

Opérateur en cybersécurité

RNCP38290 · RNCP · Publiée

L'essentiel

Niveau de qualification	Niveau 5
Code(s) NSF	326
Formacode(s)	31006, 24220, 31032, 31038
Code(s) ROME	M1810, M1801, M1806, M1802
Type d'enregistrement	Enregistrement sur demande
Date d'enregistrement	15/11/2023
Date d'échéance	15/11/2024

Certificateur(s)

ECOLE EUROPEENNE D INTELLIGENCE ECONOMIQUE · SIRET : 49203893000011

Partenaires habilités

4 organismes habilités, d'après la liste publiée par France compétences : 4 à former et organiser l'évaluation.

Organisme	SIRET	Habilitation
APAVE EXPLOITATION FRANCE	90386961800012	Former et organiser l'évaluation
IFPASS//JEDHA	92242930300014	Former et organiser l'évaluation
OFFENSIVE SECURITY	95389509100015	Former et organiser l'évaluation
PARTENAIRES PARTICULIERS	89519916400024	Former et organiser l'évaluation

Résumé de la certification

OBJECTIFS ET CONTEXTE

La cybersécurité est un enjeu majeur pour la France. Le pays est régulièrement la cible de cyberattaques, qui peuvent entraîner des conséquences économiques, politiques et sociales importantes.

Le gouvernement français a pris des mesures qui ont permis de renforcer la cybersécurité du pays, mais il reste encore beaucoup à faire. Le risque cyber a considérablement augmenté ces dernières années, en particulier depuis la crise sanitaire et le conflit russo-ukrainien, concomitant à la numérisation des processus et modes de travail et aux avancées technologiques telles que l'IA et l'informatique quantique. L'ambition nationale dans ce domaine est régulièrement actualisée dans différents documents institutionnels, comme la Revue Nationale Stratégique 2022 publiée par le Secrétariat Général de la Défense et de la Sécurité Nationale qui vise une « résilience cyber de premier rang ».

La cyberdéfense doit donc suivre et faire face aux menaces afin de protéger l'ensemble de nos systèmes et réseaux : hôpitaux, sites industriels, OIV...

Pour se protéger, les entreprises et administrations font alors appel à un opérateur en cybersécurité.

La mission de l'opérateur en cybersécurité est de protéger les données et la fiabilité du système informatique d'une entreprise ou d'une administration en matière de prévention, détection et correction.

Pour cela, il réalise un diagnostic du système d'information dans le but de déceler les éventuels points faibles, apporte différentes solutions de protection pour sécuriser les informations et les données de l'entreprise, met en place les différents processus de sécurité, garantit la pérennité des systèmes de sécurité et actualise ces derniers en

fonction des nouvelles menaces et des dernières technologies. Il est aussi responsable de rétablir dans les meilleures conditions le système d'information ayant subi une attaque.

ACTIVITÉS VISÉES

- Activité 1 - Mise en place de tâches de contrôle et suivi de l'évolution des systèmes
- Activité 2 - Détection de fichiers corrompus avec du code malveillant
- Activité 3 - Gestion d'un parc informatique composé de plusieurs systèmes
- Activité 4 - Optimisation de la gestion des ressources des applications et amélioration de leur scalabilité
- Activité 5 - Prise en compte d'une situation de handicap
- Activité 6 - Administration d'une base de données
- Activité 7 - Conception d'une architecture de bases de données pour une application
- Activité 8 - Configuration et administration d'un réseau d'entreprise
- Activité 9 - Installation d'un réseau d'entreprise
- Activité 10 - Administration d'un réseau d'entreprise et sécurisation des échanges
- Activité 11 - Configuration et administration des réseaux sans fil
- Activité 12 - Mise en place et administration de réseaux virtualisés
- Activité 13 - Surveillance des réseaux informatiques d'une entreprise et détection des potentielles menaces
- Activité 14 - Gestion d'une protection des systèmes d'information
- Activité 15 - Application des mesures de sécurisation des réseaux sans fil
- Activité 16 - Vérification périodique de la sécurisation du réseau filaire d'entreprise (blue, red et purple teams)
- Activité 17 - Vérification périodique de la sécurisation des postes utilisateurs
- Activité 18 - Sécurisation des serveurs et applications web de l'entreprise
- Activité 19 - Recherche et évaluation de la surface d'attaque
- Activité 20 - Sécurisation des échanges
- Activité 21 - Gestion des données

