

Expert en cybersécurité industrielle

RNCP42082 · RNCP · Publiée

L'essentiel

Niveau de qualification	Niveau 7
Code(s) NSF	326
Formacode(s)	31045, 31038, 31094, 31082, 24426
Code(s) ROME	M1802, M1810, M1801, M1805, M1806
Type d'enregistrement	Enregistrement sur demande
Date d'enregistrement	01/04/2026
Date d'échéance	01/04/2029

Certificateur(s)

FONDATION LA MACHE · SIRET : 50215377800019

Résumé de la certification

OBJECTIFS ET CONTEXTE

L'Expert en cybersécurité industrielle évolue dans un secteur en pleine transformation, où la digitalisation des environnements industriels modifie profondément les modes de production et accroît la surface d'exposition aux cybermenaces. Les systèmes de contrôle-commande (SCADA, PLC, ICS), historiquement isolés, sont désormais interconnectés avec les systèmes d'information classiques (IT), les plateformes cloud, les réseaux d'entreprise et les équipements IoT industriels (IIoT). Cette convergence IT/OT expose les infrastructures critiques à des attaques sophistiquées pouvant entraîner des arrêts de production, des défaillances de sûreté, des perturbations logistiques ou des impacts environnementaux et humains. La filière de la cybersécurité est devenue en à peine quelques années un domaine dans lequel il existe désormais une diversité de postes largement méconnue.

Le métier d'Expert en cybersécurité industrielle s'exerce dans un contexte marqué par la transformation profonde des systèmes de production et la multiplication des menaces visant les environnements industriels. Les entreprises industrielles – PME, ETI et grands groupes –, les opérateurs d'importance vitale (OIV), les opérateurs de services essentiels (OSE), les intégrateurs OT/IT, les bureaux d'études spécialisés et les prestataires en cybersécurité industrielle constituent les principaux cadres d'exercice. Ces organisations sont confrontées à des enjeux critiques de continuité d'activité, de sûreté de fonctionnement et de conformité réglementaire, renforçant la nécessité d'un haut niveau d'expertise pour protéger les systèmes industriels (SCADA, PLC, ICS, IIoT) et les processus de production.

ACTIVITÉS VISÉES

Réalisation d'un audit de cybersécurité industrielle
Supervision de la sécurité du système d'information industriel
Élaboration de la politique et de la stratégie de cybersécurité industrielle
Déploiement et diffusion de la culture de cybersécurité
Déploiement et intégration des solutions de cybersécurité OT/IT
Administration et maintien en condition de sécurité (MCS)
Pilotage stratégique et coordination du dispositif de cybersécurité
Veille, conformité et amélioration continue du dispositif de cybersécurité

COMPÉTENCES ATTESTÉES

Analyser les besoins en cybersécurité des systèmes industriels et des équipements de contrôle-commande (SCADA, automates, capteurs) 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.

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

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.

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

Mettre en place l'architecture et les outils de supervision de la sécurité des environnements industriels en déployant les solutions de journalisation, de collecte et de monitoring adaptées aux contraintes IT/OT afin d'assurer l'observation continue du système d'information industriel.

Évaluer les risques de sécurité spécifiques aux environnements industriels en identifiant les vulnérabilités à l'aide d'outils adaptés à l'environnement et aux moyens de l'entreprise afin de préparer des mesures de réduction de l'impact lié à ces risques

Analyser les événements, alertes et anomalies issues des environnements OT (SCADA, PLC, HMI) en tenant compte des dépendances de production et des exigences de sûreté de fonctionnement, afin d'identifier les déviations significatives et d'évaluer leur impact opérationnel.

Détecter les menaces pesant sur les environnements industriels en configurant et ajustant les règles de corrélation, signatures, scénarios d'attaque et outils de détection (SIEM, IDS/IPS industriels) afin d'identifier les activités suspectes et les tentatives de compromission.

Proposer des mesures de contournements, d'amélioration des capacités de détection et de réaction 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.

Définir les modalités de gestion de crise en mobilisant les ressources techniques et humaines afin d'améliorer les capacités de défense, de réaction et maintenir un niveau de sécurité adapté à la structure.

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.

