

Expert en gouvernance de la sécurité des réseaux et des systèmes (MS)

RNCP36855 · RNCP · Publiée

L'essentiel

Niveau de qualification	Niveau 7
Code(s) NSF	326n
Formacode(s)	31006, 24293
Code(s) ROME	M1802, M1805
Type d'enregistrement	Enregistrement sur demande
Date d'enregistrement	29/09/2022
Date d'échéance	29/09/2027

Certificateur(s)

INSTITUT MINES TELECOM - TELECOM SUDPARIS · SIRET : 18009202500055

Résumé de la certification

OBJECTIFS ET CONTEXTE

L'Expert en gouvernance de la sécurité des réseaux et systèmes conçoit les architectures de sécurité, élabore et met en place un plan de sécurité destiné à la protection des ressources vitales des entreprises, des collectivités locales, territoriales... contre les attaques internes et externes de toute nature : intrusions, destruction ou exfiltration de données.

ACTIVITÉS VISÉES

L'Expert en gouvernance de la sécurité des réseaux et systèmes conçoit des architectures de sécurité, élabore et met en place un plan de sécurité destiné à la protection des ressources vitales des entreprises, des collectivités locales ou territoriales contre les attaques de toute nature : intrusions, destruction ou exfiltration de données.

Il a pour principales activités :

L'analyse et le traitement des problématiques de cybersécurité, en particulier celles spécifiques aux Opérateurs de Services Essentiels (OSE) : il identifie les problématiques juridiques des opérateurs puis élabore et met en place des solutions y répondant ;

La conduite de projets de cybersécurité : il conçoit des solutions répondant à un cahier des charges, les réalise et les déploie, rédige un rapport sur les réalisations ;

L'analyse des menaces réseau et des mécanismes de sécurisation : il identifie les vulnérabilités, met en place des mécanismes de filtrage, dans le cadre d'une politique de sécurité ;

L'analyse des vulnérabilités et la sécurisation des applications informatiques : il analyse les applications existantes et met en œuvre des méthodologies de développement d'applications sécurisées ;

L'audit du système d'information : il analyse les risques du SI, identifie les vulnérabilités du web, élabore des règles pour la détection d'intrusion ;

Le déploiement de services d'authentification, de chiffrement et de protection de la vie privée dans un système d'information.

COMPÉTENCES ATTESTÉES

Analyser les besoins en cybersécurité des systèmes industriels et des Opérateurs de Services Essentiels dans le cadre de la loi du 26 février 2018 transposant la directive NIS (3) au droit français et dans le respect des obligations requises par l'ANSSI(2)

Proposer et déployer une solution technique répondant aux besoins et aux contraintes d'un Opérateur de Service Essentiel, c'est-à-dire conforme aux 23 règles de sécurité à appliquer dans les 4 domaines que sont : la gouvernance de la sécurité des réseaux et systèmes d'information, la protection des réseaux et systèmes d'information, la défense des réseaux et systèmes d'information et la résilience des activités.

Identifier les réglementations des cadres juridiques français et européen qui s'appliquent dans des situations concrètes liées à la cybersécurité, notamment au sein des Opérateurs de Services Essentiels

Déterminer le rôle et les missions des acteurs cybersécurité de l'entreprise pour organiser efficacement la gestion et la mise en œuvre de solutions

Établir et analyser l'état de l'art associé à une problématique de cybersécurité afin d'en déterminer les enjeux et de concevoir une contribution scientifique permettant d'y répondre

Concevoir un prototype répondant à un cahier des charges et permettant de traiter la problématique identifiée en argumentant les choix réalisés

Réaliser et déployer un prototype de la solution permettant d'évaluer sa faisabilité technique afin de s'assurer que la solution réponde fonctionnellement au cahier des charges

Identifier les différents types d'attaques portant sur le réseau ainsi que les mécanismes de sécurité permettant de faire face à chacun de ces types d'attaques afin de mettre en œuvre les mécanismes de sécurité les plus efficaces face aux menaces identifiées

Mettre en œuvre les règles de filtrage appropriées afin de bloquer des attaques réseau sans entraver le fonctionnement des applications

Configurer et tester un pare-feu nouvelle génération (NGFW) afin de mettre en place une politique de sécurité qui vise à protéger un réseau interne tout en filtrant l'accès à certains services pour les utilisateurs de ce réseau interne

Analyser les vulnérabilités classiques des systèmes d'exploitation et des applications informatiques, identifier les solutions permettant d'y remédier

Mettre en œuvre des mécanismes de contrôle d'accès et d'isolation de fichiers sur un système Unix afin d'empêcher des attaques en confidentialité et en intégrité sur ces fichiers