COMPÉTENCES ATTESTÉES

- C1. Développer des scripts d'automatisation afin d'automatiser des tâches répétitives
- C2. Identifier les potentielles vulnérabilités d'un système d'information afin de prévenir des bugs potentiels et mauvaises pratiques de programmation
- C3. Gérer un parc informatique composé de systèmes d'exploitation propriétaires et libres afin d'appréhender l'ensemble des risques liés à une gestion potentiellement défaillante des serveurs et d'anticiper une menace
- C4. Déployer des applications au sein d'environnements virtualisés afin d'optimiser la gestion des ressources des applications et amélioration de leur scalabilité
- C5. Favoriser l'inclusion professionnelle d'une personne en situation de handicap afin d'aménager son poste et son environnement de travail
- C6. Administrer des bases de données de type relationnel afin de maintenir un environnement de base de données robuste et sécurisé.
- C7. Concevoir une architecture de bases de données pour une application afin de préparer la mise en place d'une application de façon sécurisée.
- C8. Administrer un réseau d'entreprise afin de gérer son architecture, son fonctionnement et son organisation
- C9. Déployer et gérer les réseaux à accès pour la connexion des terminaux et usagers (mode projet) afin d'installer un réseau d'entreprise
- C10. Gérer l'articulation des réseaux de transport afin d'interconnecter plusieurs réseaux
- C11. Configurer les réseaux sans fil et mobilité afin de proposer des réseaux sans fil sécurisés et adaptés aux besoins de connectivité d'une entreprise
- C12. Configurer et administrer des réseaux virtualisés afin de gérer des réseaux virtualisés
- C13. Superviser les réseaux informatiques d'une entreprise, les équipements d'infrastructure actifs, systèmes d'exploitation, bases de données afin de détecter des anomalies ou des comportements anormaux et d'isoler les potentielles menaces
- C14. Sécuriser des réseaux et des échanges afin de mettre en œuvre une politique de chiffrement et de sécurité d'accès aux données au sein de l'entreprise
- C15. Attaquer un réseau sans fil afin de tester la sécurité d'un réseau sans fil
- C16. Cartographier les vulnérabilités d'un réseau d'entreprise afin de recréer les conditions d'un piratage informatique
- C17. Utiliser les vulnérabilités d'un réseau d'entreprise dans le cadre de l'attaque d'une machine Windows afin de de

sécuriser les postes des utilisateurs d'un réseau d'entreprise

C18. Utiliser les vulnérabilités d'un réseau d'entreprise dans le cadre d'attaques avancées afin de garantir la sécurisation des applications web de l'entreprise

C19. Utiliser les vulnérabilités Web dans le cadre de la phase de reconnaissance de serveurs afin de repérer les failles existantes et de les corriger

C20. Utiliser les vulnérabilités Web dans le cadre d'attaques sur authentification afin de vérifier le respect des politiques et procédures de gestion des accès.

