

# Expert en cybersécurité (MS)

RNCP41445 · RNCP · Publiée

## L'essentiel

|                         |                                   |
|-------------------------|-----------------------------------|
| Niveau de qualification | Niveau 7                          |
| Code(s) NSF             | 326                               |
| Formacode(s)            | 31006, 31038, 24220               |
| Code(s) ROME            | M1801, M1802, M1810, M1805, M1806 |
| Type d'enregistrement   | Enregistrement sur demande        |
| Date d'enregistrement   | 27/10/2025                        |
| Date d'échéance         | 27/10/2030                        |

## Certificateur(s)

INSTITUT MINES TELECOM - IMT NORD EUROPE · SIRET : 18009202500139

## Résumé de la certification

### OBJECTIFS ET CONTEXTE

La cybersécurité est un enjeu stratégique pour l'économie et les institutions : elle s'est imposée ces dernières années à tous ceux qui utilisent des outils numériques, du particulier aux entreprises, en passant par les institutions nationales. Les entreprises ont aujourd'hui bien conscience de ces risques, et recrutent des spécialistes pour pallier les défauts de sécurité des matériels et logiciels préexistants, pour protéger leurs infrastructures et leur activité, et pour prévenir les attaques. C'est à ce besoin particulier que s'attache à répondre la certification Expert en Cybersécurité (MS), pour que les entreprises puissent recruter des experts capables de relever les défis liés à la sécurité des systèmes informatiques.

### ACTIVITÉS VISÉES

Analyse des besoins en sécurité informatique de l'entreprise :

- Identification et qualification des risques (matrices d'impact et de probabilité, mise en œuvre de méthodologies reconnues)
- Audits et pentesting (tests d'intrusion, conformité, robustesse)
- Préconisations en matière de prévention et de sécurité (mesures techniques et organisationnelles)

Pilotage de projets de sécurité du SI :

- Planification et management des projets et gestion des interdépendances au sein et entre les projets (plannings, livrables, jalons critiques).
- Management et animation de l'équipe (attribution des rôles et responsabilités, supervision des activités)
- Reporting de l'avancement des chantiers (rédaction de rapports, participation aux comités de pilotage)
- Exploitation des CDC technique ou fonctionnel (analyse des besoins exprimés, déclinaison des spécifications)

Déploiement et administration des solutions de sécurité des SI :

- Choix et configuration des paramètres du SI
- Maintenance des systèmes de sécurité SI (mises à jour, patch management, journaux de sécurité)
- Gestion et exploitation des droits d'accès
- Mise à jour de la documentation (documentation des incidents, maintien des procédures opérationnelles)
- Vérification de l'application des règles de sécurité (audits internes, identification des écarts, mesures correctives)
- Identification des vulnérabilités (analyses automatisées, simulations d'attaque)

Gestion des incidents et des crises cyber:

- Création et déploiement d'un PCRA
- Pilotage du SOC (Security Operations Center) : coordination des analystes, exploitation des solutions SIEM

- Détection des incidents, intrusions et anomalies réseau (outils IDS/IPS, analyse comportementale UEBA)
- Mesures d'impact (matrices) des incidents et qualification des incidents (classification par gravité et criticité)
- Communication interne et externe (dissémination et reporting, déclarations d'incidents)
- Post-mortem des incidents (analyse des causes racines RCA)

Soutien et conseil à la construction d'une architecture informatique fonctionnelle sécurisée :

- Veille sur les évolutions techniques, technologiques et réglementaires en matière de cybersécurité
- Sensibilisation et formation sur les sujets de sécurité des SI
- Conseil stratégique sur la qualité en matière de robustesse et résilience du système (analyse des tendances et préconisations)
- Vérification de la conformité réglementaire

#### COMPÉTENCES ATTESTÉES

Auditer l'infrastructure du SI en matière de cybersécurité (infra réseau, système d'exploitation, serveurs, données et applications), en mesurant la conformité (méthodologie EBIOS RM) par rapport aux standards organisationnels (PSSI et procédures internes), technologiques (ISO 27001, NIST) et réglementaires (RGPD), afin d'identifier et qualifier les failles, les risques et les vulnérabilités.

