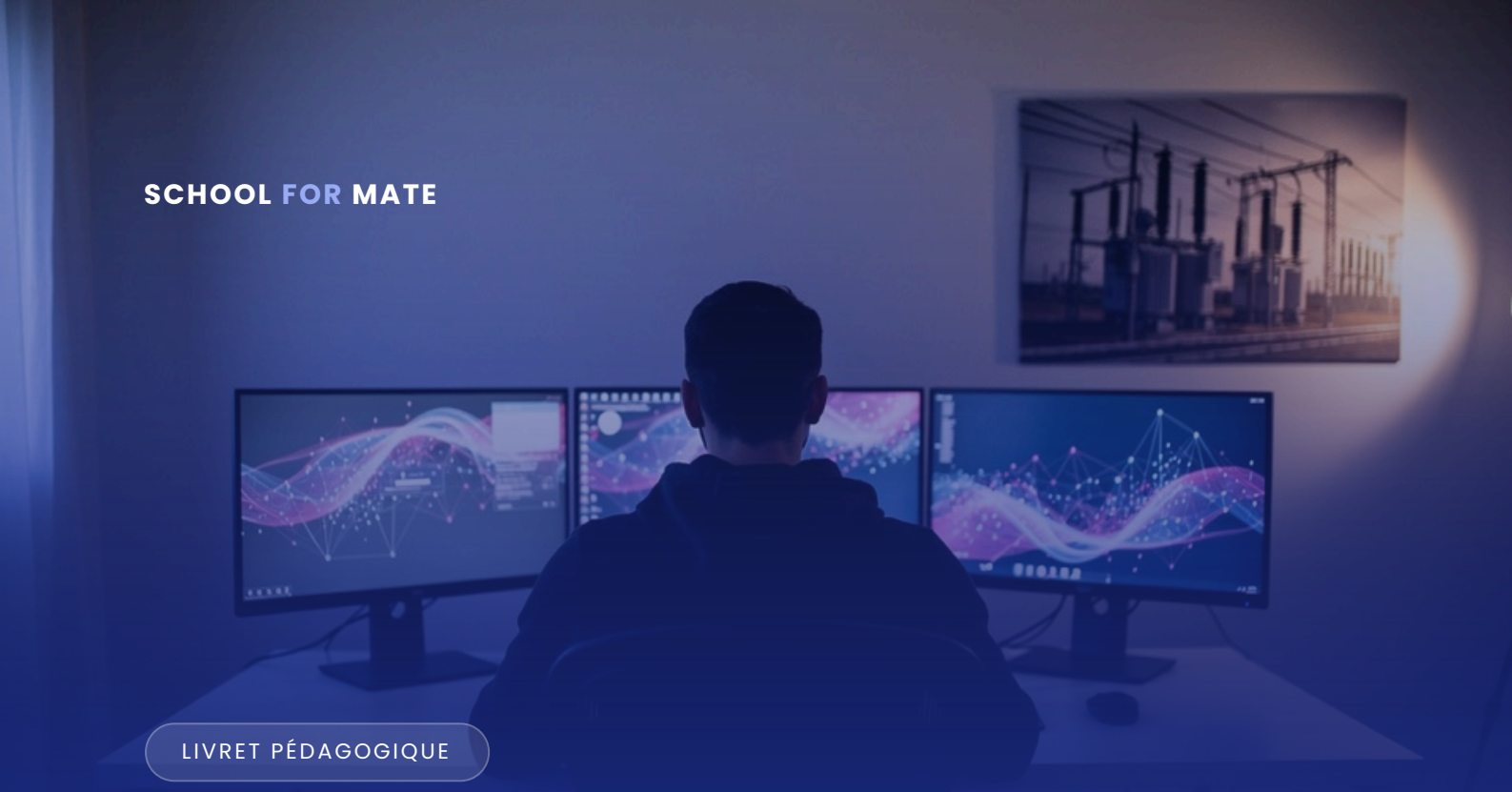
SCHOOL FOR MATE



LIVRET PÉDAGOGIQUE

Opérateur en cybersécurité

RNCP41678 · Certification RNCP · Niveau 5

Ce parcours de 440 heures prépare au titre RNCP41678 Opérateur en cybersécurité (niveau 5) et couvre l'intégralité des six blocs de compétences du référentiel France Compétences, de la programmation défensive à la supervision d'un SOC. Il est livré en marque blanche, clé en main, pour permettre à votre organisme de former des opérateurs capables de prévenir, détecter et corriger les menaces pesant sur un système d'information.

VOLUME HORAIRE	COURS	BLOCS
440 h	20	6

01 · PRÉSENTATION

La formation en bref

Intitulé	Opérateur en cybersécurité
Code	RNCP41678
Type	Certification RNCP
Niveau	Niveau 5
Certificateur	ECOLE EUROPEENNE D INTELLIGENCE ECONOMIQUE
Durée	440 h, 20 cours
Modalité	Formation à distance (e-learning), tutorat assuré par l'organisme de formation
Formats	SCORM 1.2 / 2004, xAPI, sources éditables
Mise à jour	Novembre 2026
Fin d'enregistrement de la certification	27/11/2028

Le métier et les compétences visées

L'opérateur en cybersécurité protège les données et la fiabilité du système d'information d'une entreprise ou d'une administration selon trois axes : prévention, détection et correction. Il réalise un diagnostic du système d'information pour déceler les points faibles, propose et déploie des solutions de protection, met en place les processus de sécurité et en garantit la pérennité en les actualisant face aux nouvelles menaces et aux évolutions technologiques. Il administre les systèmes, les réseaux, les bases de données et les applications, supervise les journaux d'événements, qualifie les alertes et rétablit le système dans les meilleures conditions après un incident. Il intervient en SOC, au sein d'une DSI, chez un prestataire de services ou dans une infrastructure critique.

