

Expert en cybersécurité industrielle

RNCP36586 · RNCP · Publiée

L'essentiel

Niveau de qualification	Niveau 7
Code(s) NSF	326
Formacode(s)	31081, 31045, 24220, 31094, 31038
Code(s) ROME	M1802, M1810, M1801, M1805, M1806
Type d'enregistrement	Enregistrement sur demande
Date d'enregistrement	01/07/2022
Date d'échéance	01/07/2025

Certificateur(s)

FONDATION LA MACHE · SIRET : 50215377800019

Partenaires habilités

1 organisme habilité, d'après la liste publiée par France compétences : 1 à former et organiser l'évaluation.

Organisme	SIRET	Habilitation
ELYSIUM SECURITY	82827112200032	Former et organiser l'évaluation

Résumé de la certification

OBJECTIFS ET CONTEXTE

Il y a une vingtaine d'années, les usines mettaient un point d'honneur à soigner le bon fonctionnement de leurs machines afin d'assurer la production de biens manufacturés, la production d'énergie, la pétrochimie ou encore le traitement de l'eau. Cette tâche revenait principalement aux automaticiens et aux informaticiens. Aujourd'hui, les préoccupations des acteurs industriels ont changé. Les installations sont désormais informatisées et interconnectées à des systèmes d'information. Internet se présente alors au cœur du processus de fabrication des usines en permettant une communication entre chaque maillon des chaînes de production et d'approvisionnement, des outils et postes de travail. Malgré une flexibilité de fabrication et une productivité accrue, les acteurs de l'industrie doivent maintenant faire face aux cyberattaques qui menacent continuellement la communication et le bon fonctionnement des plates-formes et logiciels. Ces actes malveillants peuvent aboutir à l'arrêt de la production de manière intempestive ou pire : à la destruction du système industriel visé. Plus qu'une contrainte, la cybersécurité industrielle s'impose de plus en plus aux acteurs de l'économie comme un atout de compétitivité. C'est d'ailleurs tout l'enjeu de la certification ISO 27000 relative au management de la politique de la sécurité des systèmes d'information que d'accréditer suite à des audits, les produits et solutions délivrées par les industriels. Cependant, et malgré la multiplication des attaques et le travail de pédagogie de l'ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information), beaucoup de PMI n'ont pas encore engagé une réelle politique de cybersécurité pour la protection de leurs systèmes industriels. Les raisons sont multiples ; parmi celles-ci, se trouve le manque de compétences. L'objectif de la certification est de qualifier des chefs de projets spécialistes de haut niveau dans le domaine de la cybersécurité industrielle.

ACTIVITÉS VISÉES

Spécialiste en sécurité informatique, l'expert en cybersécurité industrielle est capable d'intervenir sur les systèmes d'information industriels pour en assurer la protection. Sa connaissance du fonctionnement de ce type d'architecture et des risques spécifiques auxquels les composants (SCADA, PLC, etc.) sont exposés constitue un atout

indispensable à la sécurité des chaînes de production industrielle qui, parce qu'elles sont souvent critiques et de plus en plus exposées, sont devenues une cible privilégiée. Les activités visées par la certification :

A1. Conception de la politique de cybersécurité du système d'information industriel

A1T1 : Analyse des besoins de la structure et du S.I. existant

A1T2 : Analyse de risques et définition de la politique de sécurité

A1T3 : Accompagnement à l'élaboration d'un système de management de la sécurité

A1T4 : Veille technologique et réglementaire en sécurité des systèmes industriels

A2. Conception et planification du projet de cybersécurité industrielle interne en lien avec la stratégie définie

A2T1 : Planification et séquençage du projet de cybersécurité industrielle

A2T2 : Investigation et traitement des incidents de sécurité

A2T3 : Management d'équipe interne et externe à l'entreprise

A3. Pilotage de la cybersécurité et déploiement de l'architecture fonctionnelle et technique

