

# Expert en renseignement et investigation sur les cybermenaces

RNCP42515 · RNCP · Publiée

## L'essentiel

|                         |                            |
|-------------------------|----------------------------|
| Niveau de qualification | Niveau 7                   |
| Code(s) NSF             | 326, 344t                  |
| Formacode(s)            | 31045, 42885, 46342        |
| Code(s) ROME            | M1802, M1805               |
| Type d'enregistrement   | Enregistrement sur demande |
| Date d'enregistrement   | 26/06/2026                 |
| Date d'échéance         | 26/06/2029                 |

## Certificateur(s)

2600 · SIRET : 89344030500025

## Résumé de la certification

### OBJECTIFS ET CONTEXTE

L'intensification des cybermenaces, leur instrumentalisation à des fins géopolitiques et l'accélération du cadre réglementaire européen (NIS2, DORA, Cyber Resilience Act) créent un besoin impérieux de professionnels capables non seulement de défendre les systèmes d'information, mais de comprendre l'adversaire, d'anticiper ses modes opératoires et de produire du renseignement exploitable par les décideurs.

L'expert en renseignement et investigation sur les cybermenaces se positionne à l'intersection de la cybersécurité, du renseignement stratégique et de l'investigation numérique. Il planifie et conduit des opérations de collecte multi-sources (OSINT, SOCMINT, Dark Web), analyse et qualifie les menaces en s'appuyant sur des référentiels tels que MITRE ATT&CK, profile les acteurs malveillants en contextualisant leurs actions dans leur environnement géopolitique et économique, et conduit des investigations forensiques et financières en appui des enquêtes judiciaires ou internes. Il produit des rapports de renseignement à différents niveaux (stratégique pour les instances dirigeantes, tactique pour les équipes opérationnelles) et assure une veille permanente sur les menaces émergentes, notamment celles liées à l'intelligence artificielle.

Ce profil hybride, combinant profondeur technique et hauteur de vue stratégique, constitue une réponse aux besoins croissants des organisations confrontées aux cybermenaces, qu'il s'agisse d'entreprises de la défense, du secteur bancaire, d'acteurs spécialisés en threat intelligence ou de services régaliens.

### ACTIVITÉS VISÉES

- Collecte et traçage du renseignement multi-sources
- Structuration, automatisation et exploitation des données collectées
- Qualification technique et caractérisation des menaces
- Profilage des acteurs et analyse de contexte
- Investigation forensique
- Investigation financière et détection de fraudes
- Production et analyse prospective du renseignement
- Communication stratégique et sensibilisation
- Veille stratégique et anticipation
- Coopération, cadre juridique et souveraineté

## COMPÉTENCES ATTESTÉES

Planifier et conduire des opérations de collecte de renseignement d'origine numérique (OSINT, GEOINT, SOCMINT, Dark Web, ...) en définissant les objectifs, les sources pertinentes et les méthodologies adaptées, en veillant à l'accessibilité des méthodologies et livrables selon les principes de la conception universelle (profils types de destinataires, structuration multi-niveaux, lisibilité, accessibilité numérique des supports) pour des professionnels aux profils diversifiés, y compris en situation de handicap, afin d'alimenter l'analyse de la menace en données fiables et exploitables.

Exploiter les outils et techniques de traçage numérique pour identifier et corréler les empreintes digitales (adresses IP, domaines, identifiants, métadonnées) d'acteurs malveillants, en respectant le cadre légal et normatif applicable (RGPD, Code pénal, IGI 1300, II 901, ...) et les exigences de protection du secret, afin de cartographier les menaces pesant sur les systèmes d'information.

Détecter et analyser les signaux faibles issus des sources ouvertes, du Dark Web et des réseaux sociaux, en identifiant les indicateurs précurseurs d'activités malveillantes, en intégrant la prévention des risques professionnels liés à l'exposition prolongée aux contenus sensibles et au travail sur écran, afin d'anticiper les menaces avant qu'elles ne frappent les systèmes d'information.

Automatiser les processus de collecte de données en développant ou paramétrant des scripts et outils de surveillance en arbitrant les choix d'automatisation entre performance, efficacité opérationnelle et sobriété des ressources mobilisées (fréquence des requêtes, volume de stockage, empreinte computationnelle), pour assurer une veille continue et optimiser l'efficacité des opérations de renseignement sur les systèmes d'information.