Définir le périmètre de sécurité du SI (par classification des actifs et matrice de criticité), en s'appuyant sur des normes et/ou des méthodes de référence (exemple : NIS2, ISO 2700X...), afin de recenser les éléments à surveiller (données sensibles, infra, applications, logiciels, hardware, facteur humain).

Analyser par comparaison critique diverses solutions technologiques (pour la gestion des endpoints, des identités, la détection, la surveillance...), en réalisant un benchmark détaillé des solutions possibles (fonctionnalités clés, compatibilité, ergonomie, fréquence de mise à jour), selon des critères de sélection identifiés (performance technique, évolutivité, intégration, coût), afin de réaliser les choix adaptés aux besoins métiers de l'entreprise.

Définir des paramètres techniques et opérationnels (architecture réseau, politique d'accès, chiffrement des données), en priorisant selon la criticité de la menace (en utilisant par exemple un tableau de bord de priorisation de la menace, ou en calculant le ROI de résolution), la vulnérabilité des systèmes d'information et les critères CID (confidentialité, intégrité, disponibilité), afin de gérer les priorités des projets SI et les interdépendances de l'ensemble des projets en cours ou à venir.

Gérer l'encadrement d'une équipe, en affectant les tâches accessibles relatives aux compétences des membres de l'équipe (par le biais d'une matrice type Skill Matrix ou d'un framework NIST NICE ou ESCF) et en utilisant les outils de gestion de projet accessibles et adaptés au contexte (en cascade ou en agilité), pour optimiser la réalisation des projets de cybersécurité tant en responsabilité hiérarchique (développement des compétences de l'équipe) que fonctionnelle (à l'aide d'une matrice RACI).

Concevoir des rapports synthétiques (de type état d'avancement, analyse des choix opérationnels, format ISO pour les audits), en justifiant les choix opérés en fonction du contexte (grâce à des Weighted Scoring Models), afin d'informer la hiérarchie et les parties prenantes de l'état d'avancement des projets informatiques.

Analyser les cahiers des charges technique et fonctionnel des projets du SI, en tenant compte des objectifs, des contraintes (temporelles, budgétaires, réglementaires) et des moyens disponibles (compatibilité de l'existant, limitations de la legacy), pour la réalisation du projet, afin de garantir la sécurité informatique du produit final (adossé par exemple au modèle STRIDE).

Mettre en œuvre les règles de filtrage appropriées (comme le principe du moindre privilège, le blocage par défaut, l'inspection profonde des paquets, l'inspection des protocoles courants), en déployant des solutions de sécurité adaptées au contexte (pare-feu, IDS/IPS, WAF, Proxy sécurisé, système anti-DDoS...), afin de bloquer des attaques sans entraver ou ralentir le fonctionnement du SI ou l'activité de l'entreprise.

Définir les éléments techniques de sécurité et les outils à mettre en œuvre, en déployant et maintenant les protocoles de sécurité (exemple : chiffrement, certificats, cloisonnement, filtrage, détection et protection contre les intrusions, authentification forte et contrôle d'accès), la sécurité physique (par sécurisation des équipements) et les outils de contrôle, afin d'entretenir la sécurité des systèmes et des réseaux en fonction du contexte de l'entreprise.

Sélectionner des solutions de gestion des accès et d'identité adaptées au contexte et besoins (intégration de mécanismes SSO, MFA, RBAC et ABAC), en identifiant tous les accès internes et externes existants et en implémentant et gérant les mécanismes d'autorisation (portail SSO), afin de mettre en place des architectures IAM (Identity Access Management).

Rédiger des rapports d'analyse et des documents de référence standardisés (exemple: rapport de faille critique) en utilisant des templates, des scanners ou des outils de type Nessus, Qualys ou Burp Suite, afin d'informer les différents métiers des vulnérabilités découvertes, et de préconiser des mesures correctives ou préventives, de rendre

compte et documenter.

Superviser la mise en œuvre des solutions de cybersécurité respectant les principes du DevSecOps, en définissant des indicateurs de suivis appropriés (tableaux de bord pour mesurer les indicateurs comme MTTR, taux d'alerte fausse/négative) et des outils de surveillance (exemple : SIEM4), pour mesurer leur efficacité et garantir le niveau de sécurité requis.