A3T1 : Gestion de l'architecture fonctionnelle de cybersécurité industrielle

A3T2 : Déploiement d'une Architecture technique de sécurité

A3T3 : Gestion de crise cyber

A4. Audit de la sécurité du système d'information et mise en place d'actions préventives en matière de cybersécurité

A4T1 : Audit de la sécurité du système d'information

A4T2 : Formation des collaborateurs

A4T3 : Processus d'amélioration des capacités de défense et de réactions

COMPÉTENCES ATTESTÉES

Les compétences visées par la certification :

B1C1 : Analyser les besoins en cybersécurité des systèmes industriels à l'aide de la description des processus de l'entreprise et d'analyses afin d'appliquer les bonnes pratiques pour la sécurité du système d'information.

B1C2 : Définir un plan d'audit adapté en termes de moyens, ressources, organisation et contraintes réglementaires afin de déterminer précisément les failles et non conformités du système d'information.

B1C3 : Analyser les écarts au regard des référentiels, processus et procédures définis au plan d'audit afin de mettre en place un plan d'actions correctives et/ou préventives pour améliorer la sécurité du système d'information.

B1C4 : Établir un plan d'action comportant les mesures techniques et organisationnelles pour corriger les non conformités afin de remédier efficacement aux failles de sécurité et non conformités en mettant en place d'une stratégie adaptée aux besoins de l'entreprise.

B2C1 : Superviser la sécurité des systèmes industriels en mettant en place des outils logiciels adéquats afin d'établir une surveillance la plus complète et à jour possible de la sécurité du système d'information.

B2C2 : Évaluer les risques de sécurité spécifiques aux environnements industriels en les identifiant à l'aide de méthodes adaptées à l'environnement et aux moyens de l'entreprise afin de préparer des mesures de réduction de l'impact lié à ces risques.

B2C3 : Évaluer les vulnérabilités des systèmes informatiques et informatiques industriels à l'aide d'outils spécifiques afin de déterminer le niveau de criticité attribué à chaque vulnérabilité détectée.

B2C4 : Détecter les alertes de sécurité à l'aide de la mise en place d'outils et services du système de gestion des événements de la sécurité afin de tenter de détecter les activités suspectes et d'atténuer les menaces.

B2C5 :

Gérer des mesures de contournements et/ou un plan de remédiation en s'appuyant sur des solutions techniques précédemment identifiées afin de pallier à de nouvelles occurrences des incidents de sécurité.

B2C6 : Mener une investigation numérique à l'aide des outils de mesures adéquats en recherchant les causes racines afin de gérer les incidents de sécurité.

B2C7 : Assurer l'amélioration continue des dispositifs de sécurité au moyen d'indicateurs évalués en fonction d'objectifs à atteindre afin de maintenir un niveau de sécurité adapté et assurer la performance du processus de sécurisation de façon continue (ressources humaines et outils de l'entreprise)

B2C8 : Définir les modalités de gestion de crise en mobilisant les ressources techniques et humaines afin d'améliorer les capacités de défense et de réaction de la structure.

B2C9 : Assurer la communication de crise en formalisant le processus de réponse aux incidents de sécurité afin d'informer efficacement les parties concernées internes et externes et contribuer à limiter les effets néfastes pour l'entreprise.

B3C1 :

Analyser les contraintes fonctionnelles et/ou organisationnelles des systèmes industriels afin d'intégrer les contraintes

spécifiques de ces systèmes à la politique de sécurité.

B3C2 : Collecter les informations auprès des directions métiers, des services qualité afin d'alimenter des processus de la sécurité informatique et informatique industrielle en cohérence avec les processus et besoins métiers de l'entreprise.

B3C3 : Définir la politique de sécurité de l'entreprise à l'aide des différents acteurs et en tenant compte des contraintes internes et externes afin de maximiser la sécurité informatique

B3C4 : Définir la stratégie de sécurité des systèmes d'information industriels à l'aide des différentes analyses d'enjeux, objectifs, procédures existantes afin de s'aligner avec la stratégie de l'entreprise et assurer la sécurité du capital informationnel.

