

Expert en cybersécurité des systèmes complexes pour l'industrie et la Défense (MS)

RNCP42813 · RNCP · Publiée

L'essentiel

Niveau de qualification	Niveau 7
Code(s) NSF	326
Formacode(s)	31045, 24220, 24454
Code(s) ROME	M1802, M1806, M1801, M1810, M1803
Type d'enregistrement	Enregistrement sur demande
Date d'enregistrement	30/09/2026
Date d'échéance	30/09/2031

Certificateur(s)

ECOLE CENTRALE DE MARSEILLE · SIRET : 19133340000015

ECOLE DE L'AIR ET DE L'ESPACE · SIRET : 13002454000010

Résumé de la certification

OBJECTIFS ET CONTEXTE

La certification d' « Expert en cybersécurité des systèmes complexes pour l'industrie et la Défense (MS) » s'inscrit dans un contexte de transformation numérique accélérée des secteurs industriel, énergétique et de défense, marqué par une augmentation continue des menaces cyber pesant sur les systèmes critiques. La convergence croissante entre systèmes d'information, systèmes industriels et systèmes embarqués impose le développement de compétences expertes capables d'appréhender la cybersécurité dans sa globalité, au-delà des seuls environnements informatiques traditionnels.

La certification a pour objectif de former des professionnels capables d'analyser les risques cyber, de concevoir et mettre en œuvre des architectures de sécurité adaptées à des systèmes complexes, d'anticiper et traiter les menaces affectant les infrastructures critiques, et de piloter des projets de cybersécurité dans des environnements à fortes contraintes opérationnelles, réglementaires et stratégiques.

Elle répond ainsi aux besoins exprimés par les entreprises industrielles, les opérateurs d'importance vitale et les acteurs de la Défense, en formant des experts immédiatement opérationnels, aptes à contribuer à la résilience et à la souveraineté numérique des organisations.

ACTIVITÉS VISÉES

Assurer la gouvernance de la cybersécurité d'un système complexe (industrie, défense) :

Élaboration des orientations stratégiques pour un système industriel complexe en matière de cybersécurité

Gestion du risque cybersécurité d'un système complexe

Identification des risques d'un système industriel complexe.

Assurer la protection d'un système complexe (industrie, défense) :

Conception d'une stratégie de sécurisation à partir des résultats de l'analyse de risque

Mise en œuvre d'une solution cryptographique et sécurisation d'un système complexe

Assurer la défense d'un système complexe (industrie, défense) :

Détection de cyber attaques sur un système industriel à l'aide d'une infrastructure adaptée

Réponse aux incidents de sécurité et renforcement post-attaque du système (Stopper, investiguer, remédier et revenir à une situation normale)

Manager une équipe et un projet de cybersécurité des systèmes complexes (industrie, défense) :

Mise en place la gouvernance d'un projet de cybersécurité des systèmes complexes

Management d'équipes pluridisciplinaires et intégration de la cybersécurité tout au long du cycle de vie du système concerné

Gestion de crise et résilience des systèmes face aux cybermenaces

COMPÉTENCES ATTESTÉES

Positionner la cybersécurité dans un contexte national et international en identifiant la réglementation idoine, afin de garantir la conformité réglementaire et la soutenabilité juridique et stratégique de l'organisation.

Conduire une veille stratégique en cybersécurité en recherchant et en collectant du renseignement sur les menaces induites (cyber threat intelligence), afin d'anticiper les attaques, prioriser les risques et orienter les décisions de sécurité et de protection du système d'information.

Rédiger la stratégie cybersécurité d'un système industriel complexe en prenant en compte la stratégie de développement de l'entreprise, afin de prévenir efficacement les risques et les menaces tout en assurant la résilience, la continuité d'activité et l'alignement avec les objectifs stratégiques de l'entreprise.

Élaborer des stratégies d'anticipation du risque cyber en proposant des mesures de protection et de sécurité adaptées aux menaces et modes opératoires identifiés, afin de réduire l'exposition aux risques, garantir la sécurité du système industriel et assurer la continuité de ses activités.

