

Spécialiste en renseignement et investigation sur les cybermenaces

RNCP42863 · RNCP · Publiée

L'essentiel

Niveau de qualification	Niveau 6
Code(s) NSF	310, 320, 326
Formacode(s)	31045
Code(s) ROME	M1802, M1801, M1806, M1810
Type d'enregistrement	Enregistrement sur demande
Date d'enregistrement	30/09/2026
Date d'échéance	30/09/2029

Certificateur(s)

ECOLE SUP LIBRE SCIENC COM APPLIQUEES · SIRET : 78430830600074

Résumé de la certification

OBJECTIFS ET CONTEXTE

La certification professionnelle de « Spécialiste en renseignement et investigation sur les cybermenaces » s'inscrit dans un contexte de montée en puissance, de diffusion et de complexification des cybermenaces, qui touchent désormais l'ensemble des organisations publiques et privées. L'évolution des modes opératoires, la sophistication des attaquants et la porosité croissante entre cybercriminalité, enjeux géopolitiques et économiques renforcent le besoin de compétences spécialisées en analyse et en production de renseignement cyber.

L'objectif de cette certification professionnelle est de former des professionnels capables de collecter, structurer et analyser des données issues d'environnements numériques complexes, afin de produire un renseignement exploitable pour la détection, la compréhension et l'anticipation des cybermenaces. Elle vise ainsi à structurer un métier émergent à l'interface de la cybersécurité, de l'investigation numérique et de l'intelligence stratégique, en réponse aux besoins croissants du marché et aux exigences accrues des organisations en matière de sécurité et de maîtrise des risques.

ACTIVITÉS VISÉES

Analyse de l'écosystème des cybermenaces : Identification des typologies de menaces, des modes opératoires et des structures d'acteurs ; Analyse des dimensions géopolitiques, économiques, sociétales et technologiques influençant les cybermenaces ; Caractérisation des logiques d'action et des capacités des acteurs malveillants

Cartographie des risques numériques : Cartographie des menaces, des vulnérabilités et des actifs exposés ; Représentation des interactions entre acteurs, systèmes et vecteurs d'attaque ; Hiérarchisation des risques en fonction des impacts et des probabilités ; Formalisation des enjeux stratégiques prioritaires pour le donneur d'ordre

Collecte d'informations multi-sources : Définition d'une stratégie de recherche adaptée à une problématique d'investigation ; Collecte d'informations en sources ouvertes, réseaux sociaux et sources humaines ; Exploration d'environnements numériques complexes incluant web de surface, deep web et dark web ; Qualification de la fiabilité et de la pertinence des informations collectées

Structuration et qualification des données d'investigation : Organisation et centralisation des données collectées ; Nettoyage et normalisation des données ; Qualification des données : source, fiabilité, typologie ; Traçabilité des données et des transformations

Traitement du renseignement cyber : Croisement et corrélation des données issues de sources multiples ; Reconstitution de scénarios d'attaque et des chaînes d'événements ; Identification des modes opératoires et des

objectifs des attaquants ; Production d'analyses exploitables pour la compréhension des menaces
Investigation des incidents et activités malveillantes : Détection de signaux faibles et d'activités suspectes ; Analyse des comportements frauduleux et malveillants ; Exploitation des traces techniques et des preuves numériques ; Participation aux dispositifs de gestion d'incidents de cybersécurité
Production de livrables de renseignement : Structuration des analyses issues du traitement de l'information ; Formalisation des conclusions et des hypothèses ; Rédaction de notes de renseignement et de rapports d'analyse ; Synthèse des informations à destination des décideurs
Visualisation et diffusion du renseignement : Représentation visuelle des données et des analyses ; Adaptation des messages aux publics cibles ; Choix des supports et des formats de diffusion ; Diffusion sécurisée des informations sensibles

COMPÉTENCES ATTESTÉES

Identifier les acteurs, typologies de menaces et modes opératoires d'un environnement numérique donné, en mobilisant des grilles d'analyse structurées, des sources spécialisées et des bases de renseignement, afin de caractériser les dynamiques de menace dans un contexte organisationnel ou sectoriel.

Analyser les dynamiques géopolitiques, économiques et informationnelles influençant les cybermenaces, en exploitant des sources ouvertes, des données territoriales et des indicateurs stratégiques, afin d'anticiper les évolutions des risques et leurs impacts sur les organisations.

Cartographier les menaces, vulnérabilités, acteurs et impacts d'un système d'information ou d'un environnement cible, en utilisant des outils de modélisation et de visualisation de données, en optimisant le volume de données manipulées afin de limiter l'empreinte numérique, afin de prioriser les risques.