Analyser une vulnérabilité du noyau Linux pouvant conduire à une élévation de privilèges afin de déterminer les correctifs à apporter

Identifier les risques, découvrir les vulnérabilités afin d'évaluer la sécurité du système d'information

Appliquer la démarche d'analyse de risque EBIOS et employer les outils d'audit d'un réseau afin de professionnaliser la démarche d'audit d'un SI afin de professionnaliser la démarche d'audit d'un SI

Concevoir des règles pour la détection d'intrusion dans le contexte d'un centre de sécurité opérationnelle (SOC) afin de réduire le niveau d'exposition des SI aux risques externes comme internes

Élaborer une méthodologie de réponse à incident pour faire face à des intrusions réelles afin de plus rapidement et efficacement réagir en cas d'attaques

Auditer une application Web et rédiger un rapport d'audit afin d'identifier les vulnérabilités web

Établir les besoins en chiffrement et en authentification dans l'architecture d'un système d'information afin de garantir la confidentialité des données sensibles et de certifier l'identité des utilisateurs de manière robuste

Générer des certificats numériques X.509 et déployer une infrastructure à clés publiques (PKI) afin de mettre en œuvre des connexions sécurisées en HTTPS

Configurer et déployer un réseau privé virtuel (VPN) IPsec entre deux sites distants afin de déterminer les options adéquates à utiliser pour répondre aux différents besoins, notamment en confidentialité et en authentification

Mettre en œuvre des mécanismes d'anonymisation des données afin d'assurer la conformité avec le RGPD

Blocs de compétences

RNCP36855BC01 — Analyser et traiter les problématiques de cybersécurité spécifiques aux Opérateurs de Services Essentiels

LISTE DE COMPÉTENCES

Analyser les besoins en cybersécurité des systèmes industriels et des Opérateurs de Services Essentiels dans le cadre de la loi du 26 février 2018 transposant la directive NIS (3) au droit français et dans le respect des obligations requises par l'ANSSI ;

Proposer et déployer une solution technique répondant aux besoins et aux contraintes d'un Opérateur de Service Essentiel, c'est-à-dire conforme aux 23 règles de sécurité à appliquer dans les 4 domaines que sont :

la gouvernance de la sécurité des réseaux et systèmes d'information, la protection des réseaux et systèmes

d'information, la défense des réseaux et systèmes d'information et la résilience des activités ;
Identifier les réglementations des cadres juridiques français et européen qui s'appliquent dans des situations concrètes liées à la cybersécurité, notamment au sein des Opérateurs de Services Essentiels ;
Déterminer le rôle et les missions des acteurs cybersécurité de l'entreprise pour organiser efficacement la gestion et la mise en œuvre de solutions, en tenant compte de personnel avec un handicap.

MODALITÉS D'ÉVALUATION

Étude de cas portant sur une problématique technique spécifique aux Opérateurs de Services Essentiels

Étude de cas + soutenance visant à traiter des problématiques techniques et juridiques rencontrées par des entreprises

Rapport écrit visant à cartographier les métiers et les pratiques de la cybersécurité au sein des opérateurs de services essentiels

RNCP36855BC02 — Conduire un projet de cybersécurité

LISTE DE COMPÉTENCES

Établir et analyser l'état de l'art associé à une problématique de cybersécurité afin d'en déterminer les enjeux et de concevoir une contribution scientifique permettant d'y répondre

Concevoir un prototype répondant à un cahier des charges et permettant de traiter la problématique identifiée en argumentant les choix réalisés

Réaliser et déployer un prototype de la solution permettant d'évaluer sa faisabilité technique afin de s'assurer que la solution réponde fonctionnellement au cahier des charges

MODALITÉS D'ÉVALUATION

Un projet est à mener sur un sujet de cybersécurité avec livrable de dossiers et soutenance orale devant jury

RNCP36855BC03 — Analyser les menaces réseau et les mécanismes de sécurisation

LISTE DE COMPÉTENCES

Identifier les différents types d'attaques portant sur le réseau ainsi que les mécanismes de sécurité permettant de faire face à chacun de ces types d'attaques afin de mettre en œuvre les mécanismes de sécurité les plus efficaces face aux menaces identifiées

Mettre en œuvre les règles de filtrage appropriées afin de bloquer des attaques réseau sans entraver le fonctionnement des applications

Configurer et tester un pare-feu nouvelle génération (NGFW) afin de mettre en place une politique de sécurité qui vise à protéger un réseau interne tout en filtrant l'accès à certains services pour les utilisateurs de ce réseau interne