C21. Utiliser les vulnérabilités Web dans le cadre d'attaques sur CMS afin de protéger l'entreprise de la fuite de données personnelles ou sensibles

Blocs de compétences

RNCP38290BC01 — Réaliser des tâches de programmation

LISTE DE COMPÉTENCES

Développer des scripts d'automatisation, en utilisant les langages les plus utilisés dans le domaine de la sécurité (Python, Bash et C) afin d'automatiser des tâches répétitives

Identifier les potentielles vulnérabilités d'un système d'information en analysant des programmes informatiques développés en Python, Bash et C, en utilisant un outil d'IA afin de prévenir des bugs potentiels et mauvaises pratiques de programmation

MODALITÉS D'ÉVALUATION

Mise en situation professionnelle

- Automatisation de 5 tâches répétitives
- Lecture de trois scripts d'exécution contenant des vulnérabilités et des actions qui visent à nuire aux cibles visées
- Etude de documents et réalisation de l'automatisation d'une tâche
- Analyse de scripts préexistants et recherche de vulnérabilités

RNCP38290BC02 — Configurer et administrer des systèmes et applications dans un environnement virtualisé

LISTE DE COMPÉTENCES

Gérer un parc informatique composé de systèmes d'exploitation propriétaires et libres en assurant l'installation et la maintenance d'un système d'exploitation MICROSOFT & LINUX, en appliquant les correctifs relatifs aux vulnérabilités découvertes par les organismes de détection et de prévention sur les systèmes concernés, en vérifiant que les standards de sécurité sont appliqués afin d'appréhender l'ensemble des risques liés à une gestion potentiellement défaillante des serveurs et d'anticiper une menace

Déployer des applications au sein d'environnements virtualisés en installant et en configurant un serveur virtualisé (VmWare, Hyper V, XEN ...), en appliquant les règles nécessaires pour limiter les risques de failles de sécurité liés à la virtualisation, en utilisant une technologie de conteneurisation (Docker) pour empaqueter les applications et leurs dépendances, en appliquant les procédures d'installation et de configuration nécessaires, en sécurisant l'accès à un serveur virtualisé dans le cadre de la mise en place de la politique de sécurité afin d'optimiser la gestion des ressources des applications et amélioration de leur scalabilité

Favoriser l'inclusion professionnelle d'une personne en situation de handicap en proposant par défaut des équipements et logiciels qui puissent être utilisés par toute personne, quel que soit son handicap potentiel, en proposant, à défaut, des équipements et des logiciels adaptés, en les réglant et en les paramétrant afin d'aménager son poste et son environnement de travail

MODALITÉS D'ÉVALUATION

Mise en situation professionnelle

- Mise en place d'un serveur avec des contraintes de configuration définies dans le cahier des charges d'un client fictif
- Déploiement d'applications dans un environnement virtualisé pour répondre à une expression de besoin
- Identification d'équipements ou de matériels adaptés aux situations de handicap
- Identification des adaptations et des paramétrages sur les logiciels

RNCP38290BC03 — Installer et gérer des bases de données relationnelles

LISTE DE COMPÉTENCES

Administrer des bases de données de type relationnel en s'appuyant sur la méthode MERISE, en effectuant des requêtes SQL, en gérant la conception des bases de données en utilisant Oracle,

MySQL, PostgreSQL, en utilisant les outils de gestion de SGBDR, en appliquant les règles de sécurité sur une base de données relationnelle afin de maintenir un environnement de base de données robuste et sécurisé.

Concevoir une architecture de bases de données pour une application en proposant des solutions techniques (mode projet), en préparant la création des tables de la base, en s'assurant de la fonctionnalité et du bon fonctionnement de la base afin de préparer la mise en place d'une application de façon sécurisée.

MODALITÉS D'ÉVALUATION

Mise en situation professionnelle

- Création d'un schéma de base de données relationnelle
- Installation et administration d'une base de données

RNCP38290BC04 — Configurer et administrer un réseau d'entreprise

LISTE DE COMPÉTENCES

Administrer un réseau d'entreprise en configurant un NAT et un DNS, en calculant et gérant les adressages privés, en détectant les erreurs sur un réseau en analysant le trafic par la connaissance des protocoles IPV4/IPV6, ICMP et de couche Transport: TCP, UDP, en paramétrant les différentes applications à déployer au sein d'une entreprise: de la messagerie à la VOD (Skype, Zoom, etc.) afin de gérer son architecture, son fonctionnement et son organisation