Mener une investigation numérique à l'aide des outils d'analyse forensique, de journalisation et de corrélation d'événements en recherchant les causes racines afin de gérer les incidents de sécurité.

Analyser les contraintes fonctionnelles et/ou organisationnelles des systèmes industriels en s'appuyant sur les documents d'architecture, les entretiens avec les acteurs métiers et techniques, l'analyse des processus de production et les référentiels industriels applicables (IEC 62443, guides ANSSI) afin d'intégrer les contraintes spécifiques de ces systèmes à la politique de sécurité.

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

Définir la politique de sécurité de l'entreprise à l'aide des différents acteurs, en tenant compte des contraintes internes et externes et en s'appuyant sur les principes de défense en profondeur afin de maximiser la sécurité informatique

Participer à la définition de la stratégie de sécurité des systèmes d'information et systèmes industriels à l'aide des différentes analyses et procédures existantes en alignant les objectifs IT/OT, les exigences de production et les cadres réglementaires applicables afin de s'aligner avec la stratégie de l'entreprise et assurer la sécurité du capital informationnel.

Sécuriser la chaîne d'approvisionnement numérique et industrielle en identifiant les dépendances critiques et en intégrant des exigences de cybersécurité dans les contrats et processus fournisseurs afin de réduire les risques liés aux tiers.

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.

Concevoir une stratégie de sensibilisation à la cybersécurité industrielle en définissant les objectifs, les cibles, les supports et les indicateurs d'impact, afin d'ancrer durablement la culture de sécurité au sein de l'organisation.

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.

Animer un réseau de correspondants ou de référents cybersécurité au sein des services IT, OT et métiers, afin de favoriser la circulation des bonnes pratiques, la détection précoce des incidents et le partage de connaissances

Concevoir une architecture sécurisée système et réseau, adaptée aux contraintes des systèmes industriels, à l'aide des bonnes pratiques, d'outils techniques afin d'aligner les infrastructures aux besoins et à la stratégie de sécurité de l'entreprise.

Concevoir une architecture sécurisée applicative et de données, adaptée aux contraintes des systèmes industriels, à l'aide des bonnes pratiques, d'outils techniques au niveau applicatif afin d'aligner les infrastructures aux besoins et à la stratégie de sécurité de l'entreprise.

Mettre en œuvre des solutions de cybersécurité IT/OT adaptées aux contraintes des environnements SCADA et des réseaux industriels en s'appuyant sur les bonnes pratiques admises (éditeurs, constructeurs ou profession) afin de garantir un niveau adapté de sécurité du système d'informations.

Administrer les solutions de cybersécurité du système d'information et du système d'information industriel conformément aux bonnes pratiques et à la politique de sécurité de l'entreprise afin d'assurer le fonctionnement opérationnel des systèmes vitaux de l'organisation.

Gérer le cycle de vie, la configuration et la maintenance sécurisée des composants IT/OT (postes industriels, automates, serveurs, équipements réseau) en appliquant des procédures de durcissement, de mise à jour et de contrôle de versions afin d'assurer la conformité et la stabilité des environnements industriels.

Sécuriser les flux de données et les accès distants entre les réseaux IT, les réseaux OT et la zone d'interconnexion IT/OT (DMZ industrielle) en mettant en œuvre des solutions de segmentation, de filtrage et d'authentification forte afin de prévenir les intrusions et garantir l'intégrité des échanges.

Déployer des outils de supervision, de corrélation et d'automatisation de la cybersécurité (SOC, SIEM, SOAR, IDS/IPS industriels) afin d'optimiser la détection des menaces et la réactivité opérationnelle des équipes cyber.

Assurer la communication à l'aide des outils adéquats afin de veiller à la bonne diffusion des informations liées à la sécurité auprès des acteurs IT, OT et des équipes intervenant en zone d'interconnexion (DMZ, passerelles) et à la bonne application des mesures de sécurité définies au sein de l'organisation.

Organiser les interventions des équipes à l'aide d'outils et méthodes appropriées de gestion de projets et techniques de communication, en tenant compte des principes d'inclusion, d'accessibilité et d'adaptation des environnements de travail afin d'améliorer la coordination des différentes composantes opérationnelles et décisionnelles de l'entreprise.

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 continue du processus de sécurisation

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

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 légales et réglementaires applicables.