B3C5 : Assurer la continuité d'activité des systèmes industriels en concevant un plan de continuité et de reprise d'activité afin de limiter les effets d'incidents de sécurité sur le fonctionnement normal de l'entreprise.

B3C6 : Sensibiliser les acteurs et les utilisateurs à la cybersécurité à l'aide d'un plan de formation des équipes techniques et non techniques pour améliorer leur niveau de compréhension des problématiques de sécurité informatique et informatique industrielle.

B4C1 : Mettre en œuvre des solutions de correction ou de prévention en s'appuyant sur les standards de la sécurité afin de garantir un niveau adapté de sécurité du système d'informations.

B4C2 : Concevoir une architecture sécurisée système et réseau d'un système d'information industriel à l'aide des bonnes pratiques, de tests, de mesures, d'outils techniques au niveau réseau et système afin d'aligner les infrastructures aux besoins et à la stratégie de sécurité de l'entreprise.

B4C3 : Concevoir une architecture sécurisée applicative et de données d'un système d'information industriel à l'aide des bonnes pratiques, de tests, de mesures, d'outils techniques au niveau applicatif et données afin d'aligner les infrastructures aux besoins et à la stratégie de sécurité de l'entreprise.

B4C4 : Concevoir des solutions techniques adaptées aux contraintes et spécificités des systèmes industriels afin de sécuriser les infrastructures en tenant compte des environnements des entreprises industrielles.

B4C5 : Intégrer des solutions de cybersécurité pour l'infrastructure informatique et l'informatique industrielle afin de mettre en œuvre une architecture sécurisée du système d'information de l'organisation.

B4C6 : Administrer les solutions de cybersécurité du système d'information industriel à l'aide des éléments de la politique de sécurité de l'entreprise afin d'assurer le fonctionnement opérationnel des systèmes vitaux de l'organisation.

B5C1 : Gérer les différents outils collaboratifs nécessaires à la collaboration et au partage d'informations afin d'assurer la bonne diffusion des informations liées à la sécurité du capital informationnel de l'entreprise auprès de l'ensemble des collaborateurs, nourrir les profils compétences des collaborateurs et ainsi contribuer à la capitalisation des compétences.

B5C2 : Organiser les interventions des équipes à l'aide d'outils et méthodes appropriées de gestion de projets et techniques de communication afin d'améliorer la coordination des différentes composantes opérationnelles et décisionnelles de l'entreprise.

B5C3 : Gérer les ressources nécessaires à la sécurité des systèmes d'information industriels à l'aide des procédures de sécurité afin d'optimiser la sécurité et de contribuer au pilotage de l'entreprise.

B5C4 : Assurer la communication interne et externe en matière de sécurité de l'information à l'aide des outils dont l'entreprise est équipée, de plans de communication, de rapports d'activités afin d'atteindre la bonne application des mesures et prévenir les pratiques inadéquates en matière de sécurité des systèmes d'information.

B5C5 : Assurer une veille technique en utilisant les outils adaptés afin d'alimenter une base de ressources sur l'évolution des menaces et les méthodes utilisées ainsi que de leurs effets potentiels.

B5C6 : Mener des actions de veille réglementaire en utilisant les outils adaptés afin de garantir un niveau de sécurité du système d'information conforme aux exigences associées.

Blocs de compétences

RNCP36586BC01 — Auditer la sécurité des systèmes d'informations et des systèmes industriels

LISTE DE COMPÉTENCES

B1C1 : Analyser les besoins en cybersécurité des systèmes industriels à l'aide de la description des processus de l'entreprise et d'analyses afin d'appliquer les bonnes pratiques pour la sécurité du système d'information.

B1C2 : Définir un plan d'audit adapté en termes de moyens, ressources, organisation et contraintes réglementaires afin de déterminer précisément les failles et non conformités du système d'information.

B1C3 : Analyser les écarts au regard des référentiels, processus et procédures définis au plan d'audit afin de mettre en place un plan d'actions correctives et/ou préventives pour améliorer la sécurité du système d'information.