Animer une cellule de crise décisionnelle et des cellules de crise opérationnelles en impliquant chaque membre de l'équipe et en tenant compte des compétences et situations professionnelles individuelles afin de s'assurer de leur capacité à agir, à traiter les incidents et à communiquer pendant la crise, dans l'objectif de limiter les impacts opérationnels, décisionnels et réputationnels de l'incident.

Cartographier les composantes d'un système d'information industriel complexe en fournissant une analyse fine de la menace et des vulnérabilités/besoins en sécurité du système afin d'identifier les zones critiques, prioriser les actions de sécurisation et éclairer les décisions de protection du système.

Produire une analyse de risques exploitable par la gouvernance en appliquant une méthodologie reconnue (type EBIOS Risk Manager) pour identifier, évaluer et hiérarchiser les risques cyber, déterminer les scénarios de menace, et formaliser un plan de traitement du risque compatible avec les besoins métiers, les contraintes industrielles et l'orientation stratégique de l'organisation afin de soutenir la prise de décision, d'optimiser l'allocation des ressources et de réduire durablement l'exposition aux risques cyber.

Définir une stratégie de protection des données et des échanges en établissant une politique de chiffrement et de protection d'un système industriel complexe, adaptée aux exigences de disponibilité, de confidentialité, d'intégrité, d'authentification et de traçabilité, en tenant compte des contraintes opérationnelles et des usages nomades, afin de garantir la protection des informations sensibles, la confiance dans les échanges et la conformité aux exigences réglementaires et contractuelles.

Concevoir et formaliser un plan de traitement des risques cyber en définissant les mesures organisationnelles et techniques permettant d'atteindre la cible de sécurité définie par la gouvernance, en réduisant les risques identifiés à un niveau acceptable et maîtrisé, afin de structurer le pilotage de la sécurité, prioriser les actions et assurer un suivi cohérent de la maîtrise des risques dans la durée.

Choisir et déployer des suites et outils cryptographiques (classiques et post quantique) adaptés à un système complexe, incluant gestion des clés et certificats, chiffrement des flux et des données sensibles, afin de garantir la confidentialité, l'intégrité et l'authenticité des échanges, d'assurer la résilience face aux menaces actuelles et émergentes, et de maintenir la conformité aux exigences réglementaires et contractuelles.

Concevoir une architecture sécurisée adaptée au système complexe, incluant segmentation réseau, zones OT/IT, isolation et redondance des composants critiques, afin de réduire la surface d'attaque, limiter la propagation d'incidents, garantir la disponibilité des fonctions essentielles et assurer la résilience globale du système face aux menaces cyber.

Sécuriser les composants matériels, systèmes d'exploitation et logiciels selon les bonnes pratiques de durcissement et de supervision pour réduire les vulnérabilités exploitables, prévenir les compromissions, détecter les comportements anormaux et garantir l'intégrité, la disponibilité et la fiabilité du système complexe dans la durée.

Exploiter des capacités d'intelligence artificielle pour renforcer la détection des attaques, en utilisant, lorsque pertinent, des outils d'intelligence artificielle pour accroître la précocité et la fiabilité de la détection des cyberattaques

Concevoir une stratégie de détection adaptée à un système industriel complexe intégrant les sources de journalisation, règles de corrélation, chaînes de détection et outils (avec ou sans recours à l'IA), afin d'assurer une remontée rapide, exploitable et contextualisée des informations nécessaires à l'identification précoce des attaques.

Élaborer et conduire un dispositif de réponse à incident cyber en fournissant des informations pertinentes aux

équipes, en coordonnant les actions de confinement, d'éradication et de continuité, afin de rétablir un fonctionnement nominal du système.

Conduire un plan de remédiation suite à une attaque sur un système industriel complexe afin de garantir un retour aux conditions nominales.

