TITRE PROFESSIONNEL OPERATEUR EN CYBERSECURITE
Code RNCP : RNCP 41678
Certificateur : Ecole Européenne d'Intelligence Economique
Date d'enregistrement : 27/11/2025
Lien vers la fiche France Compétences : https://www.francecompetences.fr/recherche/rncp/41678

Contact de la personne en charge de la formation
M Cyprien Francart - Tel. : 06 70 80 01 21 - mail. : cyprien.francart@eecs.fr

Voie d'accès : Alternance / Formation continue / VAE - Formation accessible par blocs de compétences.
Niveau de sortie : niveau 5 (bac +2)
Volume horaire : 1 000 h
Durée : 24 mois minimum - début des cours en septembre

Modalités de la formation : en présentiel dans les locaux loués par l'EEIE à Versailles.

Lieu de la formation : 36 rue des Etats Généraux 78000 Versailles

Accessibilité : Nous accueillons les personnes en situation de handicap dans nos formations, sous réserve que leur état de santé le permette. Pour étudier ensemble les possibilités d'aménagement, contactez notre référent handicap : Laure de Saint Sernin : laure.desaintsernin@eeie.fr

Présentation de la formation :
La cybersécurité est aujourd'hui un enjeu stratégique pour la France, face à la multiplication des cyberattaques qui menacent les infrastructures critiques et les entreprises. L'augmentation des risques, liée à la numérisation, à l'IA et aux tensions géopolitiques, impose de renforcer la protection des systèmes d'information.
La formation prépare à ce défi en formant des opérateurs en cybersécurité, experts en prévention, détection et réponse aux incidents. Les participants apprendront à réaliser des diagnostics de sécurité, identifier les vulnérabilités, mettre en place des solutions de protection, assurer la pérennité des systèmes et intervenir efficacement en cas d'attaque. Ces compétences sont essentielles pour garantir la fiabilité des réseaux et des données dans un contexte où la cyberdéfense est devenue indispensable.

La formation est composée de 5 blocs de compétences, à savoir :
BC01 - Réaliser des tâches de programmation
BC02 - Configurer et administrer des systèmes et applications dans un environnement virtualisé
BC03 - Installer et gérer des bases de données relationnelles
BC04 - Configurer et administrer un réseau d'entreprise
BC05 - Superviser et sécuriser les réseaux et les échanges

Résultats attendus :

- La formation prépare au titre professionnel « Opérateur en Cybersécurité », enregistré au RNCP le 127/11/2025 sous le n°41678 et délivré par l'École Européenne de Cybersécurité (Groupe EEIE).
- Possibilité de validation partielle par blocs de compétences.

Points forts de la formation :

- Programme construit à partir des référentiels métiers de la cybersécurité (analyste SOC, pentester, RSSI junior, technicien cybersécurité).
- Apprentissage centré sur les situations professionnelles réelles, avec des exercices progressifs et des études de cas.
- Formateurs (Praticiens en activité) issus de l'écosystème cyber : SOC, CERT, pentests, audit de sécurité, gouvernance, réponse à incident.

Objectifs et Compétences visées, à l'issue de la formation, vous serez en mesure de :