B1C4 : Établir un plan d'action comportant les mesures techniques et organisationnelles pour corriger les non conformités afin de remédier efficacement aux failles de sécurité et non conformités en mettant en place une stratégie adaptée aux besoins de l'entreprise.

MODALITÉS D'ÉVALUATION

Rapport écrit :

A partir d'une étude de cas fournie sous forme d'un cahier des charges présentant le besoin d'une entreprise fictive, le candidat sera chargé de la réalisation d'un audit de sécurité d'un système d'information industriel.

Le candidat sera chargé de rédiger un rapport d'audit contenant les éléments suivants :

- La note de cadrage de l'audit ;
- Le champ de l'audit ;
- La méthodologie d'audit ;
- La synthèse des résultats de l'audit
- Le détail des résultats de l'audit (liste des contrôles effectués, identification des bonnes pratiques)
- La matrice des risques ;
- Le plan d'action proposé ;
- L'état de maturité de la sécurité du système d'information

Le rapport sera rédigé en français et présentera une structure organisée avec un sommaire. Au rapport sera associée d'une synthèse soutenue à l'oral d'une durée de 30 minutes.

RNCP36586BC02 — Assurer la gestion opérationnelle de la cybersécurité du système d'information et des systèmes industriels

LISTE DE COMPÉTENCES

B2C1 : Superviser la sécurité des systèmes industriels en mettant en place des outils logiciels adéquats afin d'établir une surveillance la plus complète et à jour possible de la sécurité du système d'information.

B2C2 : Évaluer les risques de sécurité spécifiques aux environnements industriels en les identifiant à l'aide de méthodes adaptées à l'environnement et aux moyens de l'entreprise afin de préparer des mesures de réduction de l'impact lié à ces risques.

B2C3 : Évaluer les vulnérabilités des systèmes informatiques et informatiques industriels à l'aide d'outils spécifiques afin de déterminer le niveau de criticité attribué à chaque vulnérabilité détectée.

B2C4 : Détecter les alertes de sécurité à l'aide de la mise en place d'outils et services du système de gestion des événements de la sécurité afin de tenter de détecter les activités suspectes et d'atténuer les menaces.

B2C5 :

Gérer des mesures de contournements et/ou un plan de remédiation en s'appuyant sur des solutions techniques précédemment identifiées afin de pallier à de nouvelles occurrences des incidents de sécurité.

B2C6 : Mener une investigation numérique à l'aide des outils de mesures adéquats en recherchant les causes racines afin de gérer les incidents de sécurité.

B2C7 : Assurer l'amélioration continue des dispositifs de sécurité au moyen d'indicateurs évalués en fonction d'objectifs à atteindre afin de maintenir un niveau de sécurité adapté et assurer la performance du processus de sécurisation de façon continue (ressources humaines et outils de l'entreprise)

B2C8 : Définir les modalités de gestion de crise en mobilisant les ressources techniques et humaines afin d'améliorer les capacités de défense et de réaction de la structure.

B2C9 : Assurer la communication de crise en formalisant le processus de réponse aux incidents de sécurité afin d'informer efficacement les parties concernées internes et externes et contribuer à limiter les effets néfastes pour l'entreprise.

MODALITÉS D'ÉVALUATION

Rapport écrit :

A partir d'une étude de cas fournie sous forme d'un cahier des charges présentant le besoin d'une entreprise fictive, portant sur la mise en application de concepts de gestion des risques et des vulnérabilités au sein d'un système industriel. Le candidat sera chargé d'établir un rapport d'analyse des risques et des vulnérabilités contenant les éléments suivants :

- Identification des scénarios pris en compte
- Dresser la liste des risques
- Dresser la liste des vulnérabilités

- Règles de surveillance du système de supervision
- Plan de remédiation

Le rapport sera rédigé en français et présentera une structure organisée avec un sommaire.

