

Expert en Cybersécurité (MS)

RNCP36072 · RNCP · Publiée

L'essentiel

Niveau de qualification	Niveau 7
Code(s) NSF	326
Formacode(s)	31045, 31038, 31025
Code(s) ROME	M1802, M1801, M1806
Type d'enregistrement	Enregistrement sur demande
Date d'enregistrement	15/12/2021
Date d'échéance	15/12/2024

Certificateur(s)

UNIVERSITE DE TECHNOLOGIE DE TROYES (UTT) · SIRET : 19101060200032

Résumé de la certification

OBJECTIFS ET CONTEXTE

L'expert en cybersécurité a pour mission principale la garantie de la protection des données informatiques exposées à des actes malveillants. Il travaille soit dans une société d'ingénierie informatique soit dans une entreprise entant que consultant en sécurité.

Le rôle d'un expert en cybersécurité c'est aussi la pérennisation des systèmes d'information. Il va d'abord aller traquer les points faibles en diagnostiquant la vulnérabilité du système de façon globale. Ensuite, faire des tests d'intrusion pour enfin, proposer des solutions aux problèmes pour améliorer la sécurité et permettre à l'entreprise de faire face aux attaques, tout en préservant sa sécurité.

ACTIVITÉS VISÉES

Diagnostic de l'incident de cybersécurité et de son ampleur

Analyse de l'incident de cybersécurité

Remédiation à l'incident de cybersécurité

Participation à l'élaboration de la PSSI

Supervision des infrastructures et des événements de sécurité

Détection des incidents et les menaces

Analyse et catégorisation des codes malveillants

Remédiation aux menaces

Veille permanente sur les menaces émergentes

Préparation de l'audit de sécurité

Réalisation des tests d'intrusion sur les systèmes, les réseaux, les applications web ou mobiles

Rédaction du rapport de résultat de l'audit de sécurité

Identification des preuves numériques

Définition de la stratégie de préservation des données numériques

Collecte des preuves numériques selon la procédure technico-légale

Traitement et analyse des preuves numériques collectées

Production des preuves numériques analysées

COMPÉTENCES ATTESTÉES

Collecter l'ensemble des informations relatives aux incidents informatiques à l'aide des outils adéquats afin d'avoir une première idée sur l'ampleur de la crise

Trier les éléments liés à l'incident en les catégorisant afin d'organiser des éléments de preuves analysables

Analyser les preuves numériques collectées selon la méthodologie forensique, méthode dont l'objectif est de produire des preuves numériques de l'attaque informatique en vue d'une procédure judiciaire ou d'une action interne à l'aide de la collecte de données brutes ou altérées pour reconstituer le déroulement de l'attaque, afin d'identifier la nature de l'incident

Contextualiser l'incident en faisant la corrélation entre signe d'incident et l'analyse de traces informatique (informations collectées) à l'aide d'outils de modélisation et/ou de visualisation afin d'établir des scénarii potentiels d'incident

Élaborer un plan de remédiation afin d'appliquer les actions nécessaires à la résolution de l'incident telles que décrites dans la politique de sécurité des systèmes d'information (PSSI) en émettant notamment des recommandations aux collaborateurs afin de répondre à la crise cyber

Enrichir la politique de sécurité (PSSI) et des documents associés avec le Responsable de la sécurité des systèmes d'information (RSSI) et/ou Directeur des systèmes d'information (DSI) en utilisant les méthodologies d'analyse de risques telles que Méhari ou EBIOS, ainsi que la norme iso 27001, spécifiant les exigences relatives aux systèmes de management de la sécurité des informations (SMSI) etc. afin d'améliorer la sécurité et la résilience du SI

Améliorer de façon continue ses pratiques en coopérant avec des experts à l'aide des outils de réponse à incident spécifiques

Assurer la supervision des infrastructures et des événements de sécurité en exploitant un système de gestion de l'information et des événements de sécurité (SIEM), en utilisant ces informations pour retracer la chronologie d'une cyberattaque afin de mettre en évidence les signaux faibles, qui d'ordinaire, passent inaperçus et d'éviter que ces mêmes attaques se reproduisent dans le futur