MODALITÉS D'ÉVALUATION

Cas pratiques

RNCP36855BC04 — Analyser les vulnérabilités et sécuriser des applications informatiques

LISTE DE COMPÉTENCES

Analyser les vulnérabilités classiques des systèmes d'exploitation et des applications informatiques, identifier les solutions permettant d'y remédier

Mettre en œuvre des mécanismes de contrôle d'accès et d'isolation de fichiers sur un système Unix afin d'empêcher des attaques en confidentialité et en intégrité sur ces fichiers

Analyser une vulnérabilité du noyau Linux pouvant conduire à une élévation de privilèges afin de déterminer les correctifs à apporter

MODALITÉS D'ÉVALUATION

Cas pratiques et étude de cas

RNCP36855BC05 — Auditer un système d'information

LISTE DE COMPÉTENCES

Identifier les risques, découvrir les vulnérabilités afin d'évaluer la sécurité du système d'information

Appliquer la démarche d'analyse de risque EBIOS et employer les outils d'audit d'un réseau afin de professionnaliser la démarche d'audit d'un SI

Concevoir des règles pour la détection d'intrusion dans le contexte d'un centre de sécurité opérationnelle (SOC) afin de réduire le niveau d'exposition des SI aux risques externes comme internes

Élaborer une méthodologie de réponse à incident pour faire face à des intrusions réelles afin de plus rapidement et

efficacement réagir en cas d'attaques

Auditer une application Web et rédiger un rapport d'audit afin d'identifier les vulnérabilités web

MODALITÉS D'ÉVALUATION

Cas pratique, étude de cas, mise en situation pratique

RNCP36855BC06 — Déployer des services d'authentification, de chiffrement et de protection de la vie privée dans un système d'information

LISTE DE COMPÉTENCES

Établir les besoins en chiffrement et en authentification dans l'architecture d'un système d'information afin de garantir la confidentialité des données sensibles et de certifier l'identité des utilisateurs de manière robuste

Générer des certificats numériques X.509 et déployer une infrastructure à clés publiques (PKI) afin de mettre en œuvre des connexions sécurisées en HTTPS

Configurer et déployer un réseau privé virtuel (VPN) IPsec entre deux sites distants afin de déterminer les options adéquates à utiliser pour répondre aux différents besoins, notamment en confidentialité et en authentification

Mettre en œuvre des mécanismes d'anonymisation des bases de données afin d'assurer la conformité avec le RGPD

MODALITÉS D'ÉVALUATION

Cas pratique

Secteur d'activité et type d'emploi

SECTEURS D'ACTIVITÉS

Toutes entreprises, collectivités, sociétés de conseil et entreprises de services du numérique (ESN).

TYPE D'EMPLOIS ACCESSIBLES

Auditeur en sécurité des systèmes d'information - environnements informatiques

Expert sécurité des systèmes et environnements informatiques

Consultant cybersécurité (ou Consultant sécurité)

Évaluateur sécurité

Architecte sécurité

Ingénieur sécurité réseau informatique - système réseau informatique

Expert sécurité des technologies d'information et de communication

Responsable sécurité des systèmes d'information / informatique

Responsable du centre de cyberdéfense

Chef sécurité de projet informatique et/ou métier

Responsable du centre opérationnel de sécurité / Responsable SOC (Security Operation Center)

RÉGLEMENTATIONS D'ACTIVITÉ

Les métiers visés par la certification ne nécessitent pas d'habilitation particulière. Néanmoins, ils nécessitent d'appliquer différentes réglementations et lois, dont :

La directive européenne NIS de 2016 qui a pour but d'assurer un niveau de sécurité élevé et commun pour les réseaux et les systèmes d'information de l'Union européenne.

La loi du 26 février 2018 transposant la directive NIS au droit français et les obligations requises par l'ANSSI, l'autorité désignée pour la France pour accompagner les OSE dans la mise en œuvre de la réglementation.

Le RGPD entré en application le 25 mai 2018, qui encadre le traitement des données de manière égalitaire sur tout le territoire de l'Union Européenne, dans la continuité de la Loi française Informatique et Libertés de 1978.

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)

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) M2X90 — Ingénieurs et cadres d'étude, recherche et développement en informatique et télécom · tension 5/5 (Très élevée) 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 M2X90 — Ingénieurs et cadres d'étude, recherche et développement en informatique et télécom M2X93 — Experts et consultants en systèmes d'information

Voies d'accès

MODALITÉS D'ACCÈS

Apprentissage

PRÉREQUIS À L'ENTRÉE EN FORMATION

Sont recevables les candidatures de 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 national de Master (liste CEFDG) ;

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

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

Titre inscrit au RNCP niveau 7 ;

Diplôme étranger équivalent aux diplômes français exigés ci-dessus.