Structurer une analyse des menaces en intégrant typologie, capacités, intentions, cibles et impacts, en consolidant les données issues de la collecte selon une grille d'analyse formalisée, afin d'établir une base d'évaluation exploitable pour la prise de décision.

Mettre en œuvre des techniques de collecte OSINT, SOCMINT et GEOINT, en utilisant des outils spécialisés, des requêtes avancées et des protocoles d'investigation, en respectant les règles de sécurité des systèmes d'information et les bonnes pratiques de protection des données, afin de recueillir des informations fiables.

Investiguer des environnements numériques incluant web de surface, deep web et dark web, en mobilisant des outils d'investigation et des techniques d'exploration sécurisées, afin d'identifier des informations sensibles tout en limitant les risques d'exposition.

Automatiser la collecte de données issues de sources numériques, en développant des scripts de scrapping et en utilisant des traitements algorithmiques notamment en Python, en optimisant les traitements pour limiter la consommation de ressources, afin d'améliorer l'efficacité de la collecte.

Structurer des données hétérogènes issues de la collecte, en les nettoyant et en les qualifiant à l'aide d'outils de gestion de la donnée et de méthodes de normalisation, en garantissant la traçabilité et la sécurisation des traitements, afin d'assurer leur exploitabilité.

Utiliser des outils d'intelligence artificielle, en formulant des requêtes adaptées et en paramétrant des dispositifs automatisés, en vérifiant la fiabilité des résultats produits, afin d'améliorer la pertinence de la collecte et de la veille.

Exploiter des données issues de la collecte en les croisant et en les corrélant, en mobilisant des méthodes de data analyse et de cyber threat intelligence (CTI), en évaluant le niveau de fiabilité des données et les incertitudes associées, afin de produire des informations exploitables pour l'analyse des menaces.

Reconstituer la chronologie d'un incident de cybersécurité, en analysant des traces numériques et des journaux techniques, afin de comprendre les enchaînements d'actions et les impacts.

Détecter des activités malveillantes et frauduleuses, en identifiant des signaux faibles et en exploitant des indicateurs techniques et comportementaux, afin de qualifier un niveau de menace.

Exploiter des traces et preuves numériques, en appliquant des méthodes d'investigation et de conservation des données, en respectant les procédures de sécurité et les règles de manipulation des environnements de travail, afin de documenter les faits.

Contribuer à la gestion d'incidents, en participant aux analyses techniques et en utilisant des outils de coordination, en appliquant les consignes de sécurité et de prévention des risques professionnels, afin de limiter les impacts.

Produire des analyses de renseignement à partir de données collectées et traitées, en hiérarchisant les informations, en formulant des scénarios d'évolution et en proposant des options de décision argumentées, afin d'éclairer la prise de décision stratégique.

Rédiger des notes de renseignement et des rapports d'analyse, en structurant les contenus et en hiérarchisant les informations, en adaptant le niveau de complexité et les formats pour garantir l'accessibilité des livrables, afin de

formaliser les résultats.

Représenter des données et analyses sous forme de cartographies et d'infographies, en utilisant des outils de visualisation et en appliquant des principes de lisibilité et d'accessibilité, afin de faciliter la compréhension.

Adapter les messages et supports de diffusion, en tenant compte du niveau technique, des besoins spécifiques des utilisateurs et des situations de handicap, afin d'assurer une transmission efficace et inclusive.

Diffuser des informations sensibles, en utilisant des outils de partage sécurisés et en appliquant des règles de confidentialité et de gestion des accès, afin de garantir la protection des données.

Blocs de compétences

RNCP42863BC01 — Analyser les environnements informationnels et l'écosystème des cybermenaces pesant sur une organisation ou un secteur

LISTE DE COMPÉTENCES

Identifier les acteurs, typologies de menaces et modes opératoires d'un environnement numérique donné, en mobilisant des grilles d'analyse structurées, des sources spécialisées et des bases de renseignement, afin de caractériser les dynamiques de menace dans un contexte organisationnel ou sectoriel.

Analyser les dynamiques géopolitiques, économiques et informationnelles influençant les cybermenaces, en exploitant des sources ouvertes, des données territoriales et des indicateurs stratégiques, afin d'anticiper les évolutions des risques et leurs impacts sur les organisations.

Cartographier les menaces, vulnérabilités, acteurs et impacts d'un système d'information ou d'un environnement cible, en utilisant des outils de modélisation et de visualisation de données, en optimisant le volume de données manipulées afin de limiter l'empreinte numérique, afin de prioriser les risques.