Identifier les différents types d'attaques réseau (détection des attaques DDoS, phishing, exploitation de failles), ainsi que les mécanismes de sécurité permettant d'y faire face, en utilisant des méthodes adaptées (UEBA, surveillance des adresses IP, monitoring des terminaux et des réseaux, détection de trafic inhabituel...) pour implémenter les mécanismes de sécurité les plus efficaces face aux menaces identifiées.

Etablir un plan de continuité et de reprise d'activités (PCRA), en définissant les processus (redondance des serveurs), en identifiant les ressources techniques (backups réguliers) et humaines ainsi que les moyens disponibles ou nécessaires et en simulant des scénarios de test (ex: panne simulée de data center), afin de rétablir le bon fonctionnement du SI et de l'activité de l'entreprise.

Animer la capitalisation de l'expérience au sein des équipes projet IT (debriefs, gestion des connaissances, méthodes de débriefing telles que 5 whys, Ishikawa) en analysant régulièrement les indicateurs de performance et les incidents (intrusions réseau, coût des downtime, MTBD, MTTR, MTTC...) et en créant un espace de documentation partagée (type Notion, Confluence ou Sharepoint) dans un objectif d'amélioration continue.

Classer les incidents détectés, en mobilisant les outils de surveillance adaptés au contexte (classification selon matrices de gravité, vraisemblance, niveaux de menace, création de workflows automatisés pour la gestion des incidents...) et des méthodes telles que EBIOS ou une cartographie des risques, pour anticiper ou réagir à une cyberattaque du SI et en gérer les conséquences.

Analyser les incidents de sécurité détectés (identification de patterns malveillants dans les logs, corrélation des événements), en mobilisant les outils adaptés de surveillance (l'analyse de risque, le monitoring en direct, ou au travers d'un CERT, débogueurs réseau), afin de réagir efficacement à une cyberattaque du système.

Communiquer auprès des parties prenantes, y compris en situation de handicap, en utilisant les supports adéquats (communication visuelle, infographies telles que conseillées par l'ANSSI et adaptés à l'entreprise), et en expliquant les enjeux du projet ou de la stratégie, afin de mobiliser les acteurs pour atteindre les objectifs fixés.

Réaliser des analyses "forensics", en déployant différentes méthodes (analyse à froid, à chaud, en temps réel, analyse mémoire, carving de données), afin d'adapter la campagne de tests et la stratégie future en matière de cybersécurité et de permettre d'autres types d'investigation (administratives, criminelles, civiles, réglementaires).

Organiser l'animation d'un système de veille active, en s'informant auprès des éditeurs, prestataires et organismes de référence tels que l'ANSSI (agrégation de flux RSS, gestion collaborative, participation à des collectifs, abonnements à une TIP) et en diffusant ces informations de manière accessible et régulière (par exemple par le biais d'un rapport mensuel sur les menaces émergentes), afin d'être toujours à la pointe en matière de menaces cyber et de réglementations en vigueur ou à venir.

Définir une charte de sécurité au sein de l'organisation, en rédigeant le ou les documents relatifs à l'application des bonnes pratiques en entreprise à destination des collaborateurs (voire par le biais d'audits internes périodiques) et en organisant des sessions d'information et de formation à l'hygiène cyber, afin d'ancrer les réflexes de sécurité dans l'entreprise et d'informer sur l'importance de la responsabilité individuelle et collective.

Conseiller la direction sur les projets et investissements à conduire (par le biais d'études de rentabilité: ROI, TCO), en présentant des indicateurs formalisés (sous forme de tableaux de bord stratégiques, d'analyse SWOT), des possibles conséquences des réglementations à venir, des risques et impacts sur l'activité de l'entreprise en cas d'attaque cyber, afin d'aider à la prise de décision et à la gouvernance du SI.

Identifier les droits, les obligations et normes applicables en matière de sécurité des SI, par le biais d'un registre de conformité, en s'appuyant sur les standards et normes relatives à la cybersécurité (exemples : RGPD, ISO27001, NIS 2, etc.) et en les comparant à l'état des lieux du SI de l'entreprise (en utilisant par exemple un logiciel GRC), afin de garantir leur conformité réglementaire et normative.

