

Opérateur en cybersécurité

RNCP34975 · RNCP · Publiée

L'essentiel

Niveau de qualification	Niveau 5
Code(s) NSF	326
Formacode(s)	31006, 24220, 31032, 31038
Code(s) ROME	M1802, M1801, M1810
Type d'enregistrement	Enregistrement sur demande
Date d'enregistrement	14/10/2020
Date d'échéance	14/10/2023

Certificateur(s)

ECOLE EUROPEENNE D INTELLIGENCE ECONOMIQUE · SIRET : 49203893000011

Résumé de la certification

OBJECTIFS ET CONTEXTE

Portée par un ensemble d'acteurs, la France a pris conscience de l'intérêt de développer la filière de la cybersécurité et s'est dotée de moyens importants pour répondre à ses objectifs.

Cet espace riche d'opportunité présente des risques et des menaces qui nécessitent d'être pris en compte dans la stratégie de développement à l'échelle nationale et européenne. A ce titre, la France a placé, grâce au Livre Blanc sur la défense et la sécurité nationale, la cybersécurité au rang de priorité nationale.

Plusieurs domaines comme la sécurité des données, la sécurité des applications, la sécurité des produits et équipements, l'infogérance et l'exploitation, la formation, etc., permettent de mettre en exergue l'émergence de nouveaux métiers, notamment celui d'opérateur en cybersécurité. Soutenue par des acteurs étatiques, tels que l'ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information), de nouveaux types d'organisation sont proposés aux entreprises et aux administrations afin de faire face à la menace.

ACTIVITÉS VISÉES

Les

opérateurs

interprètent

les

événements

de sécurité,

écoutent

le

«bruit

de

fond»

et

traitent

les alertes et les incidents. Selon la taille du SOC, les opérateurs sont organisés en niveaux à l'image d'un centre de

support. Ainsi

les opérateurs de niveau 1 dégrossissent et pré-qualifient les alertes, appels, tickets.

Leur première tâche consiste à formaliser et enregistrer le contexte de l'incident. Les activités sont majoritairement

cadrées
par
des procédures
et
tout
écart
donne systématiquement
lieu
à

une escalade vers le niveau 2. Leurs principales activités peuvent être classées en 3 parties :

Analyse et interprétation des
différentes remontées des alertes issues du centre de supervision
Anticiper les nouveaux modes opératoires des cybercriminels
Reporting et documentation

COMPÉTENCES ATTESTÉES

Réaliser des tâches de programmation
Configurer et administrer systèmes et applications dans un environnement virtualisé
Installer et gérer des bases de données relationnelles
Configurer et administrer un réseau d'entreprise
Superviser et sécuriser les réseaux et les échanges
Tester la sécurité d'un réseau informatique avec les méthodes de hacking

Blocs de compétences

RNCP34975BC01 — Réaliser des tâches de programmation

LISTE DE COMPÉTENCES

Développer des scripts d'automatisation de tâches
Développer avec les langages les plus utilisés dans le domaine de la sécurité: Python, Bash et Shell afin de rédiger des scripts d'automatisation
Analyser un programme informatique
Analyser des programmes informatiques développés en Python, Bash et Shell afin de trouver les potentielles vulnérabilités et déceler si les tâches exécutées peuvent présenter une menace pour les systèmes visés

MODALITÉS D'ÉVALUATION

Mise en situation professionnelle : 5 tâches répétitives seront à automatiser afin de valider les compétences des opérateurs
Mise en situation professionnelle : lecture de trois scripts d'exécution contenant des vulnérabilités et des actions qui visent à nuire les cibles visées

RNCP34975BC02 — Configurer et administrer systèmes et applications dans un environnement virtualisé

LISTE DE COMPÉTENCES

Gérer un parc informatique composé de systèmes d'exploitation propriétaires et libres
Assurer le bon fonctionnement d'un système d'exploitation Microsoft & Linux
Administrer correctement un système afin d'appréhender l'ensemble des risques liés à la mauvaise gestion des serveurs
Appliquer les correctifs relatifs aux dernières vulnérabilités découvertes par les organismes de détection et de prévention sur les systèmes concernés
Vérifier que les standards de sécurité soient appliqués afin de prévenir une menace
Déployer des applications au sein d'environnements virtualisés
Appliquer les règles nécessaires pour limiter les risques de failles de sécurité liés à la virtualisation
Installer et configurer un serveur virtualisé en appliquant les procédures d'installation et de configuration nécessaires
Sécuriser l'accès à un serveur virtualisé dans le cadre de la mise en place de la politique de sécurité