- Réaliser des tâches de programmation
- Développer des scripts d'automatisation
- Identifier les potentielles vulnérabilités d'un système d'information
- Gérer un parc informatique composé de systèmes d'exploitation propriétaires et libres
- Déployer des applications au sein d'environnements virtualisés
- Favoriser l'inclusion professionnelle d'une personne en situation de handicap
- Administrer des bases de données de type relationnel en s'appuyant sur la méthode MERISE
- Concevoir une architecture de bases de données pour une application en proposant des solutions techniques
- Administrer un réseau d'entreprise en configurant un NAT et un DNS
- Déployer et gérer les réseaux à accès pour la connexion des terminaux et usagers
- Gérer l'articulation des réseaux de transport en s'appuyant sur les notions d'acheminement, de commutation et de routage
- Configurer les réseaux sans fil et mobilité
- Configurer et administrer des réseaux virtualisés
- Superviser les réseaux informatiques d'une entreprise
- Sécuriser des réseaux et des échanges en utilisant les outils de gestion des identités et des accès
- Attaquer un réseau sans fil afin de tester la sécurité d'un réseau sans fil
- Cartographier les vulnérabilités d'un réseau d'entreprise
- Utiliser les vulnérabilités d'un réseau d'entreprise dans le cadre de l'attaque d'une machine Windows
- Utiliser les vulnérabilités d'un réseau d'entreprise dans le cadre d'attaques avancées
- Utiliser les vulnérabilités Web dans le cadre de la phase de reconnaissance de serveurs
- Utiliser les vulnérabilités Web dans le cadre d'attaques sur authentification
- Utiliser les vulnérabilités Web dans le cadre d'attaques sur CMS.

Métiers et débouchés :
Opérateur en cybersécurité ; Opérateur Cyber Défense ; Technicien en cybersécurité ; Analyste SOC (Security Operation Center)

Indicateurs (Données sur la dernière promotion certifiée) **:**
- Taux de réussite dans la certification : 79%
- Taux de placement en entreprise post-formation : 85%
- Nombre de diplômé satisfait de la formation : 100%

Secteurs d'activités :
- Tous les secteurs d'activité : Entreprises du secteur privé, entreprises du secteur public, fournisseurs de services de cybersécurité, institutions financières, organisations de santé, infrastructures critiques :

Public visé : Toute personne souhaitant développer des compétences en cybersécurité

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

Dispositions pratiques :
- Nombre de participants minimum : 10
- Nombre de participants maximum : 30

Modalités d'admission et délai d'accès
- Vérification des prérequis en amont de la contractualisation sur dossier, test et entretien. Admission après étude du dossier de candidature, test et entretien.

Tarifs : 9 000 € Exonération de TVA en vu de l'article 261-4-4 a. du CGI

Financement
- Différents modes de financements peuvent être mobilisés. Nous contacter pour toute demande.
- Pour le CPF :
  - Tout stagiaire faisant appel à un financement CPF a l'obligation de se présenter à la session certificative.
  - Conditions d'inscription en formation financée via le CPF : complétude d'une attestation sur l'honneur qui confirme le droit du titulaire à mobiliser ses droits : https://www.of.moncompteformation.gouv.fr/espace-public/sites/of/files/2024-01/attestation-sur-l-honneur-titulaires-de-compte.pdf
  - Pour consulter les conditions particulières titulaires : https://of.moncompteformation.gouv.fr/espace-public/sites/of/files/2025-04/CP_Titulaires_V13_VF_sign_0.pdf
  - Reste à charge pour tout financement via le CPF (décret mai 2024) hormis pour les demandeurs d'emploi : nous consulter pour toute précision.

Méthodes pédagogiques mobilisées :

- Alternance entre apports théoriques et mises en situation pratiques.
- Accompagnement individualisé tout au long de la formation.

Moyens pédagogiques :

- Vidéoprojecteur
- Tableau blanc / Paperboard
- Parc informatique dédié (PC hautes performances, VM, cartes réseau configurables)
- Laboratoires virtuels (VMware / VirtualBox / Proxmox) pour les environnements sandboxés
- Serveurs physiques dédié
- Switchs administrables, routeurs, points d'accès WiFi dédiés
- Plateforme d'e-learning / LMS
- Assistance technique et pédagogique

Modalités de suivi et d'évaluation en cours de formation :

- L'évaluation des acquis en cours de formation est réalisée sous forme QCM, mises en situation, réalisation de mission en conditions réelles, évaluations en cours et en fin de formation.

Prérequis à la validation de la certification :

- Les candidats doivent tous justifier de la moyenne à chaque module au sein des blocs de compétences pour être certifiés.