## Blocs de compétences

### RNCP41445BC01 — Concevoir des projets de sécurité des systèmes d'information

#### LISTE DE COMPÉTENCES

Auditer l'infrastructure du SI en matière de cybersécurité (infra réseau, système d'exploitation, serveurs, données et applications), en mesurant la conformité (méthodologie EBIOS RM) par rapport aux standards organisationnels (PSSI

et procédures internes), technologiques (ISO 27001, NIST) et réglementaires (RGPD), afin d'identifier et qualifier les failles, les risques et les vulnérabilités.

Définir le périmètre de sécurité du SI (par classification des actifs et matrice de criticité), en s'appuyant sur des normes et/ou des méthodes de référence (exemple : NIS2, ISO 2700X...), afin de recenser les éléments à surveiller (données sensibles, infra, applications, logiciels, hardware, facteur humain).

Analyser par comparaison critique diverses solutions technologiques (pour la gestion des endpoints, des identités, la détection, la surveillance...), en réalisant un benchmark détaillé des solutions possibles (fonctionnalités clés, compatibilité, ergonomie, fréquence de mise à jour), selon des critères de sélection identifiés (performance technique, évolutivité, intégration, coût), afin de réaliser les choix adaptés aux besoins métiers de l'entreprise.

Définir des paramètres techniques et opérationnels (architecture réseau, politique d'accès, chiffrement des données), en priorisant selon la criticité de la menace (en utilisant par exemple un tableau de bord de priorisation de la menace, ou en calculant le ROI de résolution), la vulnérabilité des systèmes d'information et les critères CID (confidentialité, intégrité, disponibilité), afin de gérer les priorités des projets SI et les interdépendances de l'ensemble des projets en cours ou à venir.

Gérer l'encadrement d'une équipe, en affectant les tâches accessibles relatives aux compétences des membres de l'équipe (par le biais d'une matrice type Skill Matrix ou d'un framework NIST NICE ou ESCF) et en utilisant les outils de gestion de projet accessibles et adaptés au contexte (en cascade ou en agilité), pour optimiser la réalisation des projets de cybersécurité tant en responsabilité hiérarchique (développement des compétences de l'équipe) que fonctionnelle (à l'aide d'une matrice RACI).

Concevoir des rapports synthétiques (de type état d'avancement, analyse des choix opérationnels, format ISO pour les audits), en justifiant les choix opérés en fonction du contexte (grâce à des Weighted Scoring Models), afin d'informer la hiérarchie et les parties prenantes de l'état d'avancement des projets informatiques.

Analyser les cahiers des charges technique et fonctionnel des projets du SI, en tenant compte des objectifs, des contraintes (temporelles, budgétaires, réglementaires) et des moyens disponibles (compatibilité de l'existant, limitations de la legacy), pour la réalisation du projet, afin de garantir la sécurité informatique du produit final (adossé par exemple au modèle STRIDE).

#### MODALITÉS D'ÉVALUATION

##### Etude de cas

à partir d'une situation donnée, en utilisant la méthodologie EBIOS RM, le candidat doit:

- mener un audit organisationnel,
- fournir une analyse de risques (types, gravité, vraisemblance),
- émettre des préconisations et des mesures de traitement du risque.

Livrable : rapport écrit étayé par défense orale.

Travail de groupe, notation individuelle.

Mise en situation professionnelle:

Le candidat doit

- déployer un SIEM à partir d'un CDC donné,
- proposer une architecture HLD,
- rédiger un rapport de déploiement étape par étape, en précisant sa méthode managériale et en justifiant la constitution de son équipe SI.

Livrable : un rapport écrit défendu en soutenance.

Rendu de groupe, notation individuelle.

## **RNCP41445BC02 — Mettre en œuvre et administrer des solutions de sécurité du système d'information**

#### LISTE DE COMPÉTENCES

Mettre en œuvre les règles de filtrage appropriées (comme le principe du moindre privilège, le blocage par défaut, l'inspection profonde des paquets, l'inspection des protocoles courants), en déployant des solutions de sécurité adaptées au contexte (pare-feu, IDS/IPS, WAF, Proxy sécurisé, système anti-DDoS...), afin de bloquer des attaques sans entraver ou ralentir le fonctionnement du SI ou l'activité de l'entreprise.