MODALITÉS D'ÉVALUATION

Mise en situation professionnelle : Mettre en place un serveur Windows avec des contraintes de configuration

proposée dans un cahier des charges client

Mise en situation professionnelle : Mettre en place un serveur Linux avec des contraintes de configuration proposée dans un cahier des charges client

Mise en situation professionnelle : Mettre en place un ensemble de serveurs virtualisés et les interconnecter

RNCP34975BC03 — Installer et gérer des bases de données relationnelles

LISTE DE COMPÉTENCES

Administrer des bases de données de type relationnel

S'appuyer sur la méthode MERISE

Effectuer des requêtes SQL

Gérer la conception des bases de données en utilisant Oracle, SQL Server Microsoft, MySql, PostgreSQL

Employer les outils de gestion de SGBDR

Appliquer les règles de sécurité sur une base de données relationnelle

MODALITÉS D'ÉVALUATION

Mise en situation professionnelle : installer et administrer une base de données

RNCP34975BC04 — Configurer et administrer un réseau d'entreprise

LISTE DE COMPÉTENCES

Administrer un réseau d'entreprise en gérant son architecture, son fonctionnement et son organisation

Configurer un NAT et un DNS

Calculer et gérer les adressages public et privé

Détecter les erreurs sur un réseau en analysant le trafic par la connaissance des protocoles IPV4/IPV6, ICMP et de couche Transport: TCP, UDP, RTP

Paramétrer les différentes applications à déployer au sein d'une entreprise: de la messagerie à la VOD (Skype, Zoom, etc.)

Déployer et gérer les réseaux à accès pour la connexion des terminaux et usagers

Choisir les différents supports de transmission: paire torsadée (ADSL, VDSL), la boucle locale optique (FTTB, FTT, FTTdp), les solutions câblo-opérateurs, les modems câbles, la boucle locale radio, wifi, les réseaux domicile (WIFI et CPL)

Choisir les solutions cellulaires appropriées au besoin des salariés (3G/4G/4G+/5G)

Paramétrer les réseaux domiciles (WIFI et CPL)

Installer un réseau en s'appuyant sur le mécanisme de la boucle locale des entreprises

Gérer l'articulation des réseaux de transport

Paramétrer son réseau en s'appuyant sur les notions d'acheminement, de commutation et de routage

Vérifier le bon fonctionnement d'un réseau local d'entreprise à partir de point de contrôle

Appliquer la commutation de labels et l'architecture MPLS au sein d'un réseau

Utiliser les VPN et les solutions pour les mettre en place

Configurer les réseaux sans fil et mobilité

Choisir le type de réseau sans fil approprié en s'appuyant sur les différentes typologies: WPAN, WLAN, WMAN, MRAN, Hot spot, hand over, roaming, GPRS, UMTS

Consulter et appliquer les référentiels des différentes technologies réseaux sans fil: IEEE 802.15, WPAN, Bluetooth, ZigBee, UWB

Appliquer les principes de IEEE 802.11 (a/b/e/g/n)

Faire une veille sur les nouvelles générations de WIFI (ac, af, ah, WiGig)

Appliquer les principes de IEEE 802.22 et les futurs produits Wi-RAN

Faire une veille sur les évolutions de l'internet ambiant: réseaux mesh, ad-hoc, réseaux de capteurs et RFID, NFC

Configurer et administrer des réseaux virtualisés

Virtualiser des serveurs et comprendre l'impact sur l'infrastructure

Appliquer la centralisation du plan de contrôle et les fonctions d'un contrôleur

Employer le protocole OpenFlow et l'évolution SDN (Software Defined Networking)

Utiliser le principe de la technique d'accès: ISO 8802.3 (CSMA/CD)

S'appuyer sur les normalisations, IEEE 802 et ISO, les couches physiques, MAC et LLC, les principaux protocoles

Configurer les réseaux locaux virtuels (VLAN), les réseaux locaux Ethernet (SAN, LAN, WLAN)

Configurer le paramétrage de pont, commutation de niveau 3, 4 et 7

MODALITÉS D'ÉVALUATION

Mise en situation professionnelle : Mettre en place un réseau local en utilisant l'outil Cisco Packet Tracer