Modalités de l'examen final :

- Une validation partielle est possible par blocs de compétences.
- La validation du diplôme est soumise aux modalités d'examen suivantes : moyenne sur l'ensemble des blocs ainsi que sur le grand oral.

Passerelles et Équivalences :

- Pour connaitre les correspondances vers d'autres certifications, consultez le site internet de France Compétences.
- Certification professionnelle reconnue en correspondance partielle : consultez la fiche France Compétences : https://www.francecompetences.fr/recherche/rncp/41678

Poursuite d'études :

- Accès à des formations de niveau supérieur en cybersécurité, sécurité des systèmes d'information, gouvernance IT, gestion des risques numériques ou management des activités cyber.

Contenu de la formation :

BLOC	Compétences visées	Séquence ou thème de formation
BLOC 1 : Réaliser des tâches de programmation	C1.1 : Développer des scripts d'automatisation	- Bases de la programmation (syntaxe, structures de contrôle)
		- Scripts d'automatisation système sous Windows et Linux
		- Automatisation des tâches d'administration courante
		- Tests et documentation des scripts d'automatisation
	C1.2 : Identifier les potentielles vulnérabilités d'un système d'information	- Panorama des vulnérabilités (référentiels, typologies, CVE)
		- Outils de scan et d'analyse de vulnérabilités
		- Lecture et interprétation de rapports de vulnérabilités
		- Qualification et priorisation des risques identifiés
BLOC 2 : Configurer et administrer des systèmes et applications dans un environnement virtualisé	C2.1 : Gérer un parc informatique composé de systèmes d'exploitation propriétaires et libres	- Installation et configuration de postes clients Windows et Linux
		- Administration de base des comptes et services
		- Gestion des mises à jour et des correctifs de sécurité
		- Inventaire et supervision d'un parc informatique
	C2.2 : Déployer des applications au sein d'environnements virtualisés	- Concepts de virtualisation (hyperviseurs, VM, snapshots)
		- Déploiement d'applications dans des machines virtuelles
		- Gestion des ressources et des performances des VM
		- Sauvegarde et restauration d'environnements virtualisés
	C2.3 : Favoriser l'inclusion professionnelle d'une personne en situation de handicap	- Sensibilisation au handicap en contexte professionnel numérique
		- Identification des besoins d'aménagements raisonnables
		- Découverte des outils d'accessibilité et de compensation
		- Posture professionnelle et communication inclusive
BLOC 3 : Installer et gérer des bases de	C3.1 : Administrer des bases de données de type relationnel en s'appuyant sur la méthode MERISE	- Modélisation MERISE (MCD, MLD) appliquée à un cas d'entreprise
		- Langage SQL de base (création, modification, requêtes)
		- Gestion des comptes, des droits et des rôles
		- Sauvegarde et restauration d'une base de données
		- Analyse des besoins et des données métiers