Détecter en temps réel les incidents et les menaces en identifiant leurs sources afin de bloquer leur accès au système informatique

Analyser le code malveillant par les techniques d'analyse statique et/ou dynamique pour le qualifier et le catégoriser

Produire un correctif à l'aide de la distribution Kali Linux (langage python, script bash sous linux, exécutable écrit en C++.) qui sera appliqué par les équipes afin de réponse à incident

Attribuer l'incident en établissant une grille d'analyse d'intrusion en utilisant les méthodes adéquates : Kill Chain, Diamond Model, la matrice MITRE ATT&CK, afin de modéliser une intrusion ciblée

Anticiper les futures évolutions des menaces à l'aide de la mise en place d'un système de veille recensant le renseignement en source ouverte (OSINT), les flux de données commerciaux et communautaires, les média sociaux (SOCMINT), le renseignement d'origine humaine et capacité d'analyse et de corrélation (HUMINT), les informations provenant du Deep et Dark web afin de limiter l'exposition de l'entreprise sur les réseaux sociaux, ou sur les moteurs de recherche, limitant ainsi la surface d'attaque que pourrait exploiter un hacker

Analyser le périmètre d'intervention des tests d'intrusion afin de lancer des tests cadrés

Réaliser des tests d'intrusion sur les systèmes, les réseaux, les applications web ou mobiles en utilisant les outils adéquats selon la méthodologie de tests d'intrusion (définition du plan d'audit, des scénarii, etc.), tout en assurant une veille technique sur les outils d'audit et les pratiques d'attaque et tests d'intrusion en respectant le Code pénal, notamment des articles 323-1 et suivants, spécifique à la cybercriminalité afin d'identifier les services vulnérables et de détecter les éventuelles menaces ou intrusions

Élaborer un rapport détaillé des résultats des tests comprenant des captures d'écran des tests et systématiquement comporter une note explicitant, pour chaque faille ou vulnérabilité découverte, la contre mesure à mettre en place, afin d'éradiquer ou de limiter le risque voire de proposer un plan de remédiation

Identifier le périmètre et l'environnement technique afin d'évaluer la quantité de données à acquérir

Définir la stratégie de préservation des données (en considérant la volumétrie des données à analyser, le temps dont on dispose, le matériel de copie dont on dispose, et d'autres contraintes externes) afin de rédiger le document de traçabilité des actions effectuées

Réaliser la collecte de façon technico-légale à l'aide d'outils de collecte dédiés (suivant les cas, en extrayant les données sur un support de type clé USB, ou bien, de réaliser une copie technico-légale avec des outils open source, tels que dd, dcfldd, présents sur la distribution Kali Linux, ou bien des outils commerciaux comme ftk imager), afin de préserver les preuves numériques

Analyser les artefacts identifiés (disque dur, mémoire, traces réseaux, journaux d'évènements, e-mail, navigateurs, smartphones ...) afin de tracer les preuves numériques

Rédiger un rapport d'analyse en adaptant son discours afin de le présenter à divers publics, techniques et institutionnels (forces de l'ordre, magistrat, équipe de réponse à incident).

Blocs de compétences

RNCP36072BC01 — Traiter les incidents de cybersécurité

LISTE DE COMPÉTENCES

Collecter l'ensemble des informations relatives aux incidents informatiques (journaux d'événements systèmes et réseau, diagrammes de topologie réseau, images systèmes) à l'aide d'outils open-source (autopsy, foremost, scalpel, volatility, plaso, log2timeline, etc.) souvent présents sur la distribution Kali Linux afin d'avoir une première idée sur l'ampleur de la crise.