Public visé

- Titulaires d'un diplôme ou titre de niveau 4 souhaitant se spécialiser en cybersécurité
- Techniciens et administrateurs systèmes et réseaux en poste, en évolution vers la cyberdéfense
- Personnes en reconversion justifiant d'une expérience significative et de compétences informatiques
- Salariés de DSI ou de services de sécurité informatique souhaitant valider leurs compétences par un titre RNCP
- Alternants et apprenants de CFA et d'organismes de formation partenaires

Prérequis

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

Objectifs pédagogiques

À l'issue du parcours, l'apprenant est capable de :

- Développer des scripts d'automatisation en Python, Bash et C pour automatiser des tâches répétitives
- Identifier les vulnérabilités et les mauvaises pratiques dans des programmes existants afin de prévenir les bugs et les failles
- Gérer un parc informatique Microsoft et Linux, appliquer les correctifs et vérifier le respect des standards de sécurité
- Déployer des applications dans des environnements virtualisés et conteneurisés en limitant les risques de sécurité
- Aménager un poste et un environnement de travail accessibles pour favoriser l'inclusion professionnelle d'une personne en situation de handicap
- Concevoir, administrer et sécuriser des bases de données relationnelles pour une application
- Installer, configurer et administrer un réseau d'entreprise filaire, sans fil et virtualisé
- Superviser les réseaux et les systèmes, analyser les journaux et qualifier la criticité des menaces
- Mettre en œuvre une politique de chiffrement, de gestion des identités et de contrôle d'accès aux données
- Conduire, dans un cadre autorisé, des tests de sécurité d'un système d'information, cartographier les vulnérabilités et proposer des remédiations

02 · FIL ROUGE PÉDAGOGIQUE

Castelane Énergie Services

IM

Inès Marchetti

Technicienne informatique devenue opératrice en cybersécurité au sein du centre de supervision de sécurité (SOC) de l'entreprise

Distribution régionale d'électricité et d'eau (infrastructure critique, entreprise fictive)

Castelane Énergie Services est une entreprise fictive de distribution d'électricité et d'eau, répartie sur plusieurs sites et agences. Son système d'information relie des postes bureautiques, des serveurs, des bases de données clients, un portail web de facturation et des équipements de supervision des installations. Compte tenu de son activité, l'entreprise est soumise à des obligations renforcées de protection de ses systèmes d'information. Inès Marchetti, technicienne informatique, est choisie pour rejoindre le tout nouveau SOC interne. Sa mission est de monter en compétence pour automatiser les contrôles, administrer le parc, fiabiliser les bases de données, sécuriser les réseaux, superviser les alertes et vérifier, dans un cadre autorisé, la solidité des défenses. Chaque cours de ce parcours lui confie une mission concrète.

Chaque cours se termine par une mise en situation dans cette entreprise : l'apprenant accompagne Inès dans des situations professionnelles réalistes, de plus en plus complexes, jusqu'à la préparation des épreuves.

La progression

1. Bloc 1 : Inès automatise les contrôles quotidiens du service informatique et apprend à relire des scripts existants pour y repérer les mauvaises pratiques.
2. Bloc 2 : Elle prend en charge le parc de postes et de serveurs Windows et Linux, déploie les applications métier dans un environnement virtualisé et équipe un collègue en situation de handicap.
3. Bloc 3 : Elle fiabilise la base de données clients de l'entreprise, puis conçoit celle d'une nouvelle application de suivi des interventions.
4. Bloc 4 : Elle installe et administre le réseau d'une nouvelle agence, depuis l'adressage jusqu'aux liaisons VPN, aux réseaux sans fil et aux réseaux virtualisés.
5. Bloc 5 : Elle met en place la supervision du SOC, qualifie les alertes, traite un incident et déploie la politique d'accès et de chiffrement.
6. Bloc 6 : Dans un cadre contractuel strict et sur un environnement de test, elle évalue les défenses de l'entreprise, cartographie les vulnérabilités et rédige le plan de remédiation présenté à la direction.

03 · ARCHITECTURE

Organisation du parcours

Le parcours est construit sur les blocs de compétences du référentiel officiel : chaque bloc regroupe les cours qui préparent à son évaluation.

N°	Bloc et cours	Durée
RNCP41678BC01 · Réaliser des tâches de programmation		**44 h**
1	Automatiser les tâches répétitives avec Python, Bash et C	22 h
2	Analyser des programmes pour identifier vulnérabilités et mauvaises pratiques	22 h
RNCP41678BC02 · Configurer et administrer des systèmers et applications dans un environnement virtualisé		**66 h**
3	Gérer un parc informatique Microsoft et Linux	22 h
4	Déployer des applications en environnement virtualisé et conteneurisé	22 h
5	Favoriser l'inclusion professionnelle : équipements, logiciels et postes accessibles	22 h
RNCP41678BC03 · Installer et gérer des bases de données relationnelles		**44 h**
6	Modéliser, interroger et administrer une base de données relationnelle sécurisée	22 h
7	Concevoir l'architecture de bases de données d'une application en mode projet	22 h
RNCP41678BC04 · Configurer et administrer un réseau d'entreprise		**110 h**
8	Administrer un réseau d'entreprise : adressage, protocoles et services	22 h
9	Déployer les réseaux d'accès et segmenter avec les VLAN en mode projet	22 h
10	Interconnecter les réseaux : acheminement, commutation, routage et VPN	22 h
11	Configurer des réseaux sans fil et de mobilité sécurisés	22 h
12	Configurer et administrer des réseaux virtualisés	22 h
RNCP41678BC05 · Superviser et sécuriser les réseaux et les échanges		**66 h**
13	Superviser les infrastructures et exploiter les journaux d'événements	22 h
14	Détecter, qualifier et traiter les menaces et les incidents	22 h
15	Sécuriser les accès et les échanges : identités, durcissement, cryptographie et filtrage	22 h
RNCP41678BC06 · Tester la sécurité d'un système informatique avec les méthodes de hacking		**110 h**
16	Cadre, méthodologie et cartographie des vulnérabilités d'un réseau d'entreprise	22 h
17	Évaluer la sécurité d'un réseau sans fil et proposer des remédiations	22 h
18	Évaluer la sécurité des postes Windows et du réseau filaire	22 h
19	Sécuriser les serveurs et applications web : reconnaissance, authentification et référentiel OWASP	22 h