Déployer et gérer les réseaux à accès pour la connexion des terminaux et usagers (mode projet) en paramétrant les réseaux domiciles (WIFI et CPL), en installant un réseau en s'appuyant sur le mécanisme de la boucle locale des entreprises, en paramétrant un système de VLAN respectant la structure organisationnelle de l'entreprise afin d'installer un réseau d'entreprise

Gérer l'articulation des réseaux de transport en s'appuyant sur les notions d'acheminement, de commutation et de routage pour le paramétrage d'un réseau, en vérifiant le bon fonctionnement d'un réseau local d'entreprise à partir d'un point de contrôle, en utilisant les VPN et les solutions pour les mettre en place afin d'interconnecter plusieurs réseaux

Configurer les réseaux sans fil et mobilité en choisissant le type de réseau sans fil approprié en s'appuyant sur les différentes typologies : WPAN, WLAN, WMAN, MRAN, Hot spot, hand over, roaming, UMTS, en consultant et appliquant les référentiels des différentes technologies réseaux sans fil : IEEE 802.15, WPAN, Bluetooth, ZigBee, UWB, en appliquant les principes de IEEE 802.11 (a/b/g/n), en réalisant une veille sur les nouvelles générations de WIFI (ac, af, ah, WiGig), en appliquant les principes de IEEE 802.22 et les futurs produits Wi-RAN, en réalisant une veille sur les évolutions de l'internet ambiant: réseaux mesh, ad-hoc, réseaux de capteurs et RFID, NFC afin de proposer des réseaux sans fil sécurisés et adaptés aux besoins de connectivité d'une entreprise

Configurer et administrer des réseaux virtualisés en virtualisant des serveurs, en intégrant l'impact de cette virtualisation sur l'infrastructure, en appliquant la centralisation du plan de contrôle et les fonctions d'un contrôleur, en employant GNS3, en utilisant le principe de la technique d'accès: ISO 8802.3 (CSMA/CD), en s'appuyant sur les normalisations, IEEE 802 et ISO, les couches physiques, MAC et LLC, les principaux protocoles, en configurant les réseaux locaux virtuels (VLAN), les réseaux locaux Ethernet (SAN, LAN, WLAN), en configurant le paramétrage de pont, commutation de niveau 3, 4 et 7 afin de gérer des réseaux virtualisés

MODALITÉS D'ÉVALUATION

Mise en situation professionnelle

- Mise en place d'un réseau local interconnecté en utilisant l'outil Cisco Packet Tracer
- Au sein d'un réseau local préexistant, recherche, analyse et dépannage des dysfonctionnements
- Mise en place d'un réseau local interconnecté en utilisant l'outil Cisco Packet Tracer incluant la mise en place d'un VPN, d'un serveur Radius et d'un réseau Wifi sécurisé
- Etude de documents, analyse et préconisations pour la mise en place d'un réseau sécurisé hétérogène

RNCP38290BC05 — Superviser et sécuriser les réseaux et les échanges

LISTE DE COMPÉTENCES

Superviser les réseaux informatiques d'une entreprise, les équipements d'infrastructure actifs, systèmes d'exploitation, bases de données en déployant une infrastructure complète et une mise en sécurisation, en utilisant les outils de manipulation de fichiers de logs, en analysant les logs, en paramétrant les outils d'analyse et de

visualisation, en utilisant les outils d'administration et de détection type SIEM, IDS/IPS, pare-feu, en analysant le niveau d'une menace et de la classer selon le niveau de criticité afin de détecter des anomalies ou des comportements anormaux et d'isoler les potentielles menaces

Sécuriser des réseaux et des échanges en utilisant les outils de gestion des identités et des accès, en mettant en œuvre les différentes étapes nécessaires au durcissement d'un poste LINUX et WINDOWS, en appliquant les principes de base de la cryptographie, en mettant en place des règles de filtrage avec les outils appropriés selon le système d'exploitation afin de mettre en œuvre une politique de chiffrement et de sécurité d'accès aux données au sein de l'entreprise