Définir les éléments techniques de sécurité et les outils à mettre en œuvre, en déployant et maintenant les protocoles de sécurité (exemple : chiffrement, certificats, cloisonnement, filtrage, détection et protection contre les intrusions, authentification forte et contrôle d'accès), la sécurité physique (par sécurisation des équipements) et les outils de contrôle, afin d'entretenir la sécurité des systèmes et des réseaux en fonction du contexte de l'entreprise.

Sélectionner des solutions de gestion des accès et d'identité adaptées au contexte et besoins (intégration de mécanismes SSO, MFA, RBAC et ABAC), en identifiant tous les accès internes et externes existants et en

implémentant et gérant les mécanismes d'autorisation (portail SSO), afin de mettre en place des architectures IAM (Identity Access Management).

Rédiger des rapports d'analyse et des documents de référence standardisés (exemple: rapport de faille critique) en utilisant des templates, des scanners ou des outils de type Nessus, Qualys ou Burp Suite, afin d'informer les différents métiers des vulnérabilités découvertes, et de préconiser des mesures correctives ou préventives, de rendre compte et documenter.

Superviser la mise en œuvre des solutions de cybersécurité respectant les principes du DevSecOps, en définissant des indicateurs de suivis appropriés (tableaux de bord pour mesurer les indicateurs comme MTTR, taux d'alerte fausse/négative) et des outils de surveillance (exemple : SIEM4), pour mesurer leur efficacité et garantir le niveau de sécurité requis.

Identifier les différents types d'attaques réseau (détection des attaques DDoS, phishing, exploitation de failles), ainsi que les mécanismes de sécurité permettant d'y faire face, en utilisant des méthodes adaptées (UEBA, surveillance des adresses IP, monitoring des terminaux et des réseaux, détection de trafic inhabituel...) pour implémenter les mécanismes de sécurité les plus efficaces face aux menaces identifiées.

#### MODALITÉS D'ÉVALUATION

Travaux pratiques:

Le candidat doit:

- déployer des méthodes d'authentification,
- gérer une identification biométrique,
- faire l'inventaire des éléments de sécurité à protéger,
- identifier des KPI et les présenter sous forme de tableau de bord,
- identifier et lister les vulnérabilités d'un système donné.

Livrable : plusieurs rapports et comptes-rendus techniques.

Travail individuel ou de groupe, notation individuelle.

Etude de cas:

Le candidat va déployer une identité numérique IAM.

Livrable: une démonstration et une soutenance orale illustrée du travail.

Travail et notation individuels.

Mise en situation professionnelle:

le candidat doit:

- configurer des firewalls dans un réseau,
- définir et implémenter une politique de filtrage et de routage,
- configurer une politique d'authentification,
- mettre en place un réseau VPN,
- configurer un proxy.

Livrable : compte-rendu écrit individuel, notation individuelle.

Mise en situation professionnelle:

Le candidat doit concevoir, déployer et configurer une architecture logicielle et matérielle pour la détection et remédiation d'attaques VoIP SIP DDoS dans un environnement SDN.

Livrable : un rapport écrit documenté qui analyse et illustre les décisions.

Travail de groupe, notation individuelle.

### **RNCP41445BC03 — Gérer les incidents et les situations de crise**

#### LISTE DE COMPÉTENCES

Etablir un plan de continuité et de reprise d'activités (PCRA), en définissant les processus (redondance des serveurs), en identifiant les ressources techniques (backups réguliers) et humaines ainsi que les moyens disponibles ou nécessaires et en simulant des scénarios de test (ex: panne simulée de data center), afin de rétablir le bon fonctionnement du SI et de l'activité de l'entreprise.

Animer la capitalisation de l'expérience au sein des équipes projet IT (debriefs, gestion des connaissances, méthodes de debriefing telles que 5 whys, Ishikawa) en analysant régulièrement les indicateurs de performance et les incidents (intrusions réseau, coût des downtime, MTDD, MTTR, MTTC...) et en créant un espace de documentation partagée (type Notion, Confluence ou Sharepoint) dans un objectif d'amélioration continue.

Classer les incidents détectés, en mobilisant les outils de surveillance adaptés au contexte (classification selon matrices de gravité, vraisemblance, niveaux de menace, création de workflows automatisés pour la gestion des incidents...) et des méthodes telles que EBIOS ou une cartographie des risques, pour anticiper ou réagir à une

cyberattaque du SI et en gérer les conséquences.