20	Protéger les CMS et les données, et s'appuyer sur les référentiels ISO 27000, NIST 800-53 et RGPD	22 h
Total du parcours		**440 h**

Répartition des modalités pédagogiques

Chaque sous-chapitre s'ouvre sur une vidéo de 3 à 5 minutes. La vidéo représente 30 % du volume horaire, complétée par du cours texte enrichi, des infographies, des études de cas, des mises en situation et des QCM.



- Vidéos : 132 h
- Cours texte et infographies : 138 h 30
- Études de cas et mises en situation : 108 h
- QCM et évaluations : 61 h 30

04 · PROGRAMME DÉTAILLÉ

Contenu des cours

RNCP41678BC01 · 44 h

Réaliser des tâches de programmation

Cours 1 · Automatiser les tâches répétitives avec Python, Bash et C

22 h

OBJECTIFS

- Choisir le langage adapté à une tâche d'automatisation dans un contexte de sécurité
- Développer des scripts fiables, documentés et réutilisables pour des contrôles récurrents

ÉVALUATION FORMATIVE

QCM de positionnement par langage et exercice guidé d'automatisation d'une tâche à partir d'un énoncé métier

CONTENUS

- Panorama des langages utilisés en cybersécurité et critères de choix
- Principes de l'automatisation : repérer et formaliser une tâche répétitive
- Structure d'un script lisible, maintenable et commenté
- Scripts d'administration et de contrôle avec Bash
- Scripts d'exploitation de données et de fichiers avec Python
- Place du langage C dans les environnements système et sécurité
- Gestion des erreurs, des droits d'exécution et des secrets dans un script
- Planification, journalisation et suivi des automatisations

Fil rouge · Inès Marchetti constate que le service informatique de Castelane Énergie Services consacre chaque matin du temps à des vérifications manuelles. Elle identifie cinq tâches répétitives et conçoit leur automatisation avec l'accord de sa responsable.

Cours 2 · Analyser des programmes pour identifier vulnérabilités et mauvaises pratiques

22 h

OBJECTIFS

- Relire un script ou un programme Python, Bash ou C et repérer les défauts de conception et de sécurité
- Utiliser un outil d'aide à l'analyse avec esprit critique et rédiger des recommandations de correction

ÉVALUATION FORMATIVE

Étude de cas : analyse de scripts préexistants, relevé argumenté des vulnérabilités et QCM de synthèse

CONTENUS

- Familles de vulnérabilités et de mauvaises pratiques de programmation
- Méthode de revue de code orientée sécurité
- Lecture de scripts contenant des actions nuisibles et identification de leur finalité
- Gestion des entrées, des droits et des données sensibles dans le code
- Usage d'un outil d'IA comme assistant d'analyse et vérification humaine de ses résultats
- Qualification et priorisation des défauts relevés
- Rédaction d'un compte rendu d'analyse et de recommandations

Fil rouge · Un prestataire livre à Castelane Énergie Services trois scripts d'exploitation. Inès les analyse avant toute mise en production, signale les défauts et les comportements suspects, puis propose des corrections à son équipe.

RNCP41678BC02 · 66 h

Configurer et administrer des systèmers et applications dans un environnement virtualisé

Cours 3 · Gérer un parc informatique Microsoft et Linux

22 h

OBJECTIFS

- Spécifier et choisir les composants matériels et systèmes en fonction des besoins de l'entreprise
- Assurer l'installation, la maintenance et la mise à jour de systèmes Microsoft et Linux conformément aux standards de sécurité

ÉVALUATION FORMATIVE

Rédaction guidée d'un cahier des charges d'équipement et QCM sur la gestion des correctifs

CONTENUS

- Composants physiques d'un poste et d'un serveur
- Rédaction d'un cahier des charges d'équipement
- Systèmes d'exploitation propriétaires et libres : critères de choix
- Installation et maintenance d'un système Microsoft
- Installation et maintenance d'un système Linux
- Veille sur les vulnérabilités publiées par les organismes de détection et de prévention
- Gestion et suivi des correctifs
- Contrôle de l'application des standards de sécurité
- Risques liés à une gestion défaillante des serveurs

Fil rouge · Castelane Énergie Services ouvre une agence. Inès rédige le cahier des charges des postes et des serveurs, puis organise le suivi des correctifs pour l'ensemble du parc Windows et Linux.