Mise en situation professionnelle reconstituée :

Évaluation des compétences à partir d'une mise en situation réelle de travail portant sur la réalisation d'une investigation numérique réalisée sur l'environnement Root-Me PRO (environnements non simulés proposant des challenges). À partir d'un scénario proposé sur la plateforme, le candidat réalise différentes analyses à partir des traces disponibles sur un système compromis.

Présentation orale :

À partir d'une étude de cas fournie sous forme d'un cahier des charges présentant le besoin d'une entreprise fictive, le candidat sera chargé de créer un tableau de bord composé d'indicateurs de sécurité informatique. Le candidat argumente le contenu de son tableau de bord par une présentation à l'oral de 10 minutes.

Conception et présentation d'un plan de gestion :

À partir d'une étude de cas fournie sous forme d'un cahier des charges présentant le besoin d'une entreprise fictive, le candidat prépare un plan de gestion de crise contenant :

- Propositions de stratégie de gestion de crise
- Fiches réflexes
- Plan de communication par type de parties concernées

Le candidat présentera son plan de gestion de crise lors d'un exercice de présentation orale de 20 minutes.

RNCP36586BC03 — Conseiller la structure en cybersécurité et organiser sa mise en œuvre

LISTE DE COMPÉTENCES

B3C1 :

Analyser les contraintes fonctionnelles et/ou organisationnelles des systèmes industriels afin d'intégrer les contraintes spécifiques de ces systèmes à la politique de sécurité.

B3C2 : Collecter les informations auprès des directions métiers, des services qualité afin d'alimenter des processus de la sécurité informatique et informatique industrielle en cohérence avec les processus et besoins métiers de l'entreprise.

B3C3 : Définir la politique de sécurité de l'entreprise à l'aide des différents acteurs et en tenant compte des contraintes internes et externes afin de maximiser la sécurité informatique

B3C4 : Définir la stratégie de sécurité des systèmes d'information industriels à l'aide des différentes analyses d'enjeux, objectifs, procédures existantes afin de s'aligner avec la stratégie de l'entreprise et assurer la sécurité du capital informationnel.

B3C5 : Assurer la continuité d'activité des systèmes industriels en concevant un plan de continuité et de reprise d'activité afin de limiter les effets d'incidents de sécurité sur le fonctionnement normal de l'entreprise.

B3C6 : Sensibiliser les acteurs et les utilisateurs à la cybersécurité à l'aide d'un plan de formation des équipes techniques et non techniques pour améliorer leur niveau de compréhension des problématiques de sécurité informatique et informatique industrielle.

MODALITÉS D'ÉVALUATION

Rédaction de document :

À partir d'une étude de cas fournie sous forme d'un cahier des charges présentant le besoin d'une entreprise fictive, le candidat sera chargé de rédiger une politique de sécurité des systèmes d'information contenant les éléments suivants :

- Analyse des contraintes métiers et réglementaires
- Liste des besoins de sécurité pour la protection de son patrimoine numérique
- Adaptation des processus de sécurité aux menaces et contraintes listées

Le document sera rédigé en anglais.

Rédaction de document :

À partir d'une étude de cas fournie sous forme d'un cahier des charges présentant le besoin d'une entreprise fictive portant sur la mise en application de la stratégie de gouvernance de la sécurité des systèmes d'information, le candidat sera chargé de rédiger un document présentant la stratégie de sécurité des systèmes d'information contenant les éléments suivants :

- Synthèse des analyses techniques et métiers
- Définition de la cible à atteindre
- Liste des projets à réaliser ordonnés dans le temps pour atteindre la cible

Rapport écrit :

A partir d'une étude de cas fournie sous forme d'un cahier des charges présentant le besoin d'une entreprise fictive portant sur la mise en œuvre de plan de continuité et de reprise d'activité, le candidat sera chargé de rédiger une proposition de plan de continuité d'activité contenant :

- Liste des activités essentielles à la continuité d'activité de l'entreprise.
- Choix argumenté du périmètre fonctionnel du plan
- Une matrice d'analyse de risques avec calcul argumenté de la criticité
- La définition des solutions de secours
- Les seuils de déclenchement du plan
- Une procédure de secours informatique
- Le plan de test du PCA

Le rapport sera rédigé en français et présentera une structure organisée avec un sommaire.