Trier les éléments liés à l'incident en les catégorisant afin d'organiser des éléments de preuves analysables

Analyser les preuves numériques collectées selon la méthodologie forensique, à l'aide de la collecte de données brutes ou altérées permettant d'identifier la nature de l'incident et de reconstituer le déroulement de l'attaque, afin de lancer une action interne ou une procédure judiciaire

Contextualiser l'incident en faisant la corrélation entre signe d'incident et l'analyse de traces informatiques (informations collectées) à l'aide d'outils de modélisation et/ou de visualisation afin d'établir des scénarii potentiels d'incidents

Élaborer un plan de remédiation afin d'appliquer les actions nécessaires à la résolution de l'incident telles que décrites dans la politique de sécurité des systèmes d'information (PSSI) en émettant notamment des recommandations aux collaborateurs afin de répondre à la crise cyber

Enrichir la politique de sécurité (PSSI) et des documents associés avec le RSSI et/ou DSI en utilisant les méthodologies d'analyse de risques telles que Méhari ou EBIOS, ainsi que la norme ISO 27001, spécifiant les exigences relatives aux systèmes de management de la sécurité des informations (SMSI) etc., afin d'améliorer la sécurité et la résilience du SI

Améliorer de façon continue ses pratiques en coopérant avec des experts à l'aide des outils de réponse à incident spécifiques (CERT, plateforme de partage, virus total)

dans le but de partager les failles, les vulnérabilités, les indices de compromission, et éviter que d'autres structures ne soient affectées par les mêmes menaces

MODALITÉS D'ÉVALUATION

Cas d'étude

RNCP36072BC02 — Analyser la menace cyber pesant sur une organisation

LISTE DE COMPÉTENCES

Assurer la supervision des infrastructures et des événements de sécurité en exploitant un système de gestion de l'information et des événements de sécurité (SIEM) et en utilisant ces informations pour retracer la chronologie d'une cyberattaque, pour mettre en évidence les signaux faibles, qui d'ordinaire, passent inaperçus. Cela permettra de mettre à jour de nouveaux risques identifiés, et d'apporter des modifications sur les équipements pour éviter que ces mêmes attaques ne se reproduisent dans le futur

Détecter en temps réel les incidents et les menaces en identifiant leurs sources afin de bloquer leur accès au système informatique

Analyser le code malveillant par les techniques d'analyse statique et/ou dynamique pour le qualifier et le catégoriser

Produire un correctif à l'aide de la distribution Kali Linux (langage python, script bash sous linux, exécutable écrit en C++) qui sera appliqué par les équipes afin de produire une réponse à incident

Attribuer l'incident en établissant une grille d'analyse d'intrusion en utilisant les méthodes adéquates :

Kill Chain, Diamond Model, la matrice MITRE ATT&CK, afin de modéliser une intrusion ciblée

Anticiper les futures évolutions des menaces à l'aide de la mise en place d'un système de veille recensant le renseignement en source ouverte (OSINT), les flux de données commerciaux et communautaires, les médias sociaux (SOCMINT), le renseignement d'origine humaine et la capacité d'analyse et de corrélation (HUMINT), les informations provenant du Deep et Dark web, afin de limiter l'exposition de l'entreprise sur les réseaux sociaux, ou sur les moteurs de recherche, limitant ainsi la surface d'attaque que pourrait exploiter un hacker

MODALITÉS D'ÉVALUATION

Cas pratique

Test écrit

RNCP36072BC03 — Auditer la sécurité technique d'une organisation

LISTE DE COMPÉTENCES

Analyser le périmètre d'intervention des tests d'intrusion

(après avoir défini le périmètre d'intervention, et la modalité des tests à utiliser, les outils de la distribution Kali Linux seront utilisés, tels que nmap, metasploit et armitage) afin de lancer des tests cadrés

Réaliser des tests d'intrusion sur les systèmes, les réseaux, les applications web ou mobiles en utilisant les outils adéquats selon la méthodologie de tests d'intrusion (définition du plan d'audit, des scénarii, etc.), tout en assurant une veille technique sur les outils d'audit et les pratiques d'attaque et tests d'intrusion en respectant le Code pénal spécifique à la cybercriminalité, les articles 323-1 et suivants notamment, afin d'identifier les services vulnérables et de détecter les éventuelles menaces ou intrusions