Piloter la conformité des environnements IT, OT et des flux IT/OT aux réglementations européennes et nationales applicables (NIS2, LPM, RGPD, directives sectorielles) en évaluant les écarts et en coordonnant les plans d'actions correctifs afin d'assurer la conformité, la traçabilité et la maîtrise du risque juridique et opérationnel.

Intégrer les enjeux environnementaux, énergétiques et les principes de sobriété numérique dans la politique de cybersécurité à l'aide d'une analyse d'impacts croisés afin de contribuer à une transformation numérique durable, alignée sur les objectifs de transition écologique et conforme aux valeurs de l'entreprise.

Blocs de compétences

RNCP42082BC01 — Auditer la sécurité du système d'information industriel

LISTE DE COMPÉTENCES

Analyser les besoins en cybersécurité des systèmes industriels et des équipements de contrôle-commande (SCADA, automates, capteurs) 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.

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

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.

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

MODALITÉS D'ÉVALUATION

Mise en situation professionnelle reconstituée d'un audit de sécurité de système d'information industriel

Soutenance orale devant un jury de professionnel

RNCP42082BC02 — Superviser la sécurité du système d'information industriel

LISTE DE COMPÉTENCES

Mettre en place l'architecture et les outils de supervision de la sécurité des environnements industriels en déployant les solutions de journalisation, de collecte et de monitoring adaptées aux contraintes IT/OT afin d'assurer l'observation continue du système d'information industriel.

Évaluer les risques de sécurité spécifiques aux environnements industriels en identifiant les vulnérabilités à l'aide d'outils adaptés à l'environnement et aux moyens de l'entreprise afin de préparer des mesures de réduction de l'impact lié à ces risques

Analyser les événements, alertes et anomalies issues des environnements OT (SCADA, PLC, HMI) en tenant compte des dépendances de production et des exigences de sûreté de fonctionnement, afin d'identifier les déviations significatives et d'évaluer leur impact opérationnel.

Détecter les menaces pesant sur les environnements industriels en configurant et ajustant les règles de corrélation, signatures, scénarios d'attaque et outils de détection (SIEM, IDS/IPS industriels) afin d'identifier les activités suspectes et les tentatives de compromission.

Proposer des mesures de contournements, d'amélioration des capacités de détection et de réaction 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.

Définir les modalités de gestion de crise en mobilisant les ressources techniques et humaines afin d'améliorer les capacités de défense, de réaction et maintenir un niveau de sécurité adapté à la structure.

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.

Mener une investigation numérique à l'aide des outils d'analyse forensique, de journalisation et de corrélation d'événements en recherchant les causes racines afin de gérer les incidents de sécurité.

MODALITÉS D'ÉVALUATION

Mise en situation professionnelle réelle (réalisé en entreprise) ou reconstituée de la conception d'un système de supervision de la sécurité d'un système d'information industriel

Soutenance orale devant un jury de professionnel

Entretien technique

RNCP42082BC03 — Définir et piloter la stratégie de cybersécurité des systèmes d'information industriels

LISTE DE COMPÉTENCES

Analyser les contraintes fonctionnelles et/ou organisationnelles des systèmes industriels en s'appuyant sur les documents d'architecture, les entretiens avec les acteurs métiers et techniques, l'analyse des processus de production et les référentiels industriels applicables (IEC 62443, guides ANSSI) afin d'intégrer les contraintes spécifiques de ces systèmes à la politique de sécurité.

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

Définir la politique de sécurité de l'entreprise à l'aide des différents acteurs, en tenant compte des contraintes internes et externes et en s'appuyant sur les principes de défense en profondeur afin de maximiser la sécurité informatique

Participer à la définition de la stratégie de sécurité des systèmes d'information et systèmes industriels à l'aide des différentes analyses et procédures existantes en alignant les objectifs IT/OT, les exigences de production et les cadres réglementaires applicables afin de s'aligner avec la stratégie de l'entreprise et assurer la sécurité du capital informationnel.

Sécuriser la chaîne d'approvisionnement numérique et industrielle en identifiant les dépendances critiques et en intégrant des exigences de cybersécurité dans les contrats et processus fournisseurs afin de réduire les risques liés aux tiers.