Renforcer la sécurité du système industriel ou de défense en capitalisant sur les résultats des investigations issues de l'attaque pour prévenir le risque de récurrence.

Définir, structurer et piloter la gouvernance cybersécurité d'un projet de système complexe, en précisant les rôles, responsabilités, processus décisionnels et indicateurs de pilotage, tout en intégrant les principes d'accessibilité, d'inclusion et de responsabilité sociétale, afin de sécuriser les choix stratégiques, et d'inscrire le projet dans une démarche durable, inclusive et conforme aux exigences réglementaires et sociétales.

Analyser, hiérarchiser et arbitrer les risques cyber d'un projet complexe en tenant compte des impacts opérationnels, humains, organisationnels et environnementaux, afin d'éclairer la prise de décision stratégique dans un contexte contraint.

Garantir la conformité réglementaire, normative et éthique du projet, en intégrant les exigences liées à la protection des données, à l'accessibilité et au développement durable, afin d'assurer la légitimité, la responsabilité sociétale et la pérennité des solutions mises en oeuvre dans le respect des cadres légaux et des engagements éthiques de l'organisation.

Piloter la mise en oeuvre des mesures de protection des systèmes complexes en intégrant des critères d'ergonomie, d'accessibilité et de sobriété numérique, afin de garantir une sécurité efficace et durable, favorisant l'inclusion des utilisateurs et la maîtrise de l'empreinte environnementale du système.

Manager des équipes pluridisciplinaires en contexte cybersécurité en prenant en compte la diversité des profils, les situations de handicap et les compétences individuelles, afin de garantir une intégration efficace et sécurisée des exigences cybersécurité dans le projet.

Piloter les activités de vérification, de validation et d'audit de sécurité en évaluant leur efficacité opérationnelle, leur conformité et leur impact environnemental, afin de garantir la fiabilité des dispositifs de protection mis en place et l'amélioration continue de la sécurité du système.

Organiser la défense et la gestion de crise cyber en assurant la continuité d'activité, la prise de décision stratégique et une communication sécurisée et accessible, afin de limiter l'impact des dommages causés

Manager les parties prenantes en situation de crise (direction, managers, employés, équipes de crise... en internes et clients, fournisseurs, autorités, médias, partenaires... en externes) ; en tenant compte des facteurs humains, organisationnels et de stress, afin de garantir l'efficacité de la réponse et la cohésion des acteurs.

Capitaliser les retours d'expérience pour renforcer la résilience afin de renforcer durablement la résilience cyber, organisationnelle et environnementale des systèmes complexes concernés.

Blocs de compétences

RNCP42813BC01 — Assurer la gouvernance de la cybersécurité d'un système complexe (industrie, défense)

LISTE DE COMPÉTENCES

Positionner la cybersécurité dans un contexte national et international en identifiant la réglementation idoine afin de garantir la conformité réglementaire et la soutenabilité juridique et stratégique de l'organisation.

Conduire une veille stratégique en cybersécurité en recherchant et en collectant du renseignement sur les menaces induites (cyber threat intelligence), afin d'anticiper les attaques, prioriser les risques et orienter les décisions de sécurité et de protection du système d'information.

Rédiger la stratégie cybersécurité d'un système industriel complexe en prenant en compte la stratégie de développement de l'entreprise, afin de prévenir efficacement les risques et les menaces tout en assurant la résilience, la continuité d'activité et l'alignement avec les objectifs stratégiques de l'entreprise.

Élaborer des stratégies d'anticipation du risque cyber en proposant des mesures de protection et de sécurité adaptées aux menaces et modes opératoires identifiés afin de réduire l'exposition aux risques, garantir la sécurité du système industriel et assurer la continuité de ses activités.

Animer une cellule de crise décisionnelle et des cellules de crise opérationnelles en impliquant chaque membre de l'équipe et en tenant compte des compétences et situations professionnelles individuelles afin de s'assurer de leur capacité à agir, à traiter les incidents et à communiquer pendant la crise, dans l'objectif de limiter les impacts opérationnels, décisionnels et réputationnels de l'incident.