Par dérogation

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 (hors stage, césure, cursus initial en alternance).

b) pour 30 % maximum du nombre d'étudiants suivant la formation Mastère Spécialisé® concernée, sont recevables les candidatures de 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

Maîtriser le français et l'anglais technique : un niveau de français global de niveau C1, un niveau d'anglais technique de niveau B2 (certains documents, cours et évaluations sont en anglais)

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

Le jury est composé de 4 membres dont 2 professionnels extérieurs à l'organisme certificateur

COMPOSITION DU JURY — VAE

Le jury est composé de 9 membres dont

3 enseignants-chercheurs dans les spécialités enseignées et 3 professionnels extérieurs à l'école et ayant une expérience dans le domaine d'activité du candidat, mais n'appartenant pas à son entreprise.

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	9 157 €
Selon la branche	7 281 € – 12 000 €
Prise en charge	Branches concernées
9 157 €	Valeur par défaut · 180 branches
12 000 €	CPNE Entreprises des activités du déchet et de la propreté urbaine, CPNE autoroutes, CPNE de l'édition de livres, de l'édition phonographique et de l'édition de musique, CPNEF de la Publicité, CPNEF de la presse et des agences de presse
10 683 €	CPNEFP de l'enseignement privé indépendant, CPNEFP de la Restauration rapide
10 164 €	CPNE Casinos, CPNE de la branche de la Distribution Directe
10 000 €	CPNE des exploitations frigorifiques, Commission Paritaire Activités de Marchés Financiers
9 992 €	CPNEF branche retraite complémentaire et prévoyance, CPNEFP Mutualité
9 000 €	CPNEFP de la branche des prestataires de services du secteur tertiaire, CPNEFP des industries des tuiles et briques
8 696 €	CPNEFP des commerces et services de l'audiovisuel, de l'électronique et de l'équipement ménager, CPNEFP des jardineries et graineteries
11 447 €	CPNE des Télécoms
11 446 €	CPNE Travail Temporaire
11 180 €	CPNEFP de la Mutualité Sociale Agricole
10 163 €	CPNEF de l'Exploitation cinématographique et de la Distribution de films
9 842 €	CPNEFP Grands Magasins/ Magasins Populaires
9 800 €	CPNEF de l'audiovisuel
8 775 €	CPNEFP de la branche des entreprises du bureau et du numérique (commerces et services)
8 701 €	CPNE FP Branche des magasins du Bricolage
8 500 €	CPNEFP de la métallurgie
8 000 €	CPNE chimie
7 500 €	CPNE des industries de santé (CPNEIS)
7 281 €	CPNEFP de la Branche des Caisses régionales de Crédit Agricole et autres organismes

Base légale

Date de décision	29/09/2022
Durée de l'enregistrement	5 ans
Date d'échéance de l'enregistrement	29/09/2027

Statistiques

Année	Certifiés	Dont VAE	Insertion 6 mois	Métier 2 ans
-------	-----------	----------	------------------	--------------

2021	17	0	100 %	—
2020	16	0	94 %	100 %
2019	15	0	93 %	100 %

Liens avec d'autres certifications

ANCIENNES VERSIONS
RNCP31043

Pour plus d'informations

LIEN VERS LE DESCRIPTIF

<https://www.telecom-sudparis.eu/formation/mastere-specialise-cybersecurite-des-operateurs-de-services-essentiels>

Fiche officielle (France Compétences)

<https://www.francecompetences.fr/recherche/rncp/36855/>

Où se former

Formations référencées	2
Organismes	1
Régions couvertes	1
Prix indicatif	8 000 €
Durée	63 – 1125 h

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

Se former en apprentissage

Formations en apprentissage	1
Organismes gestionnaires (CFA)	1
Organismes formateurs	1
Régions couvertes	1
Départements couverts	1
Organismes certifiés Qualiopi	1
Sessions	de 09/2026 à 09/2027

Catalogue des formations en apprentissage — réseau des Carif-Oref. Sans frais pour l'alternant : formation financée par l'OPCO de la branche (NPEC).

Entrées et sorties de formation

Entrées en formation	9
Parcours menés à terme	5
Taux d'achèvement	56 %
Période	09/2023 – 09/2026

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

Demande CPF — formations engagées

Dossiers CPF engagés	9
Montant total engagé	61 500 €
Coût moyen par dossier	6 833 €
Durée moyenne	949 h
Période	09/2023 – 07/2026
France compétences	50 %
Reste à charge titulaire	44 %
France Travail	5 %

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