Structurer une analyse des menaces en intégrant typologie, capacités, intentions, cibles et impacts, en consolidant les données issues de la collecte selon une grille d'analyse formalisée, afin d'établir une base d'évaluation exploitable pour la prise de décision.

MODALITÉS D'ÉVALUATION

Mise en situation professionnelle reconstituée

RNCP42863BC02 — Collecter, structurer et qualifier des données issues d'investigations numériques dans un contexte de cybermenaces

LISTE DE COMPÉTENCES

Mettre en œuvre des techniques de collecte OSINT, SOCMINT et GEOINT, en utilisant des outils spécialisés, des requêtes avancées et des protocoles d'investigation, en respectant les règles de sécurité des systèmes d'information et les bonnes pratiques de protection des données, afin de recueillir des informations fiables.

Investiguer des environnements numériques incluant web de surface, deep web et dark web, en mobilisant des outils d'investigation et des techniques d'exploration sécurisées, afin d'identifier des informations sensibles tout en limitant les risques d'exposition.

Automatiser la collecte de données issues de sources numériques, en développant des scripts de scrapping et en utilisant des traitements algorithmiques notamment en Python, en optimisant les traitements pour limiter la consommation de ressources, afin d'améliorer l'efficacité de la collecte.

Structurer des données hétérogènes issues de la collecte, en les nettoyant et en les qualifiant à l'aide d'outils de gestion de la donnée et de méthodes de normalisation, en garantissant la traçabilité et la sécurisation des traitements, afin d'assurer leur exploitabilité.

Utiliser des outils d'intelligence artificielle, en formulant des requêtes adaptées et en paramétrant des dispositifs automatisés, en vérifiant la fiabilité des résultats produits, afin d'améliorer la pertinence de la collecte et de la veille.

MODALITÉS D'ÉVALUATION

Mise en situation professionnelle reconstituée

RNCP42863BC03 — Analyser le renseignement, investiguer et gérer les incidents de sécurité dans une logique de mesure d'impact des menaces

LISTE DE COMPÉTENCES

Exploiter des données issues de la collecte en les croisant et en les corrélant, en mobilisant des méthodes de data analyse et de cyber threat intelligence (CTI), en évaluant le niveau de fiabilité des données et les incertitudes associées, afin de produire des informations exploitables pour l'analyse des menaces.

Reconstituer la chronologie d'un incident de cybersécurité, en analysant des traces numériques et des journaux techniques, afin de comprendre les enchaînements d'actions et les impacts.

Détecter des activités malveillantes et frauduleuses, en identifiant des signaux faibles et en exploitant des indicateurs techniques et comportementaux, afin de qualifier un niveau de menace.

Exploiter des traces et preuves numériques, en appliquant des méthodes d'investigation et de conservation des données, en respectant les procédures de sécurité et les règles de manipulation des environnements de travail, afin de documenter les faits.

Contribuer à la gestion d'incidents, en participant aux analyses techniques et en utilisant des outils de coordination, en appliquant les consignes de sécurité et de prévention des risques professionnels, afin de limiter les impacts.

MODALITÉS D'ÉVALUATION

Mise en situation professionnelle reconstituée

RNCP42863BC04 — Produire et diffuser du renseignement à des fins de prise de décision

LISTE DE COMPÉTENCES

Produire des analyses de renseignement à partir de données collectées et traitées, en hiérarchisant les informations, en formulant des scénarios d'évolution et en proposant des options de décision argumentées, afin d'éclairer la prise de décision stratégique.

Rédiger des notes de renseignement et des rapports d'analyse, en structurant les contenus et en hiérarchisant les informations, en adaptant le niveau de complexité et les formats pour garantir l'accessibilité des livrables, afin de formaliser les résultats.

Représenter des données et analyses sous forme de cartographies et d'infographies, en utilisant des outils de visualisation et en appliquant des principes de lisibilité et d'accessibilité, afin de faciliter la compréhension.

Adapter les messages et supports de diffusion, en tenant compte du niveau technique, des besoins spécifiques des utilisateurs et des situations de handicap, afin d'assurer une transmission efficace et inclusive.

Diffuser des informations sensibles, en utilisant des outils de partage sécurisés et en appliquant des règles de confidentialité et de gestion des accès, afin de garantir la protection des données.

MODALITÉS D'ÉVALUATION

Mise en situation professionnelle reconstituée

Secteur d'activité et type d'emploi

SECTEURS D'ACTIVITÉS

Les principaux secteurs d'activité concernés sont notamment :

les entreprises de services numériques (ESN) et les sociétés spécialisées en cybersécurité ;

les cabinets de conseil en gestion des risques, en intelligence économique et en sécurité de l'information ;

les grandes entreprises et entreprises de taille intermédiaire (ETI), notamment dans les secteurs de la banque, de l'assurance, de l'industrie, des télécommunications et de la santé ;

les organismes publics et parapublics (administrations, opérateurs d'importance vitale, institutions de défense et de sécurité) ;

les structures spécialisées dans l'analyse stratégique, la gestion de crise et la sûreté.