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.

Concevoir une stratégie de sensibilisation à la cybersécurité industrielle en définissant les objectifs, les cibles, les supports et les indicateurs d'impact, afin d'ancrer durablement la culture de sécurité au sein de l'organisation.

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.

Animer un réseau de correspondants ou de référents cybersécurité au sein des services IT, OT et métiers, afin de favoriser la circulation des bonnes pratiques, la détection précoce des incidents et le partage de connaissances

MODALITÉS D'ÉVALUATION

Mise en situation professionnelle réelle ou reconstituée portant sur le déploiement de processus organisationnels de cybersécurité (élaboration d'une stratégie de cybersécurité industrielle et de continuité d'activité)

Soutenance orale devant un jury de professionnel

Entretien technique

RNCP42082BC04 — Déployer et administrer l'architecture de cybersécurité des systèmes d'information industriels

LISTE DE COMPÉTENCES

Concevoir une architecture sécurisée système et réseau, adaptée aux contraintes des systèmes industriels, à l'aide des bonnes pratiques, d'outils techniques afin d'aligner les infrastructures aux besoins et à la stratégie de sécurité de l'entreprise.

Concevoir une architecture sécurisée applicative et de données, adaptée aux contraintes des systèmes industriels, à l'aide des bonnes pratiques, d'outils techniques au niveau applicatif afin d'aligner les infrastructures aux besoins et à la stratégie de sécurité de l'entreprise.

Mettre en œuvre des solutions de cybersécurité IT/OT adaptées aux contraintes des environnements SCADA et des réseaux industriels en s'appuyant sur les bonnes pratiques admises (éditeurs, constructeurs ou profession) afin de garantir un niveau adapté de sécurité du système d'informations.

Administrer les solutions de cybersécurité du système d'information et du système d'information industriel conformément aux bonnes pratiques et à la politique de sécurité de l'entreprise afin d'assurer le fonctionnement opérationnel des systèmes vitaux de l'organisation.

Gérer le cycle de vie, la configuration et la maintenance sécurisée des composants IT/OT (postes industriels, automates, serveurs, équipements réseau) en appliquant des procédures de durcissement, de mise à jour et de contrôle de versions afin d'assurer la conformité et la stabilité des environnements industriels.

Sécuriser les flux de données et les accès distants entre les réseaux IT, les réseaux OT et la zone d'interconnexion IT/OT (DMZ industrielle) en mettant en œuvre des solutions de segmentation, de filtrage et d'authentification forte afin de prévenir les intrusions et garantir l'intégrité des échanges.

Déployer des outils de supervision, de corrélation et d'automatisation de la cybersécurité (SOC, SIEM, SOAR, IDS/IPS industriels) afin d'optimiser la détection des menaces et la réactivité opérationnelle des équipes cyber.

MODALITÉS D'ÉVALUATION

Dossier professionnel portant sur un projet de déploiement d'un ou plusieurs environnements techniques réalisé en entreprise

Soutenance orale devant un jury de professionnel

Entretien technique

RNCP42082BC05 — Assurer la gouvernance, la conformité et l'amélioration continue du dispositif de cybersécurité industrielle

LISTE DE COMPÉTENCES

Assurer la communication à l'aide des outils adéquats afin de veiller à la bonne diffusion des informations liées à la sécurité auprès des acteurs IT, OT et des équipes intervenant en zone d'interconnexion (DMZ, passerelles) et à la bonne application des mesures de sécurité définies au sein de l'organisation.

Organiser les interventions des équipes à l'aide d'outils et méthodes appropriées de gestion de projets et techniques de communication, en tenant compte des principes d'inclusion, d'accessibilité et d'adaptation des environnements de travail afin d'améliorer la coordination des différentes composantes opérationnelles et décisionnelles de l'entreprise.

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 continue du processus de sécurisation.

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

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 légales et réglementaires applicables.

Piloter la conformité des environnements IT, OT et des flux IT/OT aux réglementations européennes et nationales

applicables (NIS2, LPM, RGPD, directives sectorielles) en évaluant les écarts et en coordonnant les plans d'actions correctifs afin d'assurer la conformité, la traçabilité et la maîtrise du risque juridique et opérationnel.