Présentation orale :

A partir d'une étude de cas fournie sous forme d'un cahier des charges présentant le besoin d'une entreprise fictive portant sur les actions de formation et de communication de sécurité informatique, le candidat sera chargé de présenter un plan d'actions de sensibilisation du personnel :

- Liste des actions de sensibilisation
- Liste des actions de formation
- Parties prenantes
- Ressources à mettre en œuvre
- Planning de réalisation, fréquence
- Objectifs attendus

Le candidat résume son plan dans une présentation orale de 20 minutes.

RNCP36586BC04 — Assurer la mise en œuvre des solutions en cybersécurité technique des systèmes d'informations et systèmes industriels

LISTE DE COMPÉTENCES

B4C1 : Mettre en œuvre des solutions de correction ou de prévention en s'appuyant sur les standards de la sécurité afin de garantir un niveau adapté de sécurité du système d'informations.

B4C2 : Concevoir une architecture sécurisée système et réseau d'un système d'information industriel à l'aide des bonnes pratiques, de tests, de mesures, d'outils techniques au niveau réseau et système afin d'aligner les infrastructures aux besoins et à la stratégie de sécurité de l'entreprise.

B4C3 : Concevoir une architecture sécurisée applicative et de données d'un système d'information industriel à l'aide des bonnes pratiques, de tests, de mesures, d'outils techniques au niveau applicatif et données afin d'aligner les infrastructures aux besoins et à la stratégie de sécurité de l'entreprise.

B4C4 : Concevoir des solutions techniques adaptées aux contraintes et spécificités des systèmes industriels afin de sécuriser les infrastructures en tenant compte des environnements des entreprises industrielles.

B4C5 : Intégrer des solutions de cybersécurité pour l'infrastructure informatique et l'informatique industrielle afin de mettre en œuvre une architecture sécurisée du système d'information de l'organisation.

B4C6 : Administrer les solutions de cybersécurité du système d'information industriel à l'aide des éléments de la politique de sécurité de l'entreprise afin d'assurer le fonctionnement opérationnel des systèmes vitaux de l'organisation.

MODALITÉS D'ÉVALUATION

Mise en situation professionnelle reconstituée :

Évaluation des compétences à partir d'une mise en situation réelle de travail s'appuyant sur un environnement technique vulnérable à protéger et d'une description associée. Le candidat sera chargé de réaliser une maquette fonctionnelle d'une solution de correction ou de prévention sur l'environnement technique étudié (sous forme de machines virtuelles).

Mise en situation professionnelle reconstituée :

Évaluation des compétences à partir d'une mise en situation réelle de travail portant sur la réalisation d'exploitation de vulnérabilités sur l'environnement Root-Me PRO (environnements non simulés proposant des challenges). A partir d'un scénario proposé sur la plateforme, le candidat réalise différentes analyses et exploitations afin de prendre le contrôle de l'environnement.

Mise en situation professionnelle reconstituée :

Évaluation des compétences à partir d'une mise en situation réelle de travail s'appuyant sur un environnement

technique vulnérable à protéger et d'une description associée. Le candidat sera chargé de réaliser une maquette fonctionnelle d'outils de sécurité pour le renforcement d'une architecture informatique vulnérable (sous forme de machines virtuelles).

Questionnaire à choix multiples :

Évaluation de compétences sous forme de test se présentant sous la forme d'une question/affirmation suivie de plusieurs propositions de réponses, parmi lesquelles se trouve(nt) une ou plusieurs réponse(s) correcte(s). Ce questionnaire est composé de questions autour des manipulations permettant de vérifier des compétences d'administration conformes des principales solutions informatiques de sécurité.