Cartographier les composantes d'un système d'information industriel complexe en fournissant une analyse fine de la menace et des vulnérabilités/besoins en sécurité du système afin d'identifier les zones critiques, prioriser les actions de sécurisation et éclairer les décisions de protection du système.

Produire une analyse de risques exploitable par la gouvernance en appliquant une méthodologie reconnue (type EBIOS Risk Manager) pour identifier, évaluer et hiérarchiser les risques cyber, déterminer les scénarios de menace, et formaliser un plan de traitement du risque compatible avec les besoins métiers, les contraintes industrielles et l'orientation stratégique de l'organisation afin de soutenir la prise de décision, d'optimiser l'allocation des ressources et de réduire durablement l'exposition aux risques cyber.

MODALITÉS D'ÉVALUATION

Mise en situation professionnelle simulée permettant l'évaluation de l'ensemble du bloc.

A partir d'un cas d'étude fictif représentatif d'un système industriel complexe confronté à des enjeux de cybersécurité, dans un travail de groupe (3 à 4 personnes), les candidats agissent en qualité d'expert en cybersécurité mandaté par la direction/un client pour structurer la gouvernance et piloter la gestion du risque. Il leur est demandé : D'analyser le contexte organisationnel, réglementaire et stratégique. D'exploiter des éléments de cyber threat intelligence fournis. D'identifier les menaces, les risques et les modes opératoires associés. De conduire une analyse de risques formalisée selon une méthodologie de référence. De réaliser la cartographie du système. D'élaborer une stratégie cybersécurité structurée et des mesures d'anticipation du risque. De proposer un dispositif de gestion de crise. D'animer une cellule de crise simulée et de justifier ses décisions.

A l'issue, une synthèse écrite est produite, elle sera soutenue individuellement à l'oral.

Livrables attendus :

Note stratégique cybersécurité structurée (veille, analyse de risques, cadre réglementaire, axes stratégiques, objectifs opérationnels, indicateurs). Cartographie du système d'information industriel, complète, ordonnée et documentée. Plan d'anticipation du risque cyber, incluant mesures de protection et de résilience. Plan de continuité d'activité / gestion de crise cyber, précisant l'organisation de la cellule de crise, les rôles, les processus de décision et de communication. Soutenance orale argumentée devant jury où chaque candidat démontre individuellement son niveau d'acquisition des compétences attendues.

RNCP42813BC02 — Assurer la protection d'un système complexe (industrie, défense)

LISTE DE COMPÉTENCES

Définir une stratégie de protection des données et des échanges en établissant une politique de chiffrement et de protection d'un système industriel complexe, adaptée aux exigences de disponibilité, de confidentialité, d'intégrité, d'authentification et de traçabilité, en tenant compte des contraintes opérationnelles et des usages nomades, afin de garantir la protection des informations sensibles, la confiance dans les échanges et la conformité aux exigences réglementaires et contractuelles.

Concevoir et formaliser un plan de traitement des risques cyber en définissant les mesures organisationnelles et techniques permettant d'atteindre la cible de sécurité définie par la gouvernance, en réduisant les risques identifiés à un niveau acceptable et maîtrisé, afin de structurer le pilotage de la sécurité, prioriser les actions et assurer un suivi cohérent de la maîtrise des risques dans la durée.

Choisir et déployer des suites et outils cryptographiques (classiques et post quantique) adaptés à un système complexe, incluant gestion des clés et certificats, chiffrement des flux et des données sensibles, afin de garantir la confidentialité, l'intégrité et l'authenticité des échanges, d'assurer la résilience face aux menaces actuelles et émergentes, et de maintenir la conformité aux exigences réglementaires et contractuelles.

Concevoir une architecture sécurisée adaptée au système complexe, incluant segmentation réseau, zones OT/IT, isolation et redondance des composants critiques, afin de réduire la surface d'attaque, limiter la propagation d'incidents, garantir la disponibilité des fonctions essentielles et assurer la résilience globale du système face aux menaces cyber.