Intégrer les enjeux environnementaux, énergétiques et les principes de sobriété numérique dans la politique de cybersécurité à l'aide d'une analyse d'impacts croisés afin de contribuer à une transformation numérique durable, alignée sur les objectifs de transition écologique et conforme aux valeurs de l'entreprise.

MODALITÉS D'ÉVALUATION

Dossier professionnel portant sur la mise en œuvre d'outils de pilotage de la cybersécurité à l'échelle de la structure.

Soutenance orale devant un jury de professionnel

Entretien technique

Secteur d'activité et type d'emploi

SECTEURS D'ACTIVITÉS

L'Expert en cybersécurité industrielle exerce principalement dans des organisations confrontées à des enjeux critiques de continuité d'activité et de protection des systèmes industriels. Les environnements d'exercice couvrent un large spectre d'acteurs : entreprises industrielles de toutes tailles (PME industrielles, ETI, grands groupes multisites), opérateurs d'importance vitale (OIV), opérateurs de services essentiels (OSE), entreprises du numérique spécialisées en OT/ICS, intégrateurs, fournisseurs d'équipements industriels, bureaux d'études et sociétés de conseil en cybersécurité. Ces structures évoluent dans un contexte marqué par la digitalisation accélérée des moyens de production, la convergence IT/OT, la montée de la robotisation et de l'IIoT, et le renforcement des contraintes réglementaires (NIS2, LPM, IEC 62443, référentiels sectoriels). L'Expert en cybersécurité industrielle évolue dans un secteur en pleine transformation, où la digitalisation des environnements industriels modifie profondément les modes de production et accroît la surface d'exposition aux cybermenaces. Les systèmes de contrôle-commande (SCADA, PLC, ICS), historiquement isolés, sont désormais interconnectés avec les systèmes d'information classiques (IT), les plateformes cloud, les réseaux d'entreprise et les équipements IoT industriels (IIoT). Cette convergence IT/OT expose les infrastructures critiques à des attaques sophistiquées pouvant entraîner des arrêts de production, des défaillances de sûreté, des perturbations logistiques ou des impacts environnementaux et humains.

Les secteurs concernés sont variés : énergie, eau et assainissement, transport, chimie, pharmacie, agroalimentaire, métallurgie, électronique, logistique, industrie 4.0, infrastructures portuaires et aéroportuaires, ou encore data centers industriels. La plupart sont soumis à des obligations réglementaires renforcées, telles que NIS2, la Loi de Programmation Militaire (LPM), les normes IEC 62443, ISO 27019, ou encore les exigences des autorités sectorielles (ANSSI, ASN, CRE, ARS, etc.).

Dans ce contexte, la cybersécurité industrielle n'est plus un enjeu optionnel : elle conditionne la continuité d'activité, la sûreté de fonctionnement, la maîtrise des risques opérationnels et la résilience globale de la chaîne de production. Les entreprises recherchent désormais des profils capables d'intervenir à la fois sur les enjeux techniques (sécurisation des environnements OT), organisationnels (politiques, processus, gouvernance) et stratégiques (anticipation des menaces, gestion de crise, conformité).

L'Expert en cybersécurité industrielle peut exercer dans des organisations de tailles et de structures variées, chacune impliquant des logiques d'intervention différentes :

- PME industrielles et ateliers de production
- ETI industrielles
- Grands groupes et organisations multisites
- Intégrateurs, bureaux d'études et cabinets de conseil

TYPE D'EMPLOIS ACCESSIBLES

- Responsable de la Sécurité des Systèmes d'information (RSSI), adjoint RSSI
- Architecte de la Sécurité des Systèmes d'information, architecte cybersécurité industrielle
- Consultant(e) en cybersécurité en ESN
- Administrateur système, réseau et sécurité des infrastructures
- Expert(e) en investigation numérique, Pentester
- Analyste SOC (Security Operation Center) niveau 2 ou 3
- Expert(e) en sécurité des IOT, ingénieur(e) sécurité Industrial IOT
- Responsable de la sécurité systèmes et réseaux OT (Operational Technology)

RÉGLEMENTATIONS D'ACTIVITÉ

L'activité de l'expert en cybersécurité industrielle n'est pas réglementée par une loi ou une réglementation spécifique. Cependant, il existe des normes et des réglementations qui encadrent les activités industrielles de manière générale et des cadres de travail auxquels chaque entreprise peut ou doit se conformer selon les secteurs d'activités (normes sectorielles, environnementales, obligations règlementaires liées au OIV etc.) comme NIS2, HDS.

