

SCHOOL FOR MATE

LIVRET PÉDAGOGIQUE

Expert en cybersécurité (MS : Mastère Spécialisé)

RNCP41445 · Certification RNCP · Niveau 7

Ce parcours de 440 heures prépare au titre Expert en cybersécurité (MS), RNCP41445 de niveau 7. Il couvre l'intégralité des quatre blocs de compétences du référentiel : audit et conception de projets de sécurité, déploiement et administration des solutions, gestion des incidents et des crises, veille, conseil et conformité. Le fil rouge est celui d'un opérateur fictif de services essentiels soumis à NIS2.

VOLUME HORAIRE	COURS	BLOCS
440 h	20	4

01 · PRÉSENTATION

La formation en bref

Intitulé	Expert en cybersécurité (MS : Mastère Spécialisé)
Code	RNCP41445
Type	Certification RNCP
Niveau	Niveau 7
Certificateur	INSTITUT MINES TELECOM - IMT NORD EUROPE
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	27/10/2030

Le métier et les compétences visées

L'expert en cybersécurité protège le système d'information d'une organisation contre les menaces numériques. Il audite l'infrastructure, qualifie les risques avec des méthodes reconnues (EBIOS RM, ISO 27001, NIST) et définit le périmètre de sécurité. Il pilote des projets de sécurisation et encadre une équipe. Il sélectionne, déploie et administre les solutions de filtrage, de détection et de gestion des identités. En situation d'incident ou de crise, il coordonne le SOC, qualifie et analyse les attaques, conduit les investigations forensics et active le plan de continuité. Conseiller de la direction, il anime la veille, garantit la conformité réglementaire (RGPD, NIS2) et diffuse une culture de sécurité auprès de l'ensemble des collaborateurs.

Public visé

- Ingénieurs et diplômés de niveau bac+5 en informatique, réseaux ou télécommunications souhaitant se spécialiser en cybersécurité
- Administrateurs systèmes et réseaux, ingénieurs d'exploitation ou architectes SI expérimentés visant un poste d'expert ou de responsable cybersécurité
- Chefs de projet SI, consultants en systèmes d'information et professionnels de la MOA souhaitant intégrer la sécurité à leurs missions
- Professionnels justifiant d'au moins 5 ans d'expérience en lien avec la cybersécurité, admis par validation des acquis personnels et professionnels (VAPP)
- Titulaires d'une licence ou d'un titre de niveau 6 justifiant d'au moins 3 ans d'expérience professionnelle dans le domaine visé (dans le cadre des dérogations prévues)

Prérequis

- Être titulaire d'un titre d'ingénieur conférant le grade de master, d'un diplôme d'école de management conférant le grade de master, d'un diplôme national de master ou d'un diplôme professionnel de niveau bac+5, d'un titre RNCP de niveau 7 ou d'un diplôme étranger équivalent
- Ou justifier d'un niveau M1 validé et d'au moins trois ans d'expérience professionnelle en lien avec la formation visée
- Par dérogation (40 % maximum de la promotion au total) : admission sur VAPP avec au moins 5 ans d'expérience en lien avec les compétences visées, ou niveau M1 avec moins de 3 ans d'expérience, ou licence (L3) ou titre RNCP de niveau 6 avec au moins 3 ans d'expérience en lien avec la formation (30 % maximum)
- Disposer de bases solides en systèmes d'exploitation, réseaux TCP/IP et administration des SI

Objectifs pédagogiques

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

- Auditer l'infrastructure d'un SI et conduire une analyse de risques selon la méthode EBIOS RM au regard de la PSSI, des normes ISO 27001 et NIST et du RGPD
- Définir le périmètre de sécurité d'un SI par la classification des actifs et une matrice de criticité alignée sur NIS2 et la famille ISO 2700x
- Comparer et sélectionner des solutions de sécurité à l'aide d'un benchmark structuré et d'un modèle de notation pondérée (Weighted Scoring Model)
- Piloter des projets de cybersécurité et encadrer une équipe en mobilisant Skill Matrix, NIST NICE ou ECSF, matrice RACI et méthodes en cascade ou agiles
- Déployer et administrer des solutions de filtrage, de chiffrement, de cloisonnement et de gestion des identités et des accès (SSO, MFA, RBAC, ABAC)
- Identifier les vulnérabilités et les attaques réseau, superviser les dispositifs de détection (SIEM, IDS/IPS, UEBA) et suivre des indicateurs comme le MTTR
- Établir et tester un plan de continuité et de reprise d'activité (PCRA) adapté aux activités critiques de l'entreprise
- Classifier, analyser et investiguer les incidents de sécurité, y compris par des analyses forensics, puis capitaliser l'expérience par une analyse des causes racines

- Communiquer en situation de crise auprès des parties prenantes, y compris les personnes en situation de handicap, avec des supports accessibles
- Animer une veille active, tenir un registre de conformité et conseiller la direction sur les investissements cyber (ROI, TCO, SWOT)

02 · FIL ROUGE PÉDAGOGIQUE

Hydrelis Services

IG

Inès Garnier

Responsable cybersécurité, nouvellement recrutée et rattachée à la direction des systèmes d'information

Production et distribution d'eau potable (opérateur régional de services essentiels)

Hydrelis Services assure la production et la distribution d'eau potable pour plusieurs agglomérations. L'entreprise compte trois usines de traitement pilotées par des automates industriels, un réseau de compteurs en télérelève, un centre de relation clients en téléphonie IP et un SI de gestion vieillissant. Son entrée dans le champ de la directive NIS2 a poussé la direction générale à créer un poste de responsable cybersécurité. Inès Garnier découvre une PSSI obsolète, des droits d'accès accumulés depuis des années, une supervision limitée et l'absence de plan de