Analyser les incidents de sécurité détectés (identification de patterns malveillants dans les logs, corrélation des événements), en mobilisant les outils adaptés de surveillance (l'analyse de risque, le monitoring en direct, ou au travers d'un CERT, débogueurs réseau), afin de réagir efficacement à une cyberattaque du système.

Communiquer auprès des parties prenantes, y compris en situation de handicap, en utilisant les supports adéquats (communication visuelle, infographies telles que conseillées par l'ANSSI et adaptés à l'entreprise), et en expliquant les enjeux du projet ou de la stratégie, afin de mobiliser les acteurs pour atteindre les objectifs fixés.

Réaliser des analyses "forensics", en déployant différentes méthodes (analyse à froid, à chaud, en temps réel, analyse mémoire, carving de données), afin d'adapter la campagne de tests et la stratégie future en matière de cybersécurité et de permettre d'autres types d'investigation (administratives, criminelles, civiles, réglementaires).

#### MODALITÉS D'ÉVALUATION

Travaux pratiques:

Le candidat doit:

- détecter, caractériser et corriger des intrusions et anomalies réseau.

Livrable : un rapport écrit détaillé et illustré de ses choix.

Travail et notation individuels.

Etude de cas:

En possession des éléments d'une mise en situation réelle ou fictive, le candidat doit:

- cartographier les acteurs en amont d'une situation de crise,
- classifier les niveaux de criticité des situations, en fonction des CID et de la méthodologie EBIOS RM,
- organiser la gestion de crise,
- communiquer en interne et en externe sur la situation de crise,
- constituer des éléments d'une bibliothèque de crise à destination du SOC.

Livrable : une cartographie des acteurs, des tableaux détaillés, des supports de communication, des fiches documentaires, que le candidat présentera, étayera et argumentera lors d'une soutenance orale.

Travail de groupe, notation individuelle.

Travaux pratiques:

Le candidat doit, à partir d'éléments fournis, analyser une série d'incidents sous le prisme du digital forensics (post mortem).

Livrable: un dossier synthétique de ses travaux.

Travail en binôme, notation individuelle.

### **RNCP41445BC04 — Garantir la veille, le conseil et l'information en matière de sécurité des systèmes d'information**

#### LISTE DE COMPÉTENCES

Organiser l'animation d'un système de veille active, en s'informant auprès des éditeurs, prestataires et organismes de référence tels que l'ANSSI (agrégation de flux RSS, gestion collaborative, participation à des collectifs, abonnements à une TIP) et en diffusant ces informations de manière accessible et régulière (par exemple par le biais d'un rapport mensuel sur les menaces émergentes), afin d'être toujours à la pointe en matière de menaces cyber et de réglementations en vigueur ou à venir.

Définir une charte de sécurité au sein de l'organisation, en rédigeant le ou les documents relatifs à l'application des bonnes pratiques en entreprise à destination des collaborateurs (voire par le biais d'audits internes périodiques) et en organisant des sessions d'information et de formation à l'hygiène cyber, afin d'ancrer les réflexes de sécurité dans l'entreprise et d'informer sur l'importance de la responsabilité individuelle et collective.

Conseiller la direction sur les projets et investissements à conduire (par le biais d'études de rentabilité: ROI, TCO), en présentant des indicateurs formalisés (sous forme de tableaux de bord stratégiques, d'analyse SWOT), des possibles conséquences des réglementations à venir, des risques et impacts sur l'activité de l'entreprise en cas d'attaque cyber, afin d'aider à la prise de décision et à la gouvernance du SI.

Identifier les droits, les obligations et normes applicables en matière de sécurité des SI, par le biais d'un registre de conformité, en s'appuyant sur les standards et normes relatives à la cybersécurité (exemples : RGPD, ISO27001, NIS 2, etc.) et en les comparant à l'état des lieux du SI de l'entreprise (en utilisant par exemple un logiciel GRC), afin de garantir leur conformité réglementaire et normative.

#### MODALITÉS D'ÉVALUATION

Etude de cas

Le candidat doit, dans le cadre d'une recherche bibliographique analytique, et à partir de cas réels ou fictifs donnés:

- cadrer la réglementation applicable,
- vérifier l'application du contexte normatif concerné,

Livrable : un rapport synthétique argumenté et illustré reprenant l'ensemble des cas donnés.