Structurer, indexer et qualifier les données collectées en les organisant selon des taxonomies et formats standardisés (STIX/TAXII, JSON structuré), en optimisant les ressources computationnelles dans une démarche de sobriété numérique et de transition écologique, afin de garantir leur exploitabilité, leur traçabilité et leur interopérabilité avec les plateformes d'analyse.

Exploiter les outils d'intelligence artificielle et d'apprentissage automatique pour optimiser le traitement de données massives (textuelles, visuelles, comportementales) collectées lors des opérations de renseignement, en évaluant de manière critique la fiabilité et les biais des résultats produits, dans le cadre de la transition numérique des opérations de renseignement.

Analyser les indicateurs de compromission (IoCs) et les artefacts techniques d'une attaque, incluant l'analyse de malware de premier niveau (statique, comportementale), en utilisant les référentiels standards (MITRE ATT&CK, STIX/TAXII), et en structurant les productions analytiques selon les principes de la conception universelle (hiérarchisation, alternatives aux représentations graphiques telles que matrices ATT&CK ou graphes d'attribution, compatibilité avec les outils d'assistance), pour qualifier précisément le mode opératoire technique de l'adversaire et évaluer les risques pesant sur les systèmes d'information.

Cartographier les infrastructures d'attaque (serveurs C2, domaines malveillants, chaînes d'approvisionnement) en corrélant les données techniques collectées, pour identifier l'étendue de la menace et sécuriser les organisations ciblées.

Détecter et caractériser les menaces issues de l'intelligence artificielle (deepfakes audio/vidéo, contenus synthétiques, phishing automatisé par IA, empoisonnement de modèles, attaques adversariales), en intégrant la prévention des risques professionnels liés à l'exposition aux contenus perturbants, pour qualifier les nouveaux modes opératoires adverses.

Intégrer le renseignement d'origine électromagnétique (ROEM/SIGINT) dans l'analyse des cybermenaces, en corrélant les produits de renseignement technique avec les données collectées en sources ouvertes et les indicateurs de compromission, afin de produire une caractérisation enrichie de la menace.

Établir des profils d'acteurs malveillants (APT, cybercriminels, hacktivistes) en analysant leurs motivations, schémas comportementaux, capacités et historiques d'activité, pour anticiper les menaces avant qu'elles ne frappent les systèmes d'information et orienter les mesures de protection.

Contextualiser les indicateurs techniques dans leur environnement géopolitique, économique, sociétal et normatif, en croisant les données d'analyse technique avec les facteurs de contexte (conflits hybrides, guerre économique, menaces sur les infrastructures de la transition énergétique et écologique), pour produire une qualification multidimensionnelle de la menace et évaluer l'exposition des systèmes d'information au regard des exigences de conformité.

Détecter et analyser les campagnes de manipulation de l'information (désinformation, propagande computationnelle, ingérence numérique étrangère) en identifiant les réseaux d'amplification et les narratifs artificiels, y compris lorsqu'elles ciblent des publics spécifiquement vulnérables ou en situation de handicap, en s'inscrivant dans les enjeux de transition numérique responsable, pour contribuer à la souveraineté informationnelle et à la protection des

processus démocratiques.

Conduire une investigation forensique sur les systèmes d'information en respectant les protocoles de préservation des preuves (chaîne de custody, intégrité des données), en veillant à l'accessibilité des protocoles et restitutions selon les principes de la conception universelle (lisibilité juridique, structure des procès-verbaux, accessibilité pour la diversité des destinataires institutionnels — forces de l'ordre, magistrats, équipe d'investigation) pour les membres de l'équipe en situation de handicap, pour garantir la recevabilité des preuves dans un cadre juridique.

Analyser les artefacts forensiques (systèmes de fichiers, registres, logs, mémoire vive) pour reconstituer la chronologie d'un incident, identifier les vecteurs de compromission et les mécanismes de latéralisation au sein des systèmes d'information, en intégrant la prévention des risques psychosociaux liés à l'examen prolongé d'artefacts sensibles et à la pression temporelle de l'investigation (procédure de relève, limitation de la durée d'exposition, débriefing).

Garantir l'intégrité des éléments de preuve au sein de la chaîne d'enquête judiciaire en documentant les investigations selon les standards requis pour la transmission aux autorités compétentes, en garantissant la protection du secret et la conformité des procédures aux exigences réglementaires, pour faciliter les suites judiciaires éventuelles et contribuer à la sécurisation des systèmes d'information.