Mise en situation théorique: répondre à un QCM de 40 questions

Mise en situation professionnelle : au sein d'un réseau local déjà monté, paramétrer un routeur et utiliser un commutateur en utilisant l'outil Cisco Packet Tracer

Mise en situation professionnelle : au sein d'un réseau local déjà monté, mettre en place une connexion sécurisée par un tunnel VPN en utilisant l'outil Cisco Packet Tracer

Mise en situation professionnelle : configurer un réseau local WIFI en utilisant l'outil Cisco Packet Tracer

Mise en situation professionnelle : configurer un réseau local virtuel en utilisant l'outil Cisco Packet Tracer

RNCP34975BC05 — Superviser et sécuriser les réseaux et les échanges

LISTE DE COMPÉTENCES

Supervision des réseaux informatiques d'une entreprise

Utiliser les outils de manipulation de fichiers de logs

Analyser les logs afin de détecter des anomalies ou des comportements anormaux

Paramétrer les outils d'analyse et de visualisation de type Elasticsearch et Kibana

Utiliser les outils d'administration et de détection type SIEM, IDS/IPS

Analyser le niveau d'une menace et de la classer selon le niveau de criticité

Sécurisation des réseaux et des échanges

Utiliser les outils de gestion des identités et des accès afin de mettre en place une politique de sécurité d'accès aux données au sein de l'entreprise

Mettre en oeuvre les différentes étapes nécessaires au durcissement d'un poste linux et windows

Appliquer les principes de base de la cryptographie afin de mettre en place une politique de chiffrement adéquat

Mettre en place des règles de filtrage en utilisant les outils appropriés selon le système d'exploitation

MODALITÉS D'ÉVALUATION

Mise en situation professionnelle : utiliser un système de visualisation et d'interprétation de logs

Mise en situation professionnelle : Appliquer des règles de gestion d'accès en utilisant un IAM

Mise en situation professionnelle : Durcir un poste linux et windows

Mise en situation professionnelle de 2 heures: Chiffrer une communication en deux utilisateurs en utilisant un chiffrement asymétrique

Mise en situation professionnelle : appliquer des règles de parefeu sur un environnement linux

RNCP34975BC06 — Tester la sécurité d'un réseau informatique avec les méthodes de hacking

LISTE DE COMPÉTENCES

Attaquer un réseau sans fil

Gérer l'authentification sur un WLAN

Trouver le SSID

Utiliser les filtres d'adresse MAC

Utiliser le mécanisme de "Shared Key Authentication"

Attaquer un réseau sans fil par les vulnérabilités de chiffrement WLAN

Appliquer les techniques adéquates pour accélérer le processus de cracking

Décrypter des paquets

Attaquer un réseau sans fil en visant l'infrastructure

Appliquer la méthodologie pour structurer son attaque

Identifier un routeur sur un réseau

Utiliser les différents types d'attaques Deni of Service (Dos)

Appliquer les attaques Evil Twin, Rogue AP.