RNCP36586BC05 — Piloter la cybersécurité du système d'informations et des systèmes industriels

LISTE DE COMPÉTENCES

B5C1 : Gérer les différents outils collaboratifs nécessaires à la collaboration et au partage d'informations afin d'assurer la bonne diffusion des informations liées à la sécurité du capital informationnel de l'entreprise auprès de l'ensemble des collaborateurs, nourrir les profils compétences des collaborateurs et ainsi contribuer à la capitalisation des compétences.

B5C2 : Organiser les interventions des équipes à l'aide d'outils et méthodes appropriées de gestion de projets et techniques de communication afin d'améliorer la coordination des différentes composantes opérationnelles et décisionnelles de l'entreprise.

B5C3 : Gérer les ressources nécessaires à la sécurité des systèmes d'information industriels à l'aide des procédures de sécurité afin d'optimiser la sécurité et de contribuer au pilotage de l'entreprise.

B5C4 : Assurer la communication interne et externe en matière de sécurité de l'information à l'aide des outils dont l'entreprise est équipée, de plans de communication, de rapports d'activités afin d'atteindre la bonne application des mesures et prévenir les pratiques inadaptées en matière de sécurité des systèmes d'information.

B5C5 : Assurer une veille technique en utilisant les outils adaptés afin d'alimenter une base de ressources sur l'évolution des menaces et les méthodes utilisées ainsi que de leurs effets potentiels.

B5C6 : Mener des actions de veille réglementaire en utilisant les outils adaptés afin de garantir un niveau de sécurité du système d'information conforme aux exigences associées.

MODALITÉS D'ÉVALUATION

Mise en situation professionnelle reconstituée :

Évaluation des compétences à partir d'une mise en situation réelle de travail à partir d'un cahier des charges présentant le besoin d'une entreprise fictive portant sur la mise en œuvre d'outils collaboratifs. Le candidat conçoit une maquette fonctionnelle permettant de gérer et sécuriser l'accès à différents outils collaboratifs contenant à minima :

- Un jeu de métadonnées pour caractériser les données
- Un système de gestion des documents
- Un système de gestion des projets
- Un système de communication interne
- Un système de support et d'assistance semi-automatisée

Mise en situation professionnelle reconstituée :

Évaluation des compétences à partir d'une mise en situation réelle de travail s'appuyant sur un environnement technique à déployer pour l'industrialisation du processus de veille technique. Le candidat sera chargé de réaliser une maquette fonctionnelle d'une plateforme technique choisie parmi les solutions open source du marché (sous forme de machines virtuelles).

Rapport écrit :

A partir d'une étude de cas fournie sous forme d'un cahier des charges présentant le besoin d'une entreprise fictive, le candidat présente un rapport de veille réglementaire en lien avec le contexte présenté et conforme aux exigences légales et réglementaires.

- Éléments réglementaires en lien avec l'activité du cas présenté.
- Éléments de protection des données personnelles si besoin est

Le rapport sera rédigé en français et présentera une structure organisée avec un sommaire.

Secteur d'activité et type d'emploi

SECTEURS D'ACTIVITÉS

- Informatique
- Informatique industrielle

TYPE D'EMPLOIS ACCESSIBLES

- Responsable de la Sécurité des Systèmes d'information (RSSI)
- Architecte SSI(I)
- Conseiller en SSI(I) auprès de décideurs
- Expert en investigation numérique
- Analyste N2/N3 dans un SOC (Security Operation Center)
- Expert en sécurité des IOT
- Ingénieur sécurité et cryptographie – Industrial IOT

RÈGLEMENTATIONS D'ACTIVITÉ

Non concerné.