TYPE D'EMPLOIS ACCESSIBLES

Le titulaire de la certification peut exercer dans différents métiers liés à l'analyse des menaces, à la cybersécurité, au renseignement et à l'intelligence économique, notamment dans des fonctions d'analyse, de veille, d'investigation et de gestion des risques informationnels.

Les principaux métiers accessibles sont : auditeur en cybermenaces, chargé d'études en cybersécurité, chargé d'études en communication et gestion de crise, junior compliance officer, analyste OSINT, analyste CSIRT, analyste en threat intelligence, chargé de missions sûreté et analyste SOC.

RÈGLEMENTATIONS D'ACTIVITÉ

Le métier ne constitue pas, à ce jour, une profession réglementée au sens strict. Toutefois, son exercice s'inscrit dans un cadre juridique et réglementaire particulièrement structurant, qui encadre les modalités de collecte, de traitement, d'analyse et de diffusion des informations, notamment lorsqu'elles sont sensibles ou à caractère personnel. L'activité est directement impactée par plusieurs corpus réglementaires majeurs[1]. Ces cadres réglementaires influencent directement les pratiques professionnelles de ce spécialiste[2]. Ces contraintes renforcent la nécessité pour ces

professionnels de maîtriser non seulement des compétences techniques et analytiques, mais également des règles juridiques et déontologiques applicables à leur activité. Les référentiels de cette certification professionnelle intègrent pleinement ces exigences réglementaires, en exprimant clairement les contraintes à respecter dans les moyens associés aux actions exprimés dans les compétences, et en mesurant leur respect par des critères d'évaluation explicites.

[1] Protection des données personnelles : règlement (UE) 2016/679 (RGPD) et loi Informatique et Libertés ; Cadre pénal et droit du numérique (STAD) ; Secret des affaires et confidentialité : loi n°2018-670 ; Cadre européen de la cybersécurité (directive NIS2) ; Cadres spécifiques liés aux environnements sensibles : dans certains contextes (défense, sécurité nationale, opérateurs d'importance vitale), des règles complémentaires s'appliquent (classification des informations, habilitations, procédures de sécurité), renforçant les exigences en matière de confidentialité et de traçabilité.

[2] La collecte d'informations est limitée aux données accessibles légalement ou autorisées dans un cadre contractuel ou organisationnel ; les activités d'investigation numérique nécessitent la mise en œuvre de mesures de sécurité (anonymisation, cloisonnement des environnements, traçabilité des actions) ; le traitement des données impose des exigences de qualification, de fiabilité, de sécurisation et de conservation ; la diffusion du renseignement est encadrée par des règles strictes de confidentialité, de gestion des accès et de protection des informations sensibles ; les pratiques professionnelles doivent intégrer une dimension éthique, notamment dans l'utilisation d'outils d'intelligence artificielle et dans l'analyse d'informations issues d'environnements numériques

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	Lien formation-emploi, Manque de main-d'œuvre disponible
Salaire médian (mensuel)	2 704 €
Diplôme le plus fréquent	Diplôme de niveau bac+5 ou plus (doctorat, master ou équivalent) en communication et information (35 % 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) 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)	14 307
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 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

MODALITÉS D'ACCÈS
Formation initiale, VAE

PRÉREQUIS À L'ENTRÉE EN FORMATION

Les prérequis, hors VAE, incluent l'obligation d'être titulaire d'un diplôme ou titre de niveau 4.

La Validation des Acquis Professionnels et Personnels (VAPP) permet d'accéder directement à la formation sans avoir les pré requis, en faisant valider une expérience professionnelle (salariée ou non), les formations suivies et les acquis personnels développés hors de tout système de formation par l'EGE.

COMPOSITION DU JURY — FORMATION INITIALE, VAE

Le jury est composé d'au moins trois membres, experts du domaine des cybermenaces, issus du monde professionnel et/ou académique, dont une majorité est extérieure au certificateur.

Base légale

Date de décision	30/09/2026
Durée de l'enregistrement	3 ans
Date d'échéance de l'enregistrement	30/09/2029
Date de dernière délivrance possible	30/09/2033

Pour plus d'informations

Fiche officielle (France Compétences)

<https://www.francecompetences.fr/recherche/rncp/42863/>