Conduire des investigations forensiques sur systèmes intelligents et embarqués (terminaux mobiles, objets connectés, véhicules, drones) en adaptant les méthodologies d'acquisition et d'analyse aux contraintes spécifiques de ces environnements (volatilité, hétérogénéité des formats), en évaluant l'empreinte environnementale des opérations dans une démarche de transition écologique, pour extraire et exploiter les preuves numériques.

Investiguer les flux financiers numériques (cryptomonnaies, blockchain, systèmes de paiement) en mobilisant les outils de traçage et d'analyse transactionnelle, en collaboration avec les cellules de conformité (LCB-FT) et les autorités judiciaires, en s'inscrivant dans la transition numérique des processus d'investigation financière, pour identifier les circuits de blanchiment, de financement illicite ou de fraude.

Détecter et investiguer les fraudes d'origine numérique (fraude documentaire, usurpation d'identité, contenus falsifiés par IA générative, fraude e-commerce ou assimilé) en mobilisant les techniques d'authentification et d'analyse de contenus synthétiques, y compris à l'encontre de victimes spécifiquement en situation de handicap, pour qualifier le mode opératoire et soutenir les démarches d'enquête.

Produire des rapports de renseignement à différents niveaux (stratégique, tactique, opérationnel) en adaptant le contenu, le format et le vocabulaire aux destinataires, en respectant les principes de la conception universelle (strates de lecture explicitées — executive summary, synthèse tactique, annexes techniques ; langue claire ; structuration multi-niveaux ; accessibilité numérique conforme RGAA / WCAG) pour les personnes en situation de handicap, pour répondre aux besoins décisionnels de l'organisation et orienter la posture de sécurité.

Élaborer des scénarios prospectifs d'évolution de la menace en croisant les données techniques, géopolitiques, économiques et réglementaires (NIS2, DORA, CRA, AI Act), en intégrant les enjeux de transition écologique et les menaces pesant sur les infrastructures de la transition énergétique (réseaux intelligents, smart grids, mobilité durable), pour anticiper les risques futurs pesant sur les systèmes d'information et adapter la posture de conformité de l'organisation.

Formuler des recommandations actionnables et priorisées à destination des équipes opérationnelles et des décideurs, en intégrant la prévention des risques liés à la mise en œuvre des mesures correctives sur les systèmes d'information ainsi que la prévention des risques psychosociaux liés à la charge et à la tension des équipes de mise en œuvre (relève, dimensionnement, débriefing) et l'arbitrage performance / efficacité / sobriété des mesures recommandées (empreinte des dispositifs de surveillance et de protection, consommation énergétique), pour renforcer la résilience globale de l'organisation.

Présenter et défendre les analyses devant les instances dirigeantes (COMEX, état-major) en vulgarisant les aspects techniques, en s'inscrivant dans les enjeux de transformation numérique de l'organisation, pour éclairer la prise de décision stratégique et contribuer à la souveraineté des acteurs.

Conseiller les dirigeants sur l'anticipation des cybermenaces et diffuser la culture du renseignement, en s'appuyant sur des exercices de crise et des productions d'analyse stratégique, incluant la promotion de pratiques de renseignement inclusives au sein des équipes (accessibilité des outils d'analyse et de veille pour les collaborateurs en situation de handicap, aménagement des dispositifs d'astreinte et de coopération, sensibilisation aux situations de handicap), pour élever la maturité décisionnelle de l'organisation.

Organiser et piloter une veille structurée multi-dimensionnelle (technologique, géopolitique, réglementaire, sectorielle) incluant la détection de signaux faibles, en veillant à l'accessibilité des outils et livrables de veille selon les principes de la conception universelle (structure des bulletins, langue claire, accessibilité multi-supports, compatibilité avec les outils d'assistance) pour les professionnels en situation de handicap, pour anticiper les évolutions de la menace et

adapter la posture de sécurité des systèmes d'information.

Assurer une veille spécifique sur les menaces émergentes liées à l'intelligence artificielle, aux systèmes autonomes et aux technologies de rupture (quantique, IoT massif, edge computing), en s'inscrivant dans une démarche de transition numérique responsable et de sobriété, pour identifier les nouvelles surfaces d'attaque sur les systèmes d'information.