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)	Élevée (4/5) Moyenne pondérée par l'emploi ; les familles ci-dessous s'échelonnent de 3 à 5 sur 5.
Facteurs principaux	Manque de main-d'œuvre disponible, Lien formation-emploi
Salaire médian (mensuel)	2 781 €
Diplôme le plus fréquent	Diplôme de niveau bac+5 ou plus (doctorat, master ou équivalent) en communication et information (41 % des actifs en emploi)
Familles professionnelles (FAP)	M1X80 — Techniciens d'étude et de développement en informatique · tension 4/5 (Élevée) M1X81 — Techniciens de production, d'exploitation, d'installation, et de maintenance, support et services aux utilisateurs en informatique · tension 4/5 (Élevée) M2X90 — Ingénieurs et cadres d'étude, recherche et développement en informatique et télécom · tension 5/5 (Très élevée) M2X92 — Responsables et cadres de la production, de l'exploitation et de la maintenance informatique et télécom · tension 3/5 (Modérée) M2X93 — Experts et consultants en systèmes d'information · tension 5/5 (Très élevée)
Projets de recrutement (BMO 2026)	41 765
Jugés difficiles à recruter	50 %
Emplois saisonniers	2 %
Familles professionnelles (FAP)	M1X80 — Techniciens d'étude et de développement en informatique M1X81 — Techniciens de production, d'exploitation, d'installation, et de maintenance, support et services aux utilisateurs en informatique M2X90 — Ingénieurs et cadres d'étude, recherche et développement en informatique et télécom M2X92 — Responsables et cadres de la production, de l'exploitation et de la maintenance informatique et télécom M2X93 — Experts et consultants en systèmes d'information

Voies d'accès

PRÉREQUIS À L'ENTRÉE EN FORMATION

Étudiants, salariés ou demandeurs d'emploi, chaque candidat au cursus complet et donc à la certification devra être titulaire ou en cours de validation d'une certification professionnelle de niveau 6 enregistrée au Répertoire National

des Certifications Professionnelles (RNCP) dans le domaine de l'Informatique ou de l'automatisme et informatique industrielle. Les voies d'accès sont par exemple un titre professionnel « Responsable de Projets Informatiques », une licence générale (licence générale informatique spécialisation « développement » ou « cybersécurité » du CNAM). A titre dérogatoire, les candidats en possession d'une expérience professionnelle probante (minimum 2 ans d'expérience dans le domaine de la cybersécurité) peuvent accéder à la certification.

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

Le jury est composé de :

- Quatre personnes externes au centre de formation, salariés ou chefs d'entreprises dans le domaine de l'informatique ou domaine proche, exerçant depuis plusieurs années ou ayant exercé pendant plusieurs années des fonctions dans le domaine d'activité.
- Deux personnes internes au centre de formation : un responsable formation ainsi qu'un responsable pédagogique ou un membre de la direction de l'établissement.

66% sont des membres extérieurs à l'autorité délivrant la certification. Ce sont des représentants de la profession :

- 50% sont des représentants des employeurs.
- 50% sont des représentants des salariés.

Financement en alternance (NPEC)

Niveau de prise en charge d'un contrat d'apprentissage par les OPCO, fixé par France compétences par branche professionnelle (CPNE).

Prise en charge usuelle	9 384 €
Selon la branche	7 697 € – 9 785 €
Prise en charge	Branches concernées
9 384 €	Valeur par défaut · 203 branches
9 785 €	CPNE autoroutes, CPNE de l'ingénierie, des services informatiques et du conseil, CPNE des industries de santé (CPNEIS), CPNEF de l'audiovisuel, CPNEFP des commerces de gros
9 000 €	CPNE chimie, CPNEFP des industries des tuiles et briques
8 696 €	CPNEFP Import-Export
8 500 €	CPNEFP de la métallurgie
7 697 €	CPNEFP de la blanchisserie, laverie, location de linge, nettoyage à sec, pressing et teinturerie

Base légale

Date de décision	01/07/2022
Durée de l'enregistrement	3 ans
Date d'échéance de l'enregistrement	01/07/2025

Liens avec d'autres certifications

NOUVELLE(S) CERTIFICATION(S)
RNCP42082

Pour plus d'informations

LIEN VERS LE DESCRIPTIF

<https://www.ecolelamache.org/enseignement-superieur/bac5-niveau-7/>

Fiche officielle (France Compétences)

<https://www.francecompetences.fr/recherche/rncp/36586/>