MODALITÉS D'ÉVALUATION

Mise en situation professionnelle

- Mise en place d'un système de surveillance reposant sur les serveurs/agents et l'utilisation d'un IAM
- Analyse de logs et détection des compromissions du système d'information avec proposition de remédiations
- Mise en place de règles de gestion des accès et identités suivant un cahier des charges
- Chiffrement d'une communication entre deux utilisateurs en utilisant un chiffrement asymétrique

RNCP38290BC06 — Tester la sécurité d'un système informatique avec les méthodes de hacking

LISTE DE COMPÉTENCES

Attaquer un réseau sans fil en gérant l'authentification sur un WLAN, en trouvant le SSID, en utilisant les filtres d'adresse MAC, en utilisant le mécanisme de "Shared Key Authentication", en appliquant les techniques adéquates pour accélérer le processus de cracking du chiffrement sur un réseau WLAN, en décryptant des paquets, en utilisant les différents types d'attaques Deni of Service (Dos), en appliquant les attaques Evil Twin, Rogue AP, en utilisant les différents scénarios d'attaque avancée, en appliquant les méthodes de MiTM, Eavesdropping, Session hijacking, en mettant en place une échelle de gravité reposant sur des critères de confidentialité, intégrité, disponibilité, afin de tester la sécurité d'un réseau sans fil

Cartographier les vulnérabilités d'un réseau d'entreprise en appliquant la méthodologie Pentest, en utilisant les outils de scanning, en utilisant Metasploit, en utilisant les outils tels que Wireshark afin d'effectuer du sniffing, en appliquant les différentes attaques possibles sur un routeur: SSH, SNMP, SMTP, etc., en utilisant un exploit afin d'obtenir un accès machine, en détectant et contournant un firewall pour porter une attaque sur une machine WINDOWS, en appliquant la technique de port forwarding, en utilisant le pivoting, en appliquant les techniques d'élévation de privilèges afin de recréer les conditions d'un piratage informatique

Utiliser les vulnérabilités d'un réseau d'entreprise dans le cadre de l'attaque d'une machine Windows en utilisant un exploit afin d'obtenir un accès machine, en détectant et contournant un firewall pour porter une attaque sur une machine WINDOWS, en appliquant la technique de port forwarding, en utilisant le pivoting, en appliquant les techniques d'élévation de privilèges, en employant les techniques d'Anti-Virus Evasion, en manipulant les techniques d'attaque sur les navigateurs, en utilisant les outils et levier pour une attaque par social engineering, en utilisant les méthodes de gestion de patch et de mises à jour afin de sécuriser les postes des utilisateurs d'un réseau d'entreprise

Utiliser les vulnérabilités d'un réseau d'entreprise dans le cadre d'attaques avancées en utilisant les outils et techniques avancées tels que Metasploit Loader, DLL Hijacking, DLL Main, Shell Code Exec, etc., en s'appuyant sur les standards OWASP, en utilisant les différents outils de scanning proxy et Nessus, en utilisant les failles RFI & LFI, en utilisant les failles Upload, en effectuant du Cross Site Scripting et du Cross Site Request Forgery, en utilisant les techniques de SQL Injection, Clickjacking, Injection HTML, Injection de commandes, etc., en paramétrant une Exploitation Server Side et Client Side (MiTM, Social Engineering), afin de garantir la sécurisation des applications web de l'entreprise

Utiliser les vulnérabilités Web dans le cadre de la phase de reconnaissance de serveurs en s'appuyant sur les standards OWASP, en utilisant les différents outils de scanning proxy et Nessus afin de repérer les failles existantes et de les corriger

Utiliser les vulnérabilités Web dans le cadre d'attaques sur authentification en utilisant les techniques de Hijacking, Brute Force et attaque sur les protocoles sécurisés, en utilisant les techniques d'injection SQL et d'utilisation de formulaires non sécurisés afin de vérifier le respect des politiques et procédures de gestion des accès.