Cours 4 · Déployer des applications en environnement virtualisé et conteneurisé

22 h

OBJECTIFS

- Installer et configurer un serveur virtualisé en appliquant les règles qui limitent les risques liés à la virtualisation
- Empaqueter et déployer des applications avec une technologie de conteneurisation et sécuriser l'accès au serveur

ÉVALUATION FORMATIVE

Étude de cas de déploiement à partir d'une expression de besoin et QCM sur les risques de la virtualisation

CONTENUS

- Principes de la virtualisation et hyperviseurs (VMware, Hyper-V, Xen)
- Installation et configuration d'un serveur virtualisé
- Risques de sécurité propres à la virtualisation
- Règles de durcissement d'un environnement virtualisé
- Conteneurisation avec Docker : applications et dépendances
- Procédures d'installation et de configuration d'une application
- Sécurisation de l'accès au serveur virtualisé selon la politique de sécurité
- Optimisation des ressources et scalabilité des applications

Fil rouge · Le portail web de facturation de Castelane Énergie Services doit absorber les pics de consultation. Inès le déploie sur un serveur virtualisé, en conteneurs, selon l'expression de besoin du client interne.

Cours 5 · Favoriser l'inclusion professionnelle : équipements, logiciels et postes accessibles

22 h

OBJECTIFS

- Proposer par défaut des équipements et logiciels utilisables par tous, quel que soit le handicap
- Identifier, régler et paramétrer des adaptations matérielles et logicielles pour un poste donné

ÉVALUATION FORMATIVE

Étude de cas : choix d'équipements et de paramétrages adaptés à trois situations, suivi d'un QCM

CONTENUS

- Cadre de l'inclusion professionnelle et de l'aménagement de poste
- Typologie des situations de handicap et besoins associés
- Conception inclusive : accessibilité native des équipements et des logiciels
- Équipements adaptés : périphériques, affichage, audio
- Paramétrages d'accessibilité des systèmes et des logiciels
- Sécurité et accessibilité : concilier les deux exigences
- Dialogue avec le collaborateur, le manager et les acteurs de l'accompagnement
- Suivi et ajustement d'un aménagement dans le temps

Fil rouge · Un nouveau collègue en situation de handicap rejoint le service client de Castelane Énergie Services. Inès sélectionne et paramètre avec lui les équipements et les logiciels de son poste, sans affaiblir les règles de sécurité.

RNCP41678BC03 · 44 h

Installer et gérer des bases de données relationnelles

Cours 6 · Modéliser, interroger et administrer une base de données relationnelle sécurisée

22 h

OBJECTIFS

- Modéliser des données avec la méthode MERISE et interroger une base en SQL
- Administrer un SGBDR (Oracle, MySQL, PostgreSQL) et appliquer les règles de sécurité d'une base relationnelle

ÉVALUATION FORMATIVE

Exercices de modélisation et de requêtes, puis QCM sur la sécurité d'une base relationnelle

CONTENUS

- Principes du modèle relationnel et méthode MERISE
- Du modèle conceptuel au modèle logique de données
- Requêtes SQL d'interrogation et de mise à jour
- Panorama des SGBDR : Oracle, MySQL, PostgreSQL
- Installation et outils de gestion d'un SGBDR
- Gestion des utilisateurs, des rôles et des privilèges
- Règles de sécurité d'une base relationnelle
- Sauvegarde, restauration et maintien en condition opérationnelle

Fil rouge · La base des contrats clients de Castelane Énergie Services est lente et mal protégée. Inès installe un SGBDR de test, revoit les droits d'accès et applique les règles de sécurité attendues.

Cours 7 · Concevoir l'architecture de bases de données d'une application en mode projet

22 h

OBJECTIFS

- Proposer des solutions techniques de bases de données adaptées au besoin d'une application, en mode projet
- Préparer la création des tables et vérifier le bon fonctionnement de la base avant la mise en place sécurisée de l'application

ÉVALUATION FORMATIVE

Création d'un schéma de base de données relationnelle à partir d'un cahier des charges et revue par les pairs

CONTENUS

- Analyse du besoin applicatif et cadrage du projet
- Choix d'une solution technique de base de données
- Conception du schéma et des relations entre tables
- Préparation de la création des tables
- Intégrité, contraintes et qualité des données
- Prise en compte de la sécurité dès la conception
- Tests de fonctionnalité et de bon fonctionnement de la base
- Documentation et transmission aux équipes de développement

Fil rouge · Castelane Énergie Services lance une application de suivi des interventions techniques. Inès conçoit le schéma de la base, le valide avec les développeurs et vérifie son bon fonctionnement avant l'ouverture de l'application.

RNCP41678BC04 · 110 h

Configurer et administrer un réseau d'entreprise

Cours 8 · Administrer un réseau d'entreprise : adressage, protocoles et services

22 h

OBJECTIFS

- Configurer les services d'adressage, de traduction d'adresses et de résolution de noms d'un réseau d'entreprise
- Détecter des erreurs réseau par l'analyse du trafic et la connaissance des protocoles

ÉVALUATION FORMATIVE

Exercices de calcul d'adressage, étude de cas de dépannage et QCM sur les protocoles

CONTENUS

- Architecture et organisation d'un réseau d'entreprise
- Adressage IPv4 et IPv6 et gestion des adresses privées
- Configuration d'un NAT et d'un DNS
- Rôle des protocoles ICMP, TCP et UDP
- Analyse du trafic pour détecter les erreurs réseau
- Applications d'entreprise : messagerie, visioconférence, diffusion de contenus
- Paramétrage des applications à déployer
- Documentation d'un réseau

Fil rouge · À l'agence nouvellement ouverte de Castelane Énergie Services, plusieurs services sont injoignables. Inès analyse le trafic, corrige l'adressage et la résolution de noms, puis paramètre la messagerie et la visioconférence.