Évaluer les impacts des évolutions réglementaires et normatives (NIS2, DORA, CRA, AI Act, ...) et des transformations sociétales et environnementales sur le paysage des cybermenaces, en intégrant les enjeux de transition écologique et numérique responsable, pour adapter les priorités de veille, la posture de conformité et les recommandations stratégiques de l'organisation.

Coordonner les échanges avec l'écosystème cyber (CERT, CSIRT, ANSSI, forces de l'ordre, ISAC) en respectant les protocoles de partage d'information (TLP), en intégrant la prévention des risques liés à la gestion de situations d'urgence et d'astreinte, pour enrichir la connaissance de la menace et sécuriser les chaînes de valeur.

Garantir le respect du cadre juridique, normatif et éthique (RGPD, Code pénal, IGI 1300, II 901, secret professionnel, protection du secret de la défense nationale, etc.) dans la conduite des opérations de renseignement et d'investigation, et venir en soutien technique aux enquêtes en collaboration avec les autorités compétentes, pour contribuer à la souveraineté numérique.

Analyser les enjeux de souveraineté numérique et les menaces informationnelles (LMI, ingérence, espionnage industriel à vecteur cyber) en inscrivant la veille sur les cybermenaces dans une démarche d'intelligence économique, pour contribuer à la protection du patrimoine informationnel et des intérêts stratégiques de l'organisation et de la Nation, et sensibiliser les collaborateurs et dirigeants à la culture du renseignement.

## Blocs de compétences

### RNCP42515BC01 — Collecter et exploiter le renseignement d'origine numérique

#### LISTE DE COMPÉTENCES

Planifier et conduire des opérations de collecte de renseignement d'origine numérique (OSINT, GEOINT, SOCMINT, Dark Web, ...) en définissant les objectifs, les sources pertinentes et les méthodologies adaptées, en veillant à l'accessibilité des méthodologies et livrables selon les principes de la conception universelle (profils types de destinataires, structuration multi-niveaux, lisibilité, accessibilité numérique des supports) pour des professionnels aux profils diversifiés, y compris en situation de handicap, afin d'alimenter l'analyse de la menace en données fiables et exploitables.

Exploiter les outils et techniques de traçage numérique pour identifier et corréler les empreintes digitales (adresses IP, domaines, identifiants, métadonnées) d'acteurs malveillants, en respectant le cadre légal et normatif applicable (RGPD, Code pénal, IGI 1300, II 901, ...) et les exigences de protection du secret, afin de cartographier les menaces pesant sur les systèmes d'information.

Détecter et analyser les signaux faibles issus des sources ouvertes, du Dark Web et des réseaux sociaux, en identifiant les indicateurs précurseurs d'activités malveillantes, en intégrant la prévention des risques professionnels liés à l'exposition prolongée aux contenus sensibles et au travail sur écran, afin d'anticiper les menaces avant qu'elles ne frappent les systèmes d'information.

Automatiser les processus de collecte de données en développant ou paramétrant des scripts et outils de surveillance en arbitrant les choix d'automatisation entre performance, efficacité opérationnelle et sobriété des ressources mobilisées (fréquence des requêtes, volume de stockage, empreinte computationnelle), pour assurer une veille continue et optimiser l'efficacité des opérations de renseignement sur les systèmes d'information.

Structurer, indexer et qualifier les données collectées en les organisant selon des taxonomies et formats standardisés (STIX/TAXII, JSON structuré), en optimisant les ressources computationnelles dans une démarche de sobriété numérique et de transition écologique, afin de garantir leur exploitabilité, leur traçabilité et leur interopérabilité avec les plateformes d'analyse.

Exploiter les outils d'intelligence artificielle et d'apprentissage automatique pour optimiser le traitement de données massives (textuelles, visuelles, comportementales) collectées lors des opérations de renseignement, en évaluant de manière critique la fiabilité et les biais des résultats produits, dans le cadre de la transition numérique des opérations de renseignement.

#### MODALITÉS D'ÉVALUATION

Mise en situation professionnelle : à partir d'un scénario de menace, le candidat conduit une opération de collecte OSINT, structure les données recueillies et présente ses résultats devant un jury. Production de livrables (plan de

collecte, cartographie, script d'automatisation) et soutenance orale.