Travail et notation individuels.

Etude de cas:

Le candidat doit, dans le cadre d'une situation réelle ou fictive,

- procéder à l'analyse de l'application des normes ISO2700x
- vérifier la conformité au RGPD,
- identifier les enjeux juridiques et réglementaires de l'entreprise en question et créer des supports de sensibilisation à destination des employés.

Livrable : un rapport détaillé et argumenté de ses choix.

Travail de groupe, notation individuelle.

## Secteur d'activité et type d'emploi

### SECTEURS D'ACTIVITÉS

L'expert en cybersécurité (MS) peut exercer dans de grandes entreprises tout comme dans des PME. En fonction du secteur, l'expert en cybersécurité (MS) peut intervenir soit pour le compte d'un prestataire de service (par exemple une ESN) auprès d'une entreprise ou être interne à l'entreprise.

Ce métier est présent dans tous les secteurs, y compris la banque, le commerce, l'industrie, la défense, les services.

### TYPE D'EMPLOIS ACCESSIBLES

Les différents emplois visés (attendu que les termes « cybersécurité » et « sécurité informatique » recouvrent la même réalité) : Expert en cybersécurité - Consultant en cybersécurité - Responsable cybersécurité

Les autres intitulés métiers mobilisant la sécurité informatique dans leur pratique (ici encore, les intitulés anglophones sont nombreux, même au sein du marché de l'emploi français) : Architecte sécurité et réseaux - Chief Information Security Officer (CISO) - Manager de la Sécurité et des Risques de l'Information (MSRI) - Responsable risque sécurité réseaux informatiques - Responsable Sécurité de l'information - Responsable sécurité des réseaux informatiques - Responsable sécurité des systèmes d'information (RSSI)

### RÉGLEMENTATIONS D'ACTIVITÉ

La cybersécurité est un sujet qui concerne de nombreuses entreprises, secteurs et organisations, indépendamment de leur taille ou secteur d'activité. Ces risques sont généralement liés à l'activité même de l'entreprise et peuvent en menacer la survie (arrêt de la production, suppression de bases de données, rançongiciels, etc...). Néanmoins, les entreprises qui présentent des dangers de sécurité informatique liés à la nature de leur activité, telles que le secteur financier (données bancaires), celui de la santé (données personnelles des patients), des infrastructures stratégiques du pays (énergie, sécurité, services nationaux), comportent des enjeux de cybersécurité encore plus stratégiques.

Les trois grands champs d'application concernent : la sécurité des systèmes d'information, la confiance numérique, l'obligation de notification des incidents de sécurité.

Et quelques exemples de normes, règles et standards qui s'appliquent régulièrement : les directives de l'ANSSI, les directives NIS et NIS2, le RGPD, et la norme ISO 27001

## Marché du travail

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

|                                            |                                                                                                                              |
|--------------------------------------------|------------------------------------------------------------------------------------------------------------------------------|
| <b>Tension de recrutement (DARES 2024)</b> | Élevée (4/5)<br>Moyenne pondérée par l'emploi ; les familles ci-dessous s'échelonnent de 3 à 5 sur 5.                        |
| <b>Facteurs principaux</b>                 | Manque de main-d'œuvre disponible, Lien formation-emploi                                                                     |
| <b>Salaire médian (mensuel)</b>            | 2 781 €                                                                                                                      |
| <b>Diplôme le plus fréquent</b>            | Diplôme de niveau bac+5 ou plus (doctorat, master ou équivalent) en communication et information (41 % des actifs en emploi) |