Sécuriser les composants matériels, systèmes d'exploitation et logiciels selon les bonnes pratiques de durcissement et de supervision pour réduire les vulnérabilités exploitables, prévenir les compromissions, détecter les comportements anormaux et garantir l'intégrité, la disponibilité et la fiabilité du système complexe dans la durée.

MODALITÉS D'ÉVALUATION

Mise en situation professionnelle simulée permettant l'évaluation de l'ensemble du bloc.

A partir d'un cas d'étude fictif représentatif d'un système industriel complexe confronté à des enjeux de cybersécurité, dans un travail de groupe (3 à 4 personnes), les candidats agissent en tant qu'expert en cybersécurité pour protéger le système. Il est demandé : D'identifier les risques et menaces en exploitant les résultats d'une analyse de risque,

incluant les composants critiques, vulnérabilités, scénarios et niveaux de gravité. De concevoir et formaliser une stratégie de protection du système, incluant la politique de chiffrement et de protection des échanges ainsi que le plan de traitement des risques (mesures organisationnelles et techniques).

De prioriser les actions de sécurisation et définir les indicateurs de suivi opérationnel pour garantir le pilotage et la maîtrise du risque dans la durée. De concevoir et documenter une architecture sécurisée adaptée au système complexe, incluant séparation des zones OT/IT, sécurisation des flux et redondance des composants critiques. De mettre en œuvre des solutions cryptographiques et des mesures de sécurité sur systèmes et logiciels, en respectant les bonnes pratiques de durcissement et de supervision.

Une synthèse écrite est produite, elle sera soutenue individuellement à l'oral.

Livrables attendus : Rapport de stratégie de protection Politique de chiffrement, mesures organisationnelles et techniques, plan de traitement des risques. Cartographie de l'architecture sécurisée Zones OT/IT, segmentation, flux, redondance, composants critiques sécurisés. Plan de mise en œuvre des mesures de protection Sécurisation des systèmes et logiciels, déploiement des solutions cryptographiques, supervision et monitoring. Plan de traitement des risques. Mesures organisationnelles et techniques, priorisation des actions, suivi des indicateurs. Note de justification des choix de sécurité Alignement avec la gouvernance, la stratégie de l'organisation et les objectifs métiers. Soutenance orale individuelle. Présentation et justification des choix stratégiques, techniques et organisationnels, démontrant la maîtrise des compétences visées.

RNCP42813BC03 — Assurer la défense d'un système complexe (industrie, défense)

LISTE DE COMPÉTENCES

Exploiter des capacités d'intelligence artificielle pour renforcer la détection des attaques, en utilisant, lorsque pertinent, des outils d'intelligence artificielle pour accroître la précocité et la fiabilité de la détection des cyberattaques. Concevoir une stratégie de détection adaptée à un système industriel complexe intégrant les sources de journalisation, règles de corrélation, chaînes de détection et outils (avec ou sans recours à l'IA), afin d'assurer une remontée rapide, exploitable et contextualisée des informations nécessaires à l'identification précoce des attaques.

Élaborer et conduire un dispositif de réponse à incident cyber en fournissant des informations pertinentes aux équipes, en coordonnant les actions de confinement, d'éradication et de continuité, afin de rétablir un fonctionnement nominal du système

Conduire un plan de remédiation suite à une attaque sur un système industriel complexe afin de garantir un retour aux conditions nominales

Renforcer la sécurité du système industriel ou de défense en capitalisant sur les résultats des investigations issues de l'attaque pour prévenir le risque de récurrence

MODALITÉS D'ÉVALUATION

Mise en situation professionnelle simulée permettant l'évaluation de l'ensemble du bloc.

