
Convention collective	3109 — Métallurgie
Date d'échéance	21/04/2022

Certificateur(s)

UNION DES INDUSTRIES ET DES METIERS DE LA METALLURGIE (UIMM) · SIRET : 78471719100018

Commission paritaire nationale de l'emploi (CPNE) de la métallurgie – Union des industries et métiers de la métallurgie (UIMM)

<http://www.uimm.fr>

Partenaires habilités

63 organismes habilités, d'après la liste publiée par France compétences : 63 à former et organiser l'évaluation.

Organisme	SIRET	Habilitation
AFOREST	34317059300101	Former et organiser l'évaluation
AFOREST	34317059300119	Former et organiser l'évaluation
AFOREST	34317059300135	Former et organiser l'évaluation
AFOREST	34317059300150	Former et organiser l'évaluation
AFORP FORMATION (CFAI)	77572845400205	Former et organiser l'évaluation
AFPI CENTRE VAL DE LOIRE	77518765100069	Former et organiser l'évaluation
AFPI CENTRE VAL DE LOIRE	77518765100077	Former et organiser l'évaluation
AFPI CENTRE VAL DE LOIRE	77518765100085	Former et organiser l'évaluation
AFPI CENTRE VAL DE LOIRE	77518765100093	Former et organiser l'évaluation
AFPI EURE SEINE ESTUAIRE	78106280700032	Former et organiser l'évaluation

Liste complète des 63 partenaires habilités : <https://data.aktaconseil.fr/certifications/rncp28248-cqp-preventeur-trice-en-cybersecurite-des-systemes-d-informations-cqpm/partenaires>

Résumé de la certification

OBJECTIFS ET CONTEXTE

A compléter (Reprise)

ACTIVITÉS VISÉES

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.

COMPÉTENCES ATTESTÉES

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

Blocs de compétences

RNCP28248BC01 — La définition de l'architecture sécurisée d'un système d'information

LISTE DE COMPÉTENCES

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 :

Évaluation 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

RNCP28248BC02 — La prévention et intervention en cas d'incident de sécurité informatique

LISTE DE COMPÉTENCES

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

RNCP28248BC03 — Le management et la supervision d'un système d'information

LISTE DE COMPÉTENCES

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 :

Évaluation 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

Évaluation 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

Secteur d'activité et type d'emploi

SECTEURS D'ACTIVITÉS

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).

TYPE D'EMPLOIS ACCESSIBLES

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

RÈGLEMENTATIONS D'ACTIVITÉ

A compléter (Reprise)

Marché du travail

Indicateurs au niveau des familles professionnelles (FAP) des métiers visés, agrégés au niveau national — France Travail / DARES (open data).

Tension de recrutement (DARES 2024)	Très élevée (5/5)
Facteurs principaux	Lien formation-emploi, Manque de main-d'œuvre disponible
Salaire médian (mensuel)	3 115 €
Diplôme le plus fréquent	Diplôme de niveau bac+5 ou plus (doctorat, master ou équivalent) en communication et information (35 % des actifs en emploi)
Familles professionnelles (FAP)	M2X93 — Experts et consultants en systèmes d'information · tension 5/5 (Très élevée)
Projets de recrutement (BMO 2026)	4 758
Jugés difficiles à recruter	45 %
Emplois saisonniers	0 %
Familles professionnelles (FAP)	M2X93 — Experts et consultants en systèmes d'information

Voies d'accès

MODALITÉS D'ACCÈS

Formation continue, Contrat de professionnalisation, VAE

PRÉREQUIS À L'ENTRÉE EN FORMATION

A compléter (Reprise)

COMPOSITION DU JURY — FORMATION CONTINUE, CONTRAT DE PROFESSIONNALISATION, VAE

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.

Base légale

Date d'échéance de l'enregistrement	21/04/2022
-------------------------------------	------------

Pour plus d'informations

LIEN VERS LE DESCRIPTIF

<http://cqpm.fr>

<https://uimm.fr/>

Le site de la CPNE métallurgie sur les CQPM

Fiche officielle (France Compétences)