Cours 9 · Déployer les réseaux d'accès et segmenter avec les VLAN en mode projet

22 h

OBJECTIFS

- Installer un réseau d'accès pour la connexion des terminaux et des usagers en mode projet
- Paramétrer des VLAN respectant la structure organisationnelle de l'entreprise

ÉVALUATION FORMATIVE

Mini-projet de conception et de paramétrage de VLAN dans un simulateur réseau

CONTENUS

- Conduite d'un projet d'installation de réseau
- Réseaux d'accès domestiques et d'entreprise : Wi-Fi et CPL
- Mécanisme de la boucle locale d'entreprise
- Raccordement des terminaux et des usagers
- Principe et intérêt de la segmentation par VLAN
- Conception des VLAN selon l'organisation de l'entreprise
- Paramétrage des VLAN
- Recette et documentation de l'installation

Fil rouge · Inès pilote l'installation du réseau d'accès de la nouvelle agence de Castelane Énergie Services. Elle sépare les flux de l'accueil, du service technique et de la comptabilité par des VLAN.

Cours 10 · Interconnecter les réseaux : acheminement, commutation, routage et VPN

22 h

OBJECTIFS

- Paramétrer un réseau à partir des notions d'acheminement, de commutation et de routage
- Mettre en place des VPN pour interconnecter plusieurs réseaux et vérifier le bon fonctionnement du réseau local

ÉVALUATION FORMATIVE

Mise en situation dans un simulateur réseau : interconnexion de réseaux locaux et dépannage de dysfonctionnements

CONTENUS

- Notions d'acheminement, de commutation et de routage
- Paramétrage d'un réseau routé
- Vérification du bon fonctionnement depuis un point de contrôle
- Diagnostic des dysfonctionnements d'un réseau local préexistant
- Principe des VPN et cas d'usage entre sites
- Solutions de mise en place d'un VPN
- Authentification centralisée des accès réseau
- Documentation et recette de l'interconnexion

Fil rouge · Les agences de Castelane Énergie Services doivent échanger de façon sécurisée avec le siège. Inès conçoit l'interconnexion, met en place un VPN et vérifie le bon fonctionnement du réseau à partir d'un point de contrôle.

Cours 11 · Configurer des réseaux sans fil et de mobilité sécurisés

22 h

OBJECTIFS

- Choisir le type de réseau sans fil adapté à un besoin de connectivité en s'appuyant sur les typologies et les normes
- Configurer un réseau Wi-Fi sécurisé et réaliser une veille sur les évolutions des technologies sans fil

ÉVALUATION FORMATIVE

Étude de documents et préconisation d'un réseau sans fil sécurisé, suivie d'un QCM sur les normes

CONTENUS

- Typologies de réseaux sans fil : WPAN, WLAN, WMAN, WRAN, hot spot, hand over, roaming
- Technologies courte portée : IEEE 802.15, Bluetooth, ZigBee, UWB
- Principes de la norme IEEE 802.11 et de ses évolutions
- Normes IEEE 802.22 et réseaux régionaux sans fil
- Réseaux mobiles et technologies cellulaires
- Internet ambiant : réseaux mesh, ad hoc, capteurs, RFID, NFC
- Configuration sécurisée d'un réseau Wi-Fi d'entreprise
- Veille technologique sur les nouvelles générations de Wi-Fi

Fil rouge · Castelane Énergie Services souhaite couvrir son entrepôt et son accueil en Wi-Fi. Inès compare les technologies, retient une solution adaptée et la configure avec un chiffrement et une authentification conformes à la politique de sécurité.

Cours 12 · Configurer et administrer des réseaux virtualisés

22 h

OBJECTIFS

- Virtualiser des serveurs et mesurer l'impact de la virtualisation sur l'infrastructure réseau
- Configurer des réseaux locaux virtuels et des commutations de niveaux 3, 4 et 7 dans un environnement simulé

ÉVALUATION FORMATIVE

Mise en situation dans un simulateur : réseau local interconnecté incluant VPN, authentification et Wi-Fi sécurisé

CONTENUS

- Virtualisation des serveurs et impact sur l'infrastructure
- Centralisation du plan de contrôle et rôle d'un contrôleur
- Simulation de réseaux avec GNS3
- Normalisation IEEE 802 et ISO : couches physique, MAC et LLC
- Technique d'accès ISO 8802.3 (CSMA/CD) et principaux protocoles
- Réseaux locaux Ethernet : SAN, LAN, WLAN
- Configuration des VLAN, des ponts et de la commutation de niveaux 3, 4 et 7
- Mise en place d'un réseau interconnecté hétérogène et sécurisé

Fil rouge · Castelane Énergie Services veut tester une nouvelle architecture réseau avant son déploiement. Inès la modélise dans un environnement simulé, y inclut un VPN, un serveur d'authentification et un Wi-Fi sécurisé, puis formule ses préconisations.

Superviser et sécuriser les réseaux et les échanges

Cours 13 · Superviser les infrastructures et exploiter les journaux d'événements

22 h

OBJECTIFS

- Déployer une supervision reposant sur des serveurs et des agents pour les réseaux, systèmes et bases de données
- Collecter, analyser et visualiser les journaux d'événements avec les outils appropriés

ÉVALUATION FORMATIVE

Mise en situation : configuration d'une supervision et lecture guidée de tableaux de bord, suivies d'un QCM

CONTENUS

- Objectifs et architecture d'un système de supervision
- Déploiement d'une infrastructure de supervision et de sa sécurisation
- Outils de manipulation de fichiers de journaux
- Analyse et corrélation des journaux d'événements
- Paramétrage des outils d'analyse et de visualisation
- Outils d'administration et de détection : SIEM, IDS/IPS, pare-feu
- Supervision des équipements actifs, systèmes et bases de données
- Apport de l'IA à la supervision et limites d'usage

Fil rouge · Inès met en place la supervision du SOC de Castelane Énergie Services. Elle déploie des agents sur les serveurs, centralise les journaux et construit des tableaux de bord pour son équipe.