Élaborer un rapport détaillé des résultats des tests comprenant des captures d'écran des tests et, systématiquement, une note explicitant, pour chaque faille ou vulnérabilité découverte, la contre-mesure à mettre en place, afin d'éradiquer ou de limiter le risque voire de proposer un plan de remédiation

MODALITÉS D'ÉVALUATION

Cas d'étude

Cas pratique

RNCP36072BC04 — Réaliser une analyse technico-légale (forensique)

LISTE DE COMPÉTENCES

Identifier le périmètre et l'environnement technique, en accédant si nécessaire au système d'exploitation ou au matériel pour avoir une vision précise de la volumétrie des données afin d'évaluer la quantité de données à acquérir

Définir la stratégie de préservation des données (en considérant la volumétrie des données à analyser, le temps dont on dispose, le matériel de copie dont on dispose, et d'autres contraintes externes) afin de rédiger le document de traçabilité des actions effectuées

Réaliser la collecte de façon technico-légale à l'aide d'outils de collecte dédiés soit en extrayant les données sur un support de type clé USB, ou bien, soit en réalisant une copie technico-légale avec des outils open source, tels que dd, dcfldd, présents sur la distribution Kali Linux, ou bien des outils commerciaux comme ftk imager, afin de préserver les preuves numériques

Analyser des artefacts identifiés (disque dur, mémoire, traces réseaux, journaux d'évènements, e-mail, navigateurs, smartphones...) afin de tracer les preuves numériques

Rédiger un rapport d'analyse en adaptant son discours afin de le présenter à divers publics, techniques et institutionnels (forces de l'ordre, magistrat, équipe de réponse à incidents)

MODALITÉS D'ÉVALUATION

Cas d'étude

Secteur d'activité et type d'emploi

SECTEURS D'ACTIVITÉS

Grands groupes industriels

Secteur bancaire

Entreprises publiques

Administrations

PME/TPE

TYPE D'EMPLOIS ACCESSIBLES

Directeur du Système d'Information

Responsable de la Sécurité des Systèmes d'Information

Responsable CERT (Computer Emergency Response Team) ou équipe de réponse à incidents

Toutes les fonctions d'expertise en cabinet de conseil : audit, consultant, intégrateur, formateur...

Ingénieur sécurité, cybersécurité, Ingénieur Sécurité d'information

Consultant en SSI, Sécurité, Sécurité informatique

Information Security Officer

Responsable formation forensic et cybersécurité

Analyste forensic
Directeur adjoint des enquêtes de l'AMF (Autorité des marchés financiers)
Chef de laboratoire de criminalistique numérique
Enquêteur en cybercriminalité
Consultant (analyste CERT)
Consultant CERT
Analyste Sécurité CERT
Analyste SOC (security operation center)
SOC Security Analyst

RÈGLEMENTATIONS D'ACTIVITÉ

Le métier n'est pas règlementé, néanmoins dans l'exercice professionnel de son activité, l'Expert en Cybersécurité doit respecter et tenir compte des droits, obligations et normes en matière de sécurisation du système d'information pour garantir sa mise en conformité. Il doit prendre en compte les obligations réglementaires et normatives en vigueur notamment le règlement général sur la protection des données (RGPD) et veiller à ce que le plan de sécurisation soit adapté au besoin de sécurisation du système.
La prise en compte des décrets suivants reste une nécessité dans l'exercice de l'activité de l'Expert en Cybersécurité : le décret 2015-350, et 2015-351, surtout lors des activités de veille et de management du risque.