À partir d'un cas d'étude fictif représentatif d'un système industriel complexe confronté à des attaques cyber, dans un travail de groupe (3 à 4 personnes), les candidats agissent en tant qu'expert cybersécurité chargé d'assurer la défense active du système. Il leur est demandé de: Concevoir une stratégie de détection adaptée au contexte. Exploiter des outils de détection (incluant, le cas échéant, des capacités d'IA). Mener une investigation permettant de caractériser l'attaque. Définir et justifier les actions de remédiation. Élaborer et conduire un plan de réponse à incident. Formuler des recommandations de renforcement de la sécurité. Formaliser un retour d'expérience (RETEX) et proposer des mesures de renforcement pour prévenir la récurrence.

À l'issue, une synthèse écrite est produite, elle sera soutenue individuellement à l'oral.

Livrables attendus : Stratégie de détection des attaques, décrivant les sources, règles, chaînes de détection et outils mobilisés. Procédure de réponse à incident cyber, structurée (confinement, éradication, reprise). Rapport d'investigation post-incident, incluant chronologie, analyse des causes et impacts. Plan de renforcement de la sécurité, visant à prévenir la récurrence. Soutenance orale argumentée devant jury démontrant la maîtrise des compétences visées

RNCP42813BC04 — Manager une équipe et un projet de cybersécurité des systèmes complexes (industrie, défense)

LISTE DE COMPÉTENCES

Définir, structurer et piloter la gouvernance cybersécurité d'un projet de système complexe, en précisant les rôles, responsabilités, processus décisionnels et indicateurs de pilotage, tout en intégrant les principes d'accessibilité, d'inclusion et de responsabilité sociétale, afin de sécuriser les choix stratégiques, et d'inscrire le projet dans une démarche durable, inclusive et conforme aux exigences réglementaires et sociétales

Analyser, hiérarchiser et arbitrer les risques cyber d'un projet complexe en tenant compte des impacts opérationnels, humains, organisationnels et environnementaux, afin d'éclairer la prise de décision stratégique dans un contexte contraint.

Garantir la conformité réglementaire, normative et éthique du projet, en intégrant les exigences liées à la protection des données, à l'accessibilité et au développement durable, afin d'assurer la légitimité, la responsabilité sociétale et la pérennité des solutions mises en œuvre dans le respect des cadres légaux et des engagements éthiques de l'organisation.

Piloter la mise en œuvre des mesures de protection des systèmes complexes en intégrant des critères d'ergonomie, d'accessibilité et de sobriété numérique, afin de garantir une sécurité efficace et durable, favorisant l'inclusion des utilisateurs et la maîtrise de l'empreinte environnementale du système.

Manager des équipes pluridisciplinaires en contexte cybersécurité en prenant en compte la diversité des profils, les situations de handicap et les compétences individuelles, afin de garantir une intégration efficace et sécurisée des exigences cybersécurité dans le projet.

Piloter les activités de vérification, de validation et d'audit de sécurité en évaluant leur efficacité opérationnelle, leur conformité et leur impact environnemental, afin de garantir la fiabilité des dispositifs de protection mis en place et l'amélioration continue de la sécurité du système.

Organiser la défense et la gestion de crise cyber en assurant la continuité d'activité, la prise de décision stratégique et une communication sécurisée et accessible. afin de limiter l'impact des dommages causés

Manager les parties prenantes en situation de crise (direction, managers, employés, équipes de crise... en internes et clients, fournisseurs, autorités, médias, partenaires... en externes) ; en tenant compte des facteurs humains, organisationnels et de stress, afin de garantir l'efficacité de la réponse et la cohésion des acteurs.

Capitaliser les retours d'expérience pour renforcer la résilience afin de renforcer durablement la résilience cyber, organisationnelle et environnementale des systèmes complexes concernés.

MODALITÉS D'ÉVALUATION

Mise en situation professionnelle simulée (permettant l'évaluation de l'ensemble du bloc).