|                                          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Familles professionnelles (FAP)</b>   | M1X80 — Techniciens d'étude et de développement en informatique · tension 4/5 (Élevée)<br>M1X81 — Techniciens de production, d'exploitation, d'installation, et de maintenance, support et services aux utilisateurs en informatique · tension 4/5 (Élevée)<br>M2X90 — Ingénieurs et cadres d'étude, recherche et développement en informatique et télécom · tension 5/5 (Très élevée)<br>M2X92 — Responsables et cadres de la production, de l'exploitation et de la maintenance informatique et télécom · tension 3/5 (Modérée)<br>M2X93 — Experts et consultants en systèmes d'information · tension 5/5 (Très élevée) |
| <b>Projets de recrutement (BMO 2026)</b> | 41 765                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>Jugés difficiles à recruter</b>       | 50 %                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>Emplois saisonniers</b>               | 2 %                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>Familles professionnelles (FAP)</b>   | M1X80 — Techniciens d'étude et de développement en informatique<br>M1X81 — Techniciens de production, d'exploitation, d'installation, et de maintenance, support et services aux utilisateurs en informatique<br>M2X90 — Ingénieurs et cadres d'étude, recherche et développement en informatique et télécom<br>M2X92 — Responsables et cadres de la production, de l'exploitation et de la maintenance informatique et télécom<br>M2X93 — Experts et consultants en systèmes d'information                                                                                                                               |

## Voies d'accès

### PRÉREQUIS À L'ENTRÉE EN FORMATION

Sont recevables les candidatures des 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 journal officiel) ;

Diplôme d'une école de management, privée ou consulaire, conférant le grade de master (formations évaluées par la CEFDG, liste publiée au bulletin officiel du MESR) ;

Diplôme de 3ème cycle habilité par les autorités universitaires (Diplôme national de master, DEA, DESS, ...) ou diplôme professionnel de niveau BAC + 5 ;

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

Titre inscrit au Répertoire national des certifications professionnelles (RNCP) niveau 7 ;

Diplôme étranger équivalent aux diplômes français exigés ci-dessus.

Conditions d'accès dérogatoires:

a) 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 a minima de 5 années d'expérience professionnelle pour lesquelles les activités exercées ont un lien avéré avec les compétences professionnelles visées par la formation.

b) 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 trois ans d'expérience professionnelle en lien avec la formation visée.

? Diplôme de licence (L3) ou grade de Licence ou titre inscrit au RNCP niveau 6 (ancienne nomenclature niveau II) justifiant d'une expérience professionnelle de 3 ans minimum, en lien avec la formation visée

Le pourcentage total des dérogations prévues au a) et au b) ci-dessus ne doit pas excéder 40%.

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

Le jury est composé de 5 personnes : 2 personnes internes représentant l'école (directeur des programmes et directeur), et 3 personnes externes issues du monde professionnel.

Le jury de la délivrance de la certification est composé a minima de 50% professionnels du secteur dont l'un est président du jury.

## Base légale

|                                      |            |
|--------------------------------------|------------|
| Date de décision                     | 27/10/2025 |
| Durée de l'enregistrement            | 5 ans      |
| Date d'échéance de l'enregistrement  | 27/10/2030 |
| Date de dernière délivrance possible | 26/10/2034 |

## Statistiques

| Année | Certifiés | Dont VAE | Insertion 6 mois | Métier 2 ans |
|-------|-----------|----------|------------------|--------------|
| 2023  | 15        | 0        | 79 %             | —            |
| 2022  | 12        | 0        | 77 %             | 90 %         |

## Pour plus d'informations

LIEN VERS LE DESCRIPTIF

<https://imt-nord-europe.fr/annuaire-formations/mastere-specialise-en-ingenierie-de-la-cybersecurite/>

**Fiche officielle (France Compétences)**

<https://www.francecompetences.fr/recherche/rncp/41445/>

## Où se former

|                        |         |
|------------------------|---------|
| Formations référencées | 1       |
| Organismes             | 1       |
| Régions couvertes      | 1       |
| Prix indicatif         | 9 000 € |
| Durée                  | 1392 h  |

Offre de formation — MonCompteFormation (Caisse des Dépôts), licence ouverte.

## Entrées et sorties de formation

|                        |         |
|------------------------|---------|
| Entrées en formation   | 1       |
| Parcours menés à terme | 0       |
| Taux d'achèvement      | 0 %     |
| Période                | 09/2026 |

Entrées et sorties — Caisse des Dépôts (open data), tous organismes confondus.

## Demande CPF — formations engagées

|                        |         |
|------------------------|---------|
| Dossiers CPF engagés   | 1       |
| Montant total engagé   | 5 123 € |
| Coût moyen par dossier | 5 123 € |
| Durée moyenne          | 1392 h  |
| Période                | 07/2026 |