## **RNCP42515BC02 — Analyser et qualifier les cybermenaces**

### **LISTE DE COMPÉTENCES**

Analyser les indicateurs de compromission (IoCs) et les artefacts techniques d'une attaque, incluant l'analyse de malware de premier niveau (statique, comportementale), en utilisant les référentiels standards (MITRE ATT&CK, STIX/TAXII), et en structurant les productions analytiques selon les principes de la conception universelle (hiérarchisation, alternatives aux représentations graphiques telles que matrices ATT&CK ou graphes d'attribution, compatibilité avec les outils d'assistance), pour qualifier précisément le mode opératoire technique de l'adversaire et évaluer les risques pesant sur les systèmes d'information.

Cartographier les infrastructures d'attaque (serveurs C2, domaines malveillants, chaînes d'approvisionnement) en corrélant les données techniques collectées, pour identifier l'étendue de la menace et sécuriser les organisations ciblées.

Détecter et caractériser les menaces issues de l'intelligence artificielle (deepfakes audio/vidéo, contenus synthétiques, phishing automatisé par IA, empoisonnement de modèles, attaques adversariales), en intégrant la prévention des risques professionnels liés à l'exposition aux contenus perturbants, pour qualifier les nouveaux modes opératoires adverses.

Intégrer le renseignement d'origine électromagnétique (ROEM/SIGINT) dans l'analyse des cybermenaces, en corrélant les produits de renseignement technique avec les données collectées en sources ouvertes et les indicateurs de compromission, afin de produire une caractérisation enrichie de la menace.

Établir des profils d'acteurs malveillants (APT, cybercriminels, hacktivistes) en analysant leurs motivations, schémas comportementaux, capacités et historiques d'activité, pour anticiper les menaces avant qu'elles ne frappent les systèmes d'information et orienter les mesures de protection.

Contextualiser les indicateurs techniques dans leur environnement géopolitique, économique, sociétal et normatif, en croisant les données d'analyse technique avec les facteurs de contexte (conflits hybrides, guerre économique, menaces sur les infrastructures de la transition énergétique et écologique), pour produire une qualification multidimensionnelle de la menace et évaluer l'exposition des systèmes d'information au regard des exigences de conformité.

Détecter et analyser les campagnes de manipulation de l'information (désinformation, propagande computationnelle, ingérence numérique étrangère) en identifiant les réseaux d'amplification et les narratifs artificiels, y compris lorsqu'elles ciblent des publics spécifiquement vulnérables ou en situation de handicap, en s'inscrivant dans les enjeux de transition numérique responsable, pour contribuer à la souveraineté informationnelle et à la protection des processus démocratiques.

### **MODALITÉS D'ÉVALUATION**

Étude de cas technique : à partir d'un jeu de données d'incident réel ou réaliste (logs, captures réseau, échantillons), le candidat produit une analyse CTI complète incluant le profilage des acteurs et la contextualisation de la menace. Production de livrables (rapport d'analyse avec mapping MITRE ATT&CK, fiches de profil, IoCs) et soutenance avec démonstration technique.

## **RNCP42515BC03 — Conduire des investigations numériques en soutien des enquêtes**

### **LISTE DE COMPÉTENCES**

Conduire une investigation forensique sur les systèmes d'information en respectant les protocoles de préservation des preuves (chaîne de custody, intégrité des données), en veillant à l'accessibilité des protocoles et restitutions selon les principes de la conception universelle (lisibilité juridique, structure des procès-verbaux, accessibilité pour la diversité des destinataires institutionnels — forces de l'ordre, magistrats, équipe d'investigation) pour les membres de l'équipe en situation de handicap, pour garantir la recevabilité des preuves dans un cadre juridique.

Analyser les artefacts forensiques (systèmes de fichiers, registres, logs, mémoire vive) pour reconstituer la chronologie d'un incident, identifier les vecteurs de compromission et les mécanismes de latéralisation au sein des systèmes d'information, en intégrant la prévention des risques psychosociaux liés à l'examen prolongé d'artefacts sensibles et à la pression temporelle de l'investigation (procédure de relève, limitation de la durée d'exposition, débriefing).

Garantir l'intégrité des éléments de preuve au sein de la chaîne d'enquête judiciaire en documentant les investigations selon les standards requis pour la transmission aux autorités compétentes, en garantissant la protection du secret et la conformité des procédures aux exigences réglementaires, pour faciliter les suites judiciaires éventuelles et contribuer à la sécurisation des systèmes d'information.

Conduire des investigations forensiques sur systèmes intelligents et embarqués (terminaux mobiles, objets connectés, véhicules, drones) en adaptant les méthodologies d'acquisition et d'analyse aux contraintes spécifiques de ces environnements (volatilité, hétérogénéité des formats), en évaluant l'empreinte environnementale des opérations dans une démarche de transition écologique, pour extraire et exploiter les preuves numériques.