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

PRÉREQUIS À L'ENTRÉE EN FORMATION

Sont recevables les candidatures d'étudiants titulaires d'un des diplômes suivants :
Diplôme d'ingénieur habilité par la Commission des Titres d'Ingénieur (liste CTI)
Diplôme d'une école de management habilitée à délivrer le grade de Master (liste CEFDG)

Diplôme de 3e cycle habilité par les autorités universitaires (DEA, DESS, Master...) ou diplôme professionnel cohérent et équivalent avec le niveau bac+5

Diplôme de M1 ou équivalent, pour des auditeurs justifiant d'au moins trois années d'expérience professionnelle en sécurité informatique

Titre inscrit au RNCP niveau 7 (nouvelle nomenclature)

Diplôme étranger équivalent aux diplômes bac+5 français exigés ci-dessus

Conditions d'accès dérogatoires :

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 10 années d'expérience professionnelle (hors stage, césure, cursus initial en alternance).

Par dérogation pour 30 % maximum du nombre d'étudiants suivant la formation Mastère Spécialisé concernée, sont recevables les candidatures d'étudiants titulaires d'un des diplômes suivants : Niveau M1 validé ou équivalent sans expérience professionnelle, Diplôme de L3 justifiant d'une expérience adaptée de 3 ans minimum

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 de délivrance de la certification sera composé 5 membres, dont 3 professionnels externes.

Financement en alternance (NPEC)

Niveau de prise en charge d'un contrat d'apprentissage par les OPCO, fixé par France compétences par branche professionnelle (CPNE).

Prise en charge usuelle	9 000 €
Selon la branche	7 697 € – 9 800 €
Prise en charge	Branches concernées
9 000 €	Valeur par défaut · 182 branches
9 800 €	CNPE des sociétés financières, CPNE Casinos, CPNE Personnel navigant technique des exploitants d'hélicoptères, CPNE Transport aérien : personnel au sol, CPNE Travail Temporaire
8 696 €	CPNE FP Commerce de Détail de l'Horlogerie Bijouterie, CPNEFP Commerce succursaliste de la Chaussure, CPNEFP Commerce à distance, CPNEFP Grands Magasins/ Magasins Populaires, CPNEFP Import-Export
9 276 €	CPNEF de l'Exploitation cinématographique et de la Distribution de films
9 005 €	CPNE FP Branche des magasins du Bricolage
8 974 €	CPNE de la branche de la Distribution Directe
8 813 €	CPNEFP Professions de la Photographie
8 775 €	CPNEFP de la branche des entreprises du bureau et du numérique (commerces et services)
8 711 €	CPNEFP de la Branche des Caisses régionales de Crédit Agricole et autres organismes
8 600 €	CPNEFP de l'habillement, mercerie, chaussure et jouet
8 519 €	CPNE Industrie pétrolière
8 500 €	CPNEFP de la métallurgie
7 697 €	CPNEFP de la blanchisserie, laverie, location de linge, nettoyage à sec, pressing et teinturerie

Base légale

Date de décision	15/12/2021
Durée de l'enregistrement	3 ans
Date d'échéance de l'enregistrement	15/12/2024

Statistiques

Année	Certifiés	Dont VAE	Insertion 6 mois	Métier 2 ans
2019	25	0	100 %	90 %
2018	11	0	100 %	67 %

Liens avec d'autres certifications

NOUVELLE(S) CERTIFICATION(S)
RNCP40640

Pour plus d'informations

LIEN VERS LE DESCRIPTIF
<https://www.utt.fr/formations/mastere-specialise/expert-forensic-cybersecurite>

Fiche officielle (France Compétences)
<https://www.francecompetences.fr/recherche/rncp/36072/>

Entrées et sorties de formation

Entrées en formation	5
Parcours menés à terme	5
Taux d'achèvement	100 %
Période	09/2022 – 09/2025

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

Demande CPF — formations engagées

Dossiers CPF engagés	5
Montant total engagé	50 500 €
Coût moyen par dossier	10 100 €
Durée moyenne	866 h
Période	08/2022 – 10/2024
Reste à charge titulaire	42 %
France compétences	36 %
Entreprise	22 %

Formations engagées via le CPF — Caisse des Dépôts (open data), tous organismes confondus.