Utiliser les vulnérabilités Web dans le cadre d'attaques sur CMS en utilisant les techniques d'attaque sur les principaux CMS tels que WordPress, Joomla, Drupal afin de protéger l'entreprise de la fuite de données personnelles ou sensibles

MODALITÉS D'ÉVALUATION

Mise en situation professionnelle

- Mise en place d'un réseau Wifi vulnérable, attaque d'un réseau Wifi et proposition de remédiations
- Attaque fictive d'un réseau sans fil WLAN - Prise de contrôle fictive d'un réseau sans fil WLAN
- Mise en place d'un réseau filaire vulnérable, attaque et proposition de remédiations
- Attaque fictive d'un réseau filaire - Prise de contrôle fictive d'un réseau
- Utilisation d'outils de tests d'intrusion pour détecter les failles réseaux et systèmes
- Cartographie de l'ensemble des vulnérabilités découvertes sur un réseau et proposition de remédiation
- Explication et utilisation des techniques de hacking pour améliorer la résilience du système d'information
- Etude des référentiels de sécurisation d'un système d'information (famille ISO27000-Nist800-53 ; RGPD)

Secteur d'activité et type d'emploi

SECTEURS D'ACTIVITÉS

Entreprises du secteur privé : Dans les entreprises privées, l'opérateur en cybersécurité travaille le plus souvent au sein du département informatique ou du service de sécurité informatique. Il contribue à protéger les systèmes et les données de l'entreprise contre les cybermenaces, les attaques de pirates informatiques et les actes de malveillance internes ou externes.

Entreprises du secteur public : Dans le secteur public, l'opérateur en cybersécurité peut être employé par des organismes gouvernementaux, des ministères ou des agences. Sa mission consiste à protéger les infrastructures gouvernementales, les réseaux et les données sensibles contre les cyberattaques qui pourraient compromettre la sécurité nationale ou les services publics.

Fournisseurs de services de cybersécurité : L'opérateur en cybersécurité travaille pour des entreprises de services de sécurité informatique spécialisées. Ces entreprises fournissent des solutions et des services de sécurité à d'autres organisations et l'opérateur en cybersécurité intervient dans le cadre d'une prestation de services.

Institutions financières : Les banques et autres institutions financières ont des exigences de sécurité élevées en raison de la nature sensible des informations financières qu'elles gèrent. L'opérateur en cybersécurité dans ce secteur est responsable de protéger les transactions, les données des clients et les systèmes financiers contre les cybermenaces.

Organisations de santé : Les établissements de santé gèrent de grandes quantités de données sensibles sur les patients, ce qui les rend vulnérables aux attaques de ransomwares et d'autres cybermenaces. L'opérateur en cybersécurité travaille pour protéger les dossiers médicaux électroniques et les systèmes de santé contre les attaques.

Infrastructures critiques : L'opérateur en cybersécurité peut également être missionné dans la protection des infrastructures critiques telles que les réseaux d'énergie, de transport et de distribution d'eau. La cybersécurité de ces infrastructures est cruciale car une attaque pourrait entraîner des conséquences graves.

TYPE D'EMPLOIS ACCESSIBLES

- Opérateur en cybersécurité
- Opérateur Cyber Défense
- Technicien en cybersécurité
- Analyste SOC (Security Operation Center)

RÈGLEMENTATIONS D'ACTIVITÉ

L'apparition de nouvelles structures telles que les SOC permet notamment de répondre aux enjeux fixés par l'article 22 de la loi de programmation militaire (LPM) (loi n° 2013-1168 du 18 décembre 2013) qui fait suite aux préconisations du Livre blanc sur la défense et la sécurité nationale de 2013.

L'objectif est de renforcer la sécurité des systèmes d'information critiques exploités par les Opérateurs d'Importance Vitale: les systèmes d'information d'importance vitale (SIIV).