Cours 14 · Détecter, qualifier et traiter les menaces et les incidents

22 h

OBJECTIFS

- Détecter des anomalies et des compromissions à partir de l'analyse de journaux, avec ou sans assistance d'un outil d'IA
- Évaluer le niveau de criticité d'une menace, isoler les systèmes concernés et proposer des remédiations

ÉVALUATION FORMATIVE

Étude de cas : analyse de journaux, détection de compromissions et proposition de remédiations

CONTENUS

- Comportements anormaux et indicateurs de compromission
- Analyse de journaux pour détecter une compromission du système d'information
- Qualification d'une menace et grille de criticité
- Isolement des menaces et mesures de confinement
- Utilisation encadrée d'un modèle de langage et de son interface de programmation pour l'aide à l'analyse
- Remédiation et rétablissement du système d'information
- Obligations de déclaration d'incident pour les opérateurs d'importance vitale
- Rédaction d'un rapport d'incident

Fil rouge · Une série d'alertes inhabituelles apparaît sur un serveur de Castelane Énergie Services. Inès analyse les journaux, classe la menace par niveau de criticité, isole le serveur et rédige les recommandations de remédiation.

Cours 15 · Sécuriser les accès et les échanges : identités, durcissement, cryptographie et filtrage — 22 h

OBJECTIFS

- Mettre en œuvre la gestion des identités et des accès et le durcissement de postes Linux et Windows
- Appliquer les principes de la cryptographie et des règles de filtrage pour protéger les échanges et l'accès aux données

ÉVALUATION FORMATIVE

Mise en situation : règles d'identités et d'accès selon un cahier des charges et chiffrement asymétrique d'un échange

CONTENUS

- Principes de la gestion des identités et des accès
- Rédaction de règles d'accès selon un cahier des charges
- Étapes de durcissement d'un poste Linux
- Étapes de durcissement d'un poste Windows
- Principes de la cryptographie symétrique et asymétrique
- Chiffrement d'une communication entre deux utilisateurs
- Règles de filtrage selon le système d'exploitation
- Politique de chiffrement et de sécurité d'accès aux données

Fil rouge · Castelane Énergie Services doit protéger les échanges entre ses agences et ses équipes d'intervention. Inès met en place les règles d'accès, durcit les postes concernés et fait chiffrer les communications sensibles.

RNCP41678BC06 · 110 h

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

Cours 16 · Cadre, méthodologie et cartographie des vulnérabilités d'un réseau d'entreprise — 22 h

OBJECTIFS

- Situer un test d'intrusion dans son cadre juridique, contractuel et déontologique
- Appliquer la méthodologie d'un audit de sécurité pour cartographier les vulnérabilités d'un réseau et hiérarchiser les risques

ÉVALUATION FORMATIVE

Étude de cas : cartographie des vulnérabilités d'un réseau fictif avec proposition de remédiations

CONTENUS

- Cadre légal, autorisation écrite et périmètre d'un test d'intrusion
- Rôles des équipes rouge, bleue et violette
- Méthodologie d'un test d'intrusion et recherche de la surface d'attaque
- Découverte et inventaire des actifs d'un réseau d'entreprise
- Outils d'analyse de vulnérabilités et de trafic, utilisés en environnement contrôlé
- Échelle de gravité fondée sur la confidentialité, l'intégrité et la disponibilité
- Cartographie des vulnérabilités et priorisation des remédiations
- Restitution et traçabilité des résultats

Fil rouge · La direction de Castelane Énergie Services mandate Inès, par une lettre de mission précisant le périmètre, pour auditer son réseau de test. Elle recense les vulnérabilités et les classe par gravité.

Cours 17 · Évaluer la sécurité d'un réseau sans fil et proposer des remédiations

22 h

OBJECTIFS

- Évaluer, sur un réseau Wi-Fi de laboratoire, la robustesse des mécanismes d'authentification et de chiffrement
- Qualifier la gravité des faiblesses constatées et proposer des mesures de durcissement

ÉVALUATION FORMATIVE

Mise en situation en laboratoire : évaluation d'un Wi-Fi vulnérable et rédaction des remédiations

CONTENUS

- Menaces courantes sur les réseaux sans fil et risques associés
- Mécanismes d'authentification et de chiffrement d'un WLAN et leurs limites
- Mise en place d'un réseau Wi-Fi volontairement vulnérable en laboratoire
- Évaluation de la résistance aux interruptions de service, aux points d'accès pirates et à l'interception
- Scénarios d'attaque avancée étudiés en environnement fictif
- Gravité des faiblesses selon la confidentialité, l'intégrité et la disponibilité
- Remédiations et bonnes pratiques de durcissement d'un WLAN
- Rapport de test d'un réseau sans fil

Fil rouge · Avant de généraliser le Wi-Fi à toutes les agences de Castelane Énergie Services, Inès teste un réseau de laboratoire volontairement fragilisé, documente les faiblesses et propose des corrections.