La directive NIS2, transposée en droit français en 2024, constitue aujourd'hui la pierre angulaire de la régulation : elle étend le périmètre des entités soumises à des obligations de cybersécurité — notamment les secteurs critiques tels que l'énergie, les transports, l'eau, la santé, les infrastructures numériques, l'industrie manufacturière et la gestion des déchets — et impose des exigences précises en matière de gestion des risques, de sécurité opérationnelle, de supervision, de reporting d'incidents et de résilience. À ces obligations s'ajoutent les exigences sectorielles de la Loi de Programmation Militaire (LPM), qui renforcent la protection des Opérateurs d'Importance Vitale (OIV), ainsi que les normes internationales IEC 62443, devenues le référentiel incontournable pour la sécurisation des systèmes de contrôle industriel (SCADA, ICS, PLC). Dans de nombreux secteurs industriels, ces normes sont désormais intégrées contractuellement ou imposées par les autorités de régulation. Ce cadre normatif impose aux entreprises industrielles de disposer de compétences expertes capables de conduire des analyses de risques OT/ICS, de sécuriser la convergence IT/OT, de piloter les audits de conformité, de configurer des architectures industrielles sécurisées, et d'assurer une surveillance continue des environnements critiques.

Dans le cadre de la directive NIS2, l'expert en cybersécurité industrielle doit répondre à des obligations renforcées spécifiques aux environnements OT/ICS. Le texte impose, via l'article 21, une gestion systématique des risques cyber appliquée aux systèmes industriels, incluant la cartographie des actifs, l'évaluation des dépendances critiques, la segmentation OT/IT, la supervision des réseaux industriels, la gestion des accès distants, la détection des incidents ICS et l'assurance de la continuité d'activité industrielle. NIS2 introduit également des exigences de transparence et de reporting des incidents significatifs affectant les systèmes industriels, ainsi qu'une obligation de démontrer un niveau de sécurité proportionné aux risques opérationnels.

Les normes IEC 62443 constituent le référentiel technique central pour la mise en œuvre de ces exigences dans les systèmes industriels. Les normes les plus mobilisées dans l'exercice du métier sont :

- IEC 62443-2-1, définissant les exigences organisationnelles et les programmes de cybersécurité industrielle ;
- IEC 62443-3-2, portant sur les méthodes d'évaluation des risques ICS ;
- IEC 62443-3-3, spécifiant les niveaux de sécurité (SL1 à SL4) pour les systèmes et zones industrielles ;
- IEC 62443-4-1, traitant du développement sécurisé des composants industriels ;
- IEC 62443-4-2, définissant les exigences techniques applicables aux automates, équipements de terrain, serveurs industriels et composants de communication.

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) ou d'un diplôme de niveau 6 dans le domaine de l'Informatique ou de l'automatisme et informatique industrielle.

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

Trois membres externes au centre de formation, salariés, consultants ou chefs d'entreprise dans le domaine de l'informatique et de la cybersécurité, exerçant depuis plusieurs années ou ayant exercé pendant plusieurs années des fonctions dans le domaine d'activité.

Un membre de l'organisme certificateur, professionnel de l'informatique ou membre de la direction de l'établissement.

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	01/04/2026
Durée de l'enregistrement	3 ans

Date d'échéance de l'enregistrement 01/04/2029

Date de dernière délivrance possible 01/04/2033

Statistiques

Année	Certifiés	Dont VAE	Insertion 6 mois	Métier 2 ans
2025	5	0	100 %	—
2024	10	1	80 %	80 %
2023	3	0	67 %	100 %

Liens avec d'autres certifications

ANCIENNES VERSIONS

RNCP36586

CORRESPONDANCES (PAR BLOCS)

RNCP36586, RNCP37300, RNCP38463, RNCP38779, RNCP39999, RNCP40897

Pour plus d'informations

Fiche officielle (France Compétences)

<https://www.francecompetences.fr/recherche/rncp/42082/>