Les OIV sont des acteurs publics ou privés dont les activités sont jugées indispensables au bon fonctionnement et à la survie de la Nation. La liste des OIV est confidentielle, mais on estime le nombre d'OIV entre 200 et 300. Afin d'améliorer la protection de ces OIV tout en permettant à l'ANSSI de mieux les soutenir et de les accompagner en cas d'attaques informatiques, l'État a fait évoluer le Code de la défense via la LPM, pour imposer un certain nombre de règles relatives à leur cybersécurité.

La LPM s'inscrit dans la continuité d'une importante prise de conscience étatique du «risque cyber». Un large dispositif interministériel de sécurité des activités d'importance vitale (SAIV) protège les OIV des risques de sûreté

habituels depuis 2006. Les SAIV représentent des activités qui ont trait à la production et à la distribution de biens ou de services indispensables à la continuité de l'État et pour subvenir aux besoins vitaux de la population. Pour faire face aux nouvelles menaces cyber, l'article 22 de cette loi vient définir les responsabilités et les obligations des OIV en termes de protection de leurs systèmes d'information critiques. Il oblige ainsi les OIV à faire auditer leurs SIIV (Systèmes d'Information d'Importance Vitale) par des organismes qualifiés PASSI (Prestataires d'Audit SSI) ainsi qu'à mettre en œuvre les mesures de sécurité des systèmes d'informations (SSI) et des systèmes de détection qualifiés. Plus encore, l'article contraint les OIV à déclarer de façon immédiate des incidents SSI affectant de manière significative leurs SIIV.

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

Être titulaire d'un diplôme ou titre d'un niveau 4 avec un bon niveau d'anglais technique, ou avoir une expérience significative de 2 ans et les compétences informatiques nécessaires à l'exercice du métier d'opérateur et une bonne compréhension du fonctionnement des entreprises.

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

Le jury compte au moins 3 personnes, professionnels du domaine de la cybersécurité.

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	8 615 €
-------------------------	---------

Selon la branche

7 836 € – 8 838 €

Prise en charge	Branches concernées
8 615 €	Valeur par défaut · 205 branches
8 838 €	CPNE de l'ingénierie, des services informatiques et du conseil, CPNEFP de la métallurgie
8 730 €	CPNEFP des commerces et services de l'audiovisuel, de l'électronique et de l'équipement ménager, CPNEFP du Négoce de l'ameublement
8 500 €	CPNE des industries de santé (CPNEIS)
8 462 €	CPNEFP dans les établissements d'enseignement privés sous contrat
8 400 €	CPNEFP ICGV entreprises de la viande
7 836 €	CPNE des Télécoms

Base légale

Date de décision	15/11/2023
Durée de l'enregistrement	1 an
Date d'échéance de l'enregistrement	15/11/2024
Date de dernière délivrance possible	15/11/2028

Statistiques

Année	Certifiés	Dont VAE	Insertion 6 mois	Métier 2 ans
2023	11	0	91 %	—
2022	2	2	100 %	—

Liens avec d'autres certifications

ANCIENNES VERSIONS

RNCP34975

NOUVELLE(S) CERTIFICATION(S)

RNCP41678

CORRESPONDANCES (PAR BLOCS)

RNCP36164, RNCP37391, RS5031, RS5568

Pour plus d'informations

LIEN VERS LE DESCRIPTIF

<https://eecs.fr/>

Fiche officielle (France Compétences)

<https://www.francecompetences.fr/recherche/rncp/38290/>

Entrées et sorties de formation

Entrées en formation	13
----------------------	----

Parcours menés à terme	11
Taux d'achèvement	85 %
Période	03/2024 – 12/2024

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

Demande CPF — formations engagées

Dossiers CPF engagés	13
Montant total engagé	156 000 €
Coût moyen par dossier	12 000 €
Durée moyenne	600 h
Période	01/2024 – 03/2024
Régions	77 %
France Travail	19 %
France compétences	4 %
Compte d'engagement citoyen	0 %

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