Investiguer les flux financiers numériques (cryptomonnaies, blockchain, systèmes de paiement) en mobilisant les outils de traçage et d'analyse transactionnelle, en collaboration avec les cellules de conformité (LCB-FT) et les autorités judiciaires, en s'inscrivant dans la transition numérique des processus d'investigation financière, pour identifier les circuits de blanchiment, de financement illicite ou de fraude.

Détecter et investiguer les fraudes d'origine numérique (fraude documentaire, usurpation d'identité, contenus falsifiés par IA générative, fraude e-commerce ou assimilé) en mobilisant les techniques d'authentification et d'analyse de contenus synthétiques, y compris à l'encontre de victimes spécifiquement en situation de handicap, pour qualifier le mode opératoire et soutenir les démarches d'enquête.

#### MODALITÉS D'ÉVALUATION

Mise en situation d'une investigation forensique en contexte d'enquête judiciaire : le candidat reçoit une image forensique d'un système compromis et mène l'investigation complète, incluant la détection de fraude et le traçage de flux financiers. Production de livrables exploitables juridiquement et soutenance de restitution.

### **RNCP42515BC04 — Produire et diffuser le renseignement stratégique**

#### LISTE DE COMPÉTENCES

Produire des rapports de renseignement à différents niveaux (stratégique, tactique, opérationnel) en adaptant le contenu, le format et le vocabulaire aux destinataires, en respectant les principes de la conception universelle (strates de lecture explicitées — executive summary, synthèse tactique, annexes techniques ; langue claire ; structuration multi-niveaux ; accessibilité numérique conforme RGAA / WCAG) pour les personnes en situation de handicap, pour répondre aux besoins décisionnels de l'organisation et orienter la posture de sécurité.

Élaborer des scénarios prospectifs d'évolution de la menace en croisant les données techniques, géopolitiques, économiques et réglementaires (NIS2, DORA, CRA, AI Act), en intégrant les enjeux de transition écologique et les menaces pesant sur les infrastructures de la transition énergétique (réseaux intelligents, smart grids, mobilité durable), pour anticiper les risques futurs pesant sur les systèmes d'information et adapter la posture de conformité de l'organisation.

Formuler des recommandations actionnables et priorisées à destination des équipes opérationnelles et des décideurs, en intégrant la prévention des risques liés à la mise en œuvre des mesures correctives sur les systèmes d'information ainsi que la prévention des risques psychosociaux liés à la charge et à la tension des équipes de mise en œuvre (relève, dimensionnement, débriefing) et l'arbitrage performance / efficacité / sobriété des mesures recommandées (empreinte des dispositifs de surveillance et de protection, consommation énergétique), pour renforcer la résilience globale de l'organisation.

Présenter et défendre les analyses devant les instances dirigeantes (COMEX, état-major) en vulgarisant les aspects techniques, en s'inscrivant dans les enjeux de transformation numérique de l'organisation, pour éclairer la prise de décision stratégique et contribuer à la souveraineté des acteurs.

Conseiller les dirigeants sur l'anticipation des cybermenaces et diffuser la culture du renseignement, en s'appuyant sur des exercices de crise et des productions d'analyse stratégique, incluant la promotion de pratiques de renseignement inclusives au sein des équipes (accessibilité des outils d'analyse et de veille pour les collaborateurs en situation de handicap, aménagement des dispositifs d'astreinte et de coopération, sensibilisation aux situations de handicap), pour élever la maturité décisionnelle de l'organisation.

#### MODALITÉS D'ÉVALUATION

Production de livrables CTI et restitution : à partir d'un contexte organisationnel fictif et d'une menace identifiée, le candidat produit des livrables de renseignement à différents niveaux (rapport stratégique, note tactique, bulletin d'alerte, scénario prospectif) et les soutient devant un jury simulant un comité exécutif en situation d'urgence.

### **RNCP42515BC05 — Piloter la veille et la coopération en matière de cybermenaces**

#### LISTE DE COMPÉTENCES

Organiser et piloter une veille structurée multi-dimensionnelle (technologique, géopolitique, réglementaire, sectorielle) incluant la détection de signaux faibles, en veillant à l'accessibilité des outils et livrables de veille selon les principes de la conception universelle (structure des bulletins, langue claire, accessibilité multi-supports, compatibilité avec les outils d'assistance) pour les professionnels en situation de handicap, pour anticiper les évolutions de la menace et

adapter la posture de sécurité des systèmes d'information.