Utiliser les différents scénarios d'attaque avancée

Appliquer les méthodes de MiTM, Eavesdropping, Session hijacking

Cartographier les configurations de sécurité client

Attaquer un réseau sans fil type WPA-E et Radius

Appliquer les différentes attaques WPA-E et cartographier l'architecture

Configurer et installer l'AP et le FreeRadius-WPE

Pratiquer une attaque EAP

Appliquer les best practices de sécurisation WLAN-E

- Attaquer un réseau sans fil type WPS et Probe
- Appliquer les différentes attaques WPS et cartographier l'architecture
- Appliquer les techniques de Probe Sniffing
- Cartographier les vulnérabilités d'un réseau
- Appliquer la méthodologie pentest
- Utiliser les outils de scanning
- Utiliser Metasploit
- Employer les outils tels que Wireshark afin d'effectuer du sniffing
- Appliquer les méthodes pour effectuer du spoofing
- Mettre en place un MiTM
- Appliquer les bases de l'attaque VOIP
- Effectuer du flooding
- Utiliser les vulnérabilités d'un réseau dans le cadre de l'attaque routeur
- Appliquer les différentes attaques possibles sur un routeur: SSH, SNMP, CISCO, etc.
- Utiliser les vulnérabilités d'un réseau dans le cadre de l'attaque d'une machine Windows
- Utiliser un exploit afin d'obtenir un accès machine
- Détecter et désactiver d'un firewall pour porter une attaque sur une machine windows
- Appliquer la technique de port forwarding
- Utiliser le pivoting
- Appliquer la technique du tunneling
- Appliquer les techniques d'élévation de privilèges
- Utiliser les vulnérabilités d'un réseau dans le cadre de la post-exploitation
- Monitorer ses accès dans le but d'effacer ses traces.
- Utiliser les techniques de maintien de session
- Manipuler les outils tels que PowerShell et/ou WevTUTIL pour limiter les traces au sein des logs
- Utiliser les vulnérabilités d'un réseau dans le cadre d'attaques sur les postes clients
- Employer les techniques d'Anti-Virus Evasion
- Manipuler les techniques d'attaque sur les navigateurs
- Utiliser les outils et levier pour une attaque par social engineering
- Utiliser les vulnérabilités d'un réseau dans le cadre d'attaques avancées
- Connaître les outils et techniques avancées tels que Metasploit Loader, DLL Hijacking, DLL Main, Shell Code Exec, etc.
- Utiliser les vulnérabilités Web dans le cadre de la phase de reconnaissance
- S'appuyer sur les standards OWASP
- Utiliser les différents outils de scanning proxy et Nessus
- Utiliser les vulnérabilités Web dans le cadre de la phase exploitation
- Utiliser les failles RFI & LFI
- Utiliser les failles Upload
- Effectuer du Cross Site Scripting et du Cross Site Request Forgery
- Utiliser les techniques de SQL Injection, Clickjacking, Injection HTML, Injection de commandes, etc.
- Paramétrer une Exploitation Server Side et Client Side (MiTM, Social Engineering)
- Utiliser les vulnérabilités Web dans le cadre d'attaques sur authentification
- Utiliser les techniques de Hijacking, Brute Force et attaque sur les protocoles sécurisés
- Utiliser les vulnérabilités Web dans le cadre d'attaques sur CMS
- Utiliser les techniques d'attaque sur les principaux CMS tels que WordPress, Joomla, etc.

MODALITÉS D'ÉVALUATION

- Mise en situation professionnelle : Attaquer un réseau sans fil WLAN afin d'en prendre son contrôle
- Mise en situation professionnelle : Attaquer un réseau LAN entreprise
- Mise en situation professionnelle : Attaquer un site Web afin de prendre le contrôle d'un serveur

Secteur d'activité et type d'emploi

SECTEURS D'ACTIVITÉS

La cybersécurité concerne tous les secteurs d'activités sans exception. Que soit dans le domaine bancaire, du luxe,

automobile, de l'industrie (quelque soit l'activité), elle doit faire partie du quotidien afin de se prémunir de potentielles attaques.

Le déploiement généralisé des mobiles, du Cloud, des réseaux sociaux, du Business Intelligence et des objets connectés dans les marchés verticaux sont les moteurs principaux du développement de nouveaux services et technologies de cybersécurité.

TYPE D'EMPLOIS ACCESSIBLES

Opérateur en cybersécurité - Opérateur Cyber Défense

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

MODALITÉS D'ACCÈS

Formation initiale

PRÉREQUIS À L'ENTRÉE EN FORMATION

Etre titulaire d'un diplôme ou titre d'un niveau 4 (au minimum) avec un bon niveau d'anglais technique ou avoir une expérience significative de deux ans permettant d'acquérir les compétences informatiques nécessaires à l'exercice du métier d'opérateur et une bonne compréhension du fonctionnement des entreprises.

COMPOSITION DU JURY — FORMATION INITIALE

Le jury compte au moins 3 personnes.

Il est composé de professionnels du domaine de la cybersécurité.

Le président du jury est désigné par l'ensemble des membres du jury.

80% de ses membres sont extérieurs à l'organisme de formation délivrant.

100% des évaluateurs exercent une activité professionnelle en plus de leur activité pédagogique (dans 90% des cas, l'activité autre que pédagogique est l'activité principale).

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

Le jury compte au moins 3 personnes. Il est composé de professionnels du domaine de la cybersécurité.

2/3 de ses membres sont extérieurs à l'organisme de formation délivrant.

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	14/10/2020
Durée de l'enregistrement	3 ans

Liens avec d'autres certifications

NOUVELLE(S) CERTIFICATION(S)
RNCP38290

Pour plus d'informations

Fiche officielle (France Compétences)

<https://www.francecompetences.fr/recherche/rncp/34975/>