Au travers de l'expérience professionnelle du candidat correspondant à un cas complexe industriel ou défense, intégrant des contraintes réglementaires, humaines, environnementales et d'accessibilité : Le candidat définit la gouvernance cybersécurité du projet. Il analyse et arbitre les risques cyber. Il pilote des équipes hétérogènes et pluridisciplinaires. Il organise la protection, la défense et la gestion de crise. Il formule des axes d'amélioration et de résilience.

A l'issue, une synthèse écrite est produite, elle sera soutenue individuellement à l'oral.

Livrables attendus :

Dossier de gouvernance cybersécurité (organisation, gestion des risques, conformité, RSE). Dossier de pilotage de la protection (architecture, exigences, plans de vérification et d'audit). Rapport de gestion de crise et de retour d'expérience, incluant recommandations techniques, organisationnelles et durables. Soutenance orale argumentée devant jury.

Secteur d'activité et type d'emploi

SECTEURS D'ACTIVITÉS

Le secteur d'activité sur lequel débouche cette certification est vaste. Il touche tous les utilisateurs, les équipementiers, les intégrateurs, les cabinets de conseils ... impliqués dans les systèmes d'information et systèmes complexes industriels, y compris ceux destinés à l'armement et à la défense. Les titulaires de la certification peuvent ainsi exercer au sein d'organisations de tailles variées, allant de grandes entreprises industrielles à des PME ou ETI spécialisées, en passant par des cabinets de conseil, des intégrateurs de systèmes ou des organismes publics.

Plusieurs secteurs économiques sont particulièrement concernés : le secteur de l'énergie, le secteur des transports, les équipementiers et intégrateurs de systèmes industriels, le secteur de la défense

Ces environnements se caractérisent tous par des systèmes cyber-physiques complexes, interconnectés, soumis à des exigences de sûreté, de disponibilité et de résilience opérationnelle, dans un contexte de cyber menaces croissantes, notamment d'origine étatiques et hybrides.

Les titulaires de la certification sont donc amenés à exercer principalement dans des secteurs à forte criticité et à contraintes réglementaires importantes, tels que l'industrie de défense, l'aéronautique et le spatial, l'énergie (nucléaire, pétrole et gaz, réseaux électriques), les transports, les infrastructures critiques ou encore les organismes publics et les opérateurs d'importance vitale (OIV).

TYPE D'EMPLOIS ACCESSIBLES

Auditeur cybersécurité - Consultant en cybersécurité industrielle - Ingénieur cybersécurité OT- Responsable d'un centre opérationnel de sécurité (SOC) ou analyste SOC industriel - Expert en cybersécurité des systèmes industriels - Responsable de la sécurité des systèmes d'information (RSSI) - Chief Information Security Officer (CISO) au sein d'une entreprise - Responsable d'une équipe de réponse aux incidents (CERT / CSIRT) - Architecte sécurité - Expert ou analyste opérationnel en cybersécurité (conseil, assistance, supervision, réponse aux incidents)

RÈGLEMENTATIONS D'ACTIVITÉ

L'exercice des métiers visés par la certification « Expert en cybersécurité des systèmes complexes pour l'industrie et la Défense (MS) » n'est pas soumis à une réglementation professionnelle spécifique au sens d'une profession réglementée (ordre professionnel, autorisation d'exercice préalable). Toutefois, les activités exercées s'inscrivent dans des environnements fortement encadrés par des réglementations nationales, européennes et sectorielles, notamment dans les domaines industriel et défense.

Les organisations au sein desquelles interviennent les titulaires de la certification sont soumises notamment : au RGPD (protection des données personnelles). À la directive NIS2 relative à la sécurité des réseaux et des systèmes d'information. Aux obligations applicables aux opérateurs d'importance vitale et entités essentielles. À des exigences spécifiques aux secteurs défense et industries sensibles (protection du secret, contrôle des exportations, habilitations).