Assurer une veille spécifique sur les menaces émergentes liées à l'intelligence artificielle, aux systèmes autonomes et aux technologies de rupture (quantique, IoT massif, edge computing), en s'inscrivant dans une démarche de transition numérique responsable et de sobriété, pour identifier les nouvelles surfaces d'attaque sur les systèmes d'information.

Évaluer les impacts des évolutions réglementaires et normatives (NIS2, DORA, CRA, AI Act, ...) et des transformations sociétales et environnementales sur le paysage des cybermenaces, en intégrant les enjeux de transition écologique et numérique responsable, pour adapter les priorités de veille, la posture de conformité et les recommandations stratégiques de l'organisation.

Coordonner les échanges avec l'écosystème cyber (CERT, CSIRT, ANSSI, forces de l'ordre, ISAC) en respectant les protocoles de partage d'information (TLP), en intégrant la prévention des risques liés à la gestion de situations d'urgence et d'astreinte, pour enrichir la connaissance de la menace et sécuriser les chaînes de valeur.

Garantir le respect du cadre juridique, normatif et éthique (RGPD, Code pénal, IGI 1300, II 901, secret professionnel, protection du secret de la défense nationale, etc.) dans la conduite des opérations de renseignement et d'investigation, et venir en soutien technique aux enquêtes en collaboration avec les autorités compétentes, pour contribuer à la souveraineté numérique.

Analyser les enjeux de souveraineté numérique et les menaces informationnelles (LMI, ingérence, espionnage industriel à vecteur cyber) en inscrivant la veille sur les cybermenaces dans une démarche d'intelligence économique, pour contribuer à la protection du patrimoine informationnel et des intérêts stratégiques de l'organisation et de la Nation, et sensibiliser les collaborateurs et dirigeants à la culture du renseignement.

#### MODALITÉS D'ÉVALUATION

Projet professionnel avec soutenance : le candidat présente un projet réalisé en contexte professionnel démontrant sa capacité à piloter une activité de veille et de coopération en matière de cybermenaces.

## Secteur d'activité et type d'emploi

#### SECTEURS D'ACTIVITÉS

L'expert en renseignement et investigation sur les cybermenaces exerce au sein d'organisations confrontées à des menaces cyber complexes nécessitant une capacité d'anticipation, d'analyse et d'investigation. Il intervient notamment dans les entreprises spécialisées en renseignement cyber et threat intelligence, au sein des équipes CERT/CSIRT, des cellules CTI ou des directions sûreté d'organisations de toute taille, ainsi que dans les services régaliens et administrations en charge de la cybersécurité, du renseignement ou de l'investigation numérique.

Les secteurs d'activités concernés sont variés : défense et industries de la base industrielle et technologique de défense (BITD), banque, assurance et services financiers, énergie et opérateurs d'importance vitale (OIV), télécommunications, administrations publiques et services de l'État (ANSSI, services de renseignement, police judiciaire, gendarmerie), ainsi que tout secteur soumis aux exigences réglementaires renforcées (NIS2, DORA). L'expert peut exercer en tant que salarié, consultant ou prestataire, au sein de structures allant de la PME spécialisée aux grands groupes internationaux et aux administrations sensibles.

#### TYPE D'EMPLOIS ACCESSIBLES

En renseignement sur les cybermenaces (CTI) : Analyste CTI (Cyber Threat Intelligence Analyst) - Analyste de la menace cyber - Threat Hunter - Analyste SOC spécialisé CTI - Analyste CERT spécialisé CTI

En investigation numérique et forensique : Investigateur forensique / Digital Forensics (DFIR) Investigator - Analyste forensique (Forensic Analyst) - Enquêteur en criminalistique numérique - Analyste en traces numériques

En renseignement en sources ouvertes et traçage : Analyste OSINT (Open Source Intelligence Analyst) - Investigateur numérique / Cyber Investigator - Analyste en cybercriminalité

En lutte contre la fraude et investigations financières : Expert en lutte contre la fraude numérique - Analyste technique LCB-FT crypto-actifs - Investigateur blockchain

En lutte contre les manipulations de l'information : Analyste en ingérence numérique - Analyste en lutte contre les manipulations de l'information (LMI)