Cours 18 · Évaluer la sécurité des postes Windows et du réseau filaire

22 h

OBJECTIFS

- Mesurer, dans un laboratoire autorisé, l'exposition d'un poste Windows et du réseau filaire aux vecteurs d'attaque courants
- Définir les mesures de protection : gestion des correctifs, sensibilisation des utilisateurs et durcissement des postes

ÉVALUATION FORMATIVE

Mise en situation : test d'un réseau filaire vulnérable de laboratoire et proposition de remédiations

CONTENUS

- Chaîne d'une intrusion sur un réseau filaire, vue côté défense
- Services et équipements exposés sur un réseau filaire
- Mise en place d'un réseau filaire vulnérable en laboratoire
- Exposition d'un poste Windows : pare-feu, antivirus et navigateurs
- Limites des solutions antivirus et complémentarité des protections
- Ingénierie sociale : risques et sensibilisation des utilisateurs
- Gestion des correctifs et des mises à jour
- Remédiations proposées après un test sur un réseau filaire

Fil rouge · Inès réalise, sur une copie isolée du réseau de bureau de Castelane Énergie Services, un test autorisé de l'exposition des postes. Elle en déduit un plan de correctifs et une action de sensibilisation.

Cours 19 · Sécuriser les serveurs et applications web : reconnaissance, authentification et référentiel OWASP

22 h

OBJECTIFS

- Utiliser le référentiel OWASP et les outils d'analyse pour repérer les failles d'un serveur ou d'une application web, puis les corriger
- Vérifier le respect des politiques de gestion des accès et l'efficacité des protections d'authentification

ÉVALUATION FORMATIVE

Étude de cas : analyse d'un serveur web de test, relevé des failles et plan de correction

CONTENUS

- Panorama du référentiel OWASP et des principales familles de failles web
- Reconnaissance d'un serveur web et inventaire de ses expositions
- Outils d'analyse de vulnérabilités et de proxy d'inspection en environnement contrôlé
- Failles liées aux entrées utilisateur, aux fichiers et aux formulaires
- Failles liées aux sessions, aux requêtes et à l'affichage des pages
- Robustesse des mécanismes d'authentification et des protocoles sécurisés
- Politiques et procédures de gestion des accès
- Corrections et développement sécurisé

Fil rouge · Le portail de facturation de Castelane Énergie Services est audité sur son environnement de recette. Inès relève les failles, les classe selon l'OWASP et propose des correctifs aux développeurs.

Cours 20 · Protéger les CMS et les données, et s'appuyer sur les référentiels ISO 27000, NIST 800-53 et RGPD

22 h

OBJECTIFS

- Évaluer l'exposition des principaux CMS (WordPress, Joomla, Drupal) et définir les mesures de protection contre la fuite de données
- Situer ses actions dans les référentiels de sécurisation d'un système d'information et formuler un plan d'amélioration de la résilience

ÉVALUATION FORMATIVE

Étude de cas finale : cartographie consolidée, plan de remédiation et mise en regard des référentiels ISO 27000, NIST 800-53 et RGPD

CONTENUS

- Spécificités de sécurité des principaux CMS
- Évaluation de l'exposition d'un site CMS en environnement de test
- Fuite de données personnelles ou sensibles : causes et prévention
- Cartographie consolidée des vulnérabilités et plan de remédiation
- Famille de normes ISO 27000 et SMSI
- Mesures de sécurité du NIST 800-53
- Règlement général sur la protection des données (RGPD)
- Cadre réglementaire des opérateurs d'importance vitale et rôle du SOC
- Restitution à la direction : améliorer la résilience du système d'information

Fil rouge · Le site d'information clients de Castelane Énergie Services repose sur un CMS. Inès évalue son exposition, consolide la cartographie des vulnérabilités de toute sa mission et présente son plan de remédiation à la direction.

05 · CONFORMITÉ AU RÉFÉRENTIEL

Couverture des compétences

Correspondance entre les compétences du référentiel France Compétences et les cours du parcours.

Compétence	Bloc	Cours
Développer des scripts d'automatisation (Python, Bash, C)	RNCP41678BC01	1
Identifier les vulnérabilités d'un système d'information par l'analyse de programmes	RNCP41678BC01	2
Gérer un parc informatique de systèmes propriétaires et libres	RNCP41678BC02	3
Déployer des applications en environnements virtualisés	RNCP41678BC02	4
Favoriser l'inclusion professionnelle d'une personne en situation de handicap	RNCP41678BC02	5
Administrer des bases de données de type relationnel	RNCP41678BC03	6
Concevoir une architecture de bases de données pour une application	RNCP41678BC03	6, 7
Administrer un réseau d'entreprise	RNCP41678BC04	8
Déployer et gérer les réseaux à accès pour la connexion des terminaux et usagers	RNCP41678BC04	9
Gérer l'articulation des réseaux de transport	RNCP41678BC04	10
Configurer les réseaux sans fil et mobilité	RNCP41678BC04	11
Configurer et administrer des réseaux virtualisés	RNCP41678BC04	12
Superviser les réseaux, infrastructures, systèmes et bases de données	RNCP41678BC05	13, 14
Sécuriser des réseaux et des échanges (politique de chiffrement et d'accès)	RNCP41678BC05	15
Attaquer un réseau sans fil pour tester sa sécurité	RNCP41678BC06	17
Cartographier les vulnérabilités d'un réseau d'entreprise	RNCP41678BC06	16
Utiliser les vulnérabilités d'un réseau d'entreprise : attaque d'une machine Windows	RNCP41678BC06	18
Utiliser les vulnérabilités d'un réseau d'entreprise : attaques avancées	RNCP41678BC06	18, 19
Utiliser les vulnérabilités Web : reconnaissance de serveurs	RNCP41678BC06	19
Utiliser les vulnérabilités Web : attaques sur authentification	RNCP41678BC06	19
Utiliser les vulnérabilités Web : attaques sur CMS	RNCP41678BC06	20

Évaluations formatives

Chaque cours s'achève par une évaluation formative adaptée à son contenu : QCM de synthèse sur les notions clés, exercices guidés, études de cas ou mini-projets dans les simulateurs et laboratoires virtualisés. Chaque mise en situation du fil rouge Castelane Énergie Services permet à l'apprenant de mobiliser immédiatement la compétence visée. Les résultats alimentent un suivi de progression par bloc de compétences, exploitable par le formateur référent de l'organisme de formation pour tracer les acquis, conformément aux exigences de suivi du référentiel Qualiopi.