En complément du cadre réglementaire, les professionnels doivent maîtriser les référentiels et guides de bonnes pratiques tels que : les référentiels et guides publiés par l'ANSSI. Le NIST Cybersecurity Framework et les publications associées. Les normes ISO/IEC 27001 et ISO/IEC 62443 relatives respectivement aux systèmes de management de la sécurité de l'information et à la cybersécurité des systèmes industriels.

Ces cadres constituent des standards de référence largement adoptés dans les secteurs visés par la certification.

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)	2 942 €
Diplôme le plus fréquent	Diplôme de niveau bac+5 ou plus (doctorat, master ou équivalent) en communication et information (19 % des actifs en emploi)
Familles professionnelles (FAP)	M1X81 — Techniciens de production, d'exploitation, d'installation, et de maintenance, support et services aux utilisateurs en informatique · tension 4/5 (Élevée) M2X91 — Chefs de projet et directeurs de service informatique · tension 4/5 (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)	16 497
Jugés difficiles à recruter	46 %
Emplois saisonniers	2 %
Familles professionnelles (FAP)	M1X81 — Techniciens de production, d'exploitation, d'installation, et de maintenance, support et services aux utilisateurs en informatique M2X91 — Chefs de projet et directeurs de service informatique 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

Sont recevables les candidatures d'étudiants titulaires d'un des diplômes suivants :

Titre d'ingénieur diplômé conférant le grade de Master (formations évaluées par la Commission des Titres d'Ingénieur ; liste publiée au JO)

Diplôme d'une école de management privée ou consulaire conférant le grade de Master (formations évaluées par la CEFDG ;

liste publiée au JO)

Diplôme de 3ème cycle habilité par les autorités universitaires (Diplôme national de Master, DEA, DESS, ...) ou diplôme professionnel de niveau 7

Diplôme ou attestation de validation d'un niveau équivalent au M1, pour des candidats justifiant d'au moins trois années d'expérience professionnelle en lien avec la formation visée.

Titre inscrit au RNCP au niveau 7

Diplôme étranger équivalent aux diplômes français exigés ci-dessus.

Conditions d'accès dérogatoires (le pourcentage total de dérogations ne doit pas excéder 40%) :

Dans la limite de 40 % maximum de l'effectif de la promotion suivant la formation Mastère Spécialisé concernée, sont recevables, après une procédure de Validation des Acquis Personnels et Professionnels (VAPP), les candidatures de personnes justifiant à minima de 5 années d'expérience professionnelle pour lesquelles les activités exercées ont un lien avéré avec les compétences professionnelles visées par la formation.

Par dérogation pour 30 % maximum du nombre d'apprenants suivant la formation Mastère Spécialisé concernée, sont recevables les candidatures de titulaires d'un des diplômes suivants : Diplôme ou attestation de validation d'un niveau équivalent M1 sans expérience professionnelle ou ayant moins de 3 ans d'expérience professionnelle en lien avec la formation visée. Ou diplôme de Licence ou grade RNCP de niveau 6 justifiant d'une expérience adaptée de 3 ans minimum.

PRÉREQUIS À LA VALIDATION

La certification s'obtient par la validation de l'ensemble des blocs de compétences, et de la thèse professionnelle dans le cadre des voies d'accès par la formation.

COMPOSITION DU JURY — FORMATION INITIALE, FORMATION CONTINUE, VAE

Le jury de délivrance de la certification est composé de 4 personnes : 2 membres internes (issus respectivement de l'ECM et de l'EAE), et 2 membres externes , professionnels experts du domaine

Base légale

Date de décision	30/09/2026
Durée de l'enregistrement	5 ans
Date d'échéance de l'enregistrement	30/09/2031
Date de dernière délivrance possible	30/09/2035

Statistiques

Année	Certifiés	Dont VAE	Insertion 6 mois	Métier 2 ans
2024	11	0	90 %	—
2023	11	0	100 %	100 %
2022	13	0	100 %	100 %
2021	7	0	100 %	100 %

Pour plus d'informations

Fiche officielle (France Compétences)

<https://www.francecompetences.fr/recherche/rncp/42813/>