#### RÉGLEMENTATIONS D'ACTIVITÉ

L'expert en renseignement et investigation sur les cybermenaces ne relève pas d'une activité réglementée. En revanche, le domaine se situe au carrefour de plusieurs corpus juridiques et normatifs, dont :

Réglementations européennes :

Règlement Général sur la Protection des Données (RGPD) - Directive NIS 2 - Cyber Resilience Act (CRA) - Digital Operational Resilience Act (DORA) - Artificial Intelligence Act (AI Act) - Règlement e-Evidence - Règlement MiCA (Markets in Crypto-Assets) - Directives européennes anti-blanchiment (AMLD) et cadre LCB-FT

Cadre juridique national : Code pénal, articles 323-1 et suivants (atteintes aux STAD) - Code de procédure pénale - Loi n° 2015-912 du 24 juillet 2015 relative au renseignement (Code de la sécurité intérieure, Livre VIII) - Loi n° 2018-1202 du 22 décembre 2018 relative à la lutte contre la manipulation de l'information - Loi de Programmation Militaire (LPM) - Instructions Interministérielles (IGI 1300, II 901)

Cadre juridique international : Convention de Budapest sur la cybercriminalité

Normes internationales et sectorielles : ISO/CEI 27001 (management de la sécurité de l'information) - ISO/CEI 27037, 27041, 27042, 27043 (investigation numérique et traitement de la preuve) - IEC 62443 (sécurité des systèmes industriels) - PCI DSS (Payment Card Industry Data Security Standard)

Référentiels d'exigences de l'ANSSI : PRIS (Prestataire de Réponse aux Incidents de Sécurité) - PDIS (Prestataire de Détection des Incidents de Sécurité) - PASSI (Prestataire d'Audit de la Sécurité des Systèmes d'Information) - PACS (Prestataire d'Audit de la Cybersécurité)

## Marché du travail

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

|                                     |                                                                                                                                                                                                                                                                                                           |
|-------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Tension de recrutement (DARES 2024) | Très élevée (5/5)<br>Moyenne pondérée par l'emploi ; les familles ci-dessous s'échelonnent de 4 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 (41 % des actifs en emploi)                                                                                                                                                                              |
| Familles professionnelles (FAP)     | M1X80 — Techniciens d'étude et de développement 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>M2X93 — Experts et consultants en systèmes d'information · tension 5/5 (Très élevée) |
| Projets de recrutement (BMO 2026)   | 32 216                                                                                                                                                                                                                                                                                                    |
| Jugés difficiles à recruter         | 51 %                                                                                                                                                                                                                                                                                                      |
| Emplois saisonniers                 | 1 %                                                                                                                                                                                                                                                                                                       |
| Familles professionnelles (FAP)     | M1X80 — Techniciens d'étude et de développement en informatique<br>M2X90 — Ingénieurs et cadres d'étude, recherche et développement en informatique et télécom<br>M2X93 — Experts et consultants en systèmes d'information                                                                                |

## Voies d'accès

MODALITÉS D'ACCÈS  
Formation initiale, Formation continue, Apprentissage, Contrat de professionnalisation, VAE

PRÉREQUIS À L'ENTRÉE EN FORMATION  
Être titulaire d'un titre ou diplôme de niveau 6 minimum (en cybersécurité, informatique, droit, sciences politiques, économie, ou sur un domaine connexe au renseignement et à l'investigation) ou équivalent (diplôme étranger...) ou d'une expérience professionnelle équivalente. Cette équivalence sera appréciée par une commission d'admission sur la base d'une étude complète du profil du candidat.

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

Le jury est composé de 4 membres minimum dont 2 membres externes, professionnels du renseignement sur les cybermenaces (ex : analyste CTI, expert OSINT) et de l'investigation numérique (ex : analyste forensic, investigateur en cybercriminalité)

## Base légale

|                                      |            |
|--------------------------------------|------------|
| Date de décision                     | 26/06/2026 |
| Durée de l'enregistrement            | 3 ans      |
| Date d'échéance de l'enregistrement  | 26/06/2029 |
| Date de dernière délivrance possible | 26/06/2033 |

## Liens avec d'autres certifications

CORRESPONDANCES (PAR BLOCS)  
RNCP37095, RNCP40640

## Pour plus d'informations

### Fiche officielle (France Compétences)

<https://www.francecompetences.fr/recherche/rncp/42515/>