Modalités de certification

Bloc	Modalité d'évaluation
RNCP41678BC01	Mise en situation professionnelle : automatisation de 5 tâches répétitives, lecture de trois scripts contenant des vulnérabilités et des actions visant à nuire aux cibles, étude de documents suivie de l'automatisation d'une tâche, analyse de scripts préexistants et recherche de vulnérabilités.
RNCP41678BC02	Mise en situation professionnelle : rédaction d'un cahier des charges d'équipement informatique, mise en place d'un serveur selon les contraintes d'un client fictif, déploiement d'applications en environnement virtualisé pour répondre à une expression de besoin, identification d'équipements adaptés aux situations de handicap et des adaptations et paramétrages logiciels.
RNCP41678BC03	Mise en situation professionnelle : création d'un schéma de base de données relationnelle, installation et administration d'une base de données.
RNCP41678BC04	Mise en situation professionnelle : mise en place d'un réseau local interconnecté avec Cisco Packet Tracer, recherche, analyse et dépannage de dysfonctionnements sur un réseau préexistant, réseau local incluant VPN, serveur Radius et Wi-Fi sécurisé, étude de documents avec analyse et préconisations pour un réseau sécurisé hétérogène.
RNCP41678BC05	Mise en situation professionnelle : mise en place d'un système de surveillance reposant sur serveurs et agents, avec un IAM et l'usage d'outils d'IA, analyse de logs et détection de compromissions avec proposition de remédiations, mise en place de règles de gestion des accès et identités selon un cahier des charges, chiffrement asymétrique d'une communication entre deux utilisateurs.
RNCP41678BC06	Mise en situation professionnelle : mise en place d'un réseau Wi-Fi vulnérable, test et proposition de remédiations, mise en place d'un réseau filaire vulnérable, test et remédiations, utilisation d'outils de tests d'intrusion pour détecter les failles réseaux et systèmes, cartographie des vulnérabilités découvertes avec remédiations, explication des techniques de hacking pour améliorer la résilience, étude des référentiels de sécurisation (famille ISO 27000, NIST 800-53, RGPD).

Les mises en situation du parcours reprennent la logique des épreuves attendues pour chaque bloc : automatisation et analyse de scripts, cahier des charges et déploiement, schéma de base de données, réseau interconnecté dans un simulateur, supervision et analyse de journaux, tests de sécurité en laboratoire avec cartographie et remédiations. L'apprenant s'entraîne ainsi tout au long du parcours aux gestes professionnels évalués. SFM fournit le contenu pédagogique en marque blanche. L'organisation et la passation des épreuves de certification, ainsi que la décision de certification, restent de la responsabilité de l'organisme de formation et du certificateur.

06 · MOYENS ET PERSPECTIVES

Moyens pédagogiques et débouchés

Moyens pédagogiques et techniques

- Une vidéo de 3 à 5 minutes par sous-chapitre, représentant 30 % du volume horaire du parcours
- Cours texte enrichi, infographies et fiches de synthèse téléchargeables pour chaque sous-chapitre
- Mises en situation et études de cas ancrées dans le fil rouge Castelane Énergie Services
- QCM formatifs et évaluations de fin de cours avec suivi de progression par bloc de compétences
- Laboratoires virtualisés et simulateurs réseau (dont GNS3 et Cisco Packet Tracer) pour les travaux pratiques
- Environnements de test isolés et fictifs pour les exercices d'évaluation de la sécurité, sans aucune cible réelle
- Plateforme e-learning accessible à distance, personnalisable en marque blanche aux couleurs de l'organisme de formation

Débouchés et évolutions

- Opérateur en cybersécurité
- Opérateur Cyber Défense
- Technicien en cybersécurité
- Analyste SOC (Security Operation Center)
- Métiers ROME M1810 (production et exploitation de systèmes d'information) et M1801 (administration de systèmes d'information)
- Métiers ROME M1802 (expertise et support en systèmes d'information) et M1806 (conseil et maîtrise d'ouvrage en systèmes d'information)

Accessibilité

Contenus sous-titrés en français, contrastes conformes WCAG AA, navigation au clavier sur les écrans interactifs. L'organisme de formation qui diffuse le parcours adapte les modalités d'accompagnement aux personnes en situation de handicap avec son référent handicap.

Livrables fournis à l'organisme de formation

- Package SCORM 1.2 / 2004 et xAPI, compatible avec les principaux LMS
- Sources éditables des cours, scripts vidéo et banques de QCM
- Livret apprenant et grilles d'évaluation
- Licence marque blanche à vie, stagiaires illimités, maintenance 24 mois

School For Mate
On crée vos formations, vous n'avez plus qu'à les diffuser.

contact@schoolformate.com · catalogue-2026-sfm.netlify.app

Référentiel RNCP41678 consulté sur francecompetences.fr (export officiel du 4 novembre 2026). La délivrance de la certification relève exclusivement du certificateur et de l'organisme de formation habilité. Document non contractuel, susceptible d'évoluer avec le référentiel.