données relationnelles	C3.2 : Concevoir une architecture de bases de données pour une application en proposant des solutions techniques	- Normalisation et intégrité référentielle
		- Choix des index et optimisation des performances
		- Documentation du schéma de données et des choix techniques
BLOC 4 : Configurer et administrer un réseau d'entreprise	C4.1 : Administrer un réseau d'entreprise en configurant un NAT et un DNS	- Rappels sur l'adressage IP et le subnetting
		- Configuration d'un NAT (PAT, SNAT, DNAT)
		- Mise en place d'un service DNS interne
		- Tests et dépannage du nommage et de la résolution DNS
	C4.2 : Déployer et gérer les réseaux à accès pour la connexion des terminaux et usagers	- Segmentation logique et réseaux d'accès (VLAN, ports)
		- Configuration des ports d'accès pour les postes utilisateurs
		- Gestion des accès filaires et distants
		- Supervision des connexions et gestion des incidents d'accès
	C4.3 : Gérer l'articulation des réseaux de transport en s'appuyant sur les notions d'acheminement, de commutation et de routage	- Principes d'acheminement, de commutation et de routage
		- Routage statique et dynamique : notions et mise en œuvre
		- Analyse des tables de routage et des chemins
		- Résolution des incidents de connectivité réseau
	C4.4 : Configurer les réseaux sans fil et mobilité	- Paramétrage d'un point d'accès WiFi
		- Sécurisation du WiFi (chiffrement, authentification)
		- Gestion de la mobilité et du roaming
		- Surveillance et diagnostic d'un réseau sans fil
	C4.5 : Configurer et administrer des réseaux virtualisés	- Concepts de réseaux virtualisés (vSwitch, VLAN, overlay)
		- Configuration de réseaux virtuels dans un hyperviseur
		- Routage et communication entre réseaux virtuels
		- Tests de connectivité dans un environnement virtualisé
BLOC 5 : Superviser et sécuriser les réseaux et les échanges	C5.1 : Superviser les réseaux informatiques d'une entreprise	- Mise en place d'outils de supervision réseau
		- Construction de tableaux de bord et choix des indicateurs
		- Détection, qualification et traitement des alertes
		- Reporting d'incidents et amélioration continue
	C5.2 : Sécuriser des réseaux et des échanges en utilisant les outils de gestion des identités et des accès	- Principes de gestion des identités et des accès (IAM)
		- Mise en place de politiques d'accès (RBAC, moindres privilèges)
		- Gestion des comptes, des habilitations et des revues de droits

		- Journalisation des accès et contrôles de conformité
BLOC 6 : Tester la sécurité d'un système informatique avec les méthodes de hacking	C6.1 : Attaquer un réseau sans fil afin de tester la sécurité d'un réseau sans fil	- Méthodologie d'audit et de test d'intrusion WiFi
		- Outils de capture et d'analyse de trames sans fil
		- Attaques courantes sur les protocoles WiFi en environnement contrôlé
		- Recommandations de sécurisation d'un réseau sans fil
	C6.2 : Cartographier les vulnérabilités d'un réseau d'entreprise	- Techniques de reconnaissance réseau (scan IP, ports, services)
		- Identification des services exposés et des versions
		- Construction d'une carte de vulnérabilités
		- Priorisation des cibles et des corrections à mener
	C6.3 : Utiliser les vulnérabilités d'un réseau d'entreprise dans le cadre de l'attaque d'une machine Windows	- Identification de vulnérabilités exploitables sur Windows
		- Mise en œuvre d'exploits en environnement de laboratoire
		- Escalade de privilèges locale sur une machine compromise
		- Maintien d'accès et bonnes pratiques de traçabilité en test
	C6.4 : Utiliser les vulnérabilités d'un réseau d'entreprise dans le cadre d'attaques avancées	- Chaînage de vulnérabilités pour étendre le périmètre d'attaque
		- Mouvements latéraux dans le système d'information
		- Techniques de persistance en environnement de test
		- Simulation d'attaque avancée (scénarios APT) en laboratoire
	C6.5 : Utiliser les vulnérabilités Web dans le cadre de la phase de reconnaissance de serveurs	- Collecte d'informations sur les applications Web
		- Détection des technologies et des versions en place
		- Identification des surfaces d'attaque Web
		- Élaboration d'une fiche cible pour une application Web
	C6.6 : Utiliser les vulnérabilités Web dans le cadre d'attaques sur authentification	- Analyse des mécanismes d'authentification Web
		- Mises en situation d'attaques sur l'authentification en labo
		- Exploitation des faiblesses de gestion de session
		- Mesures de renforcement des mécanismes d'authentification
	C6.7 : Utiliser les vulnérabilités Web dans le cadre d'attaques sur CMS	- Analyse de la surface d'attaque d'un CMS
		- Identification de plugins, thèmes et modules vulnérables
		- Exploitation de vulnérabilités connues en environnement de test
		- Bonnes pratiques de sécurisation et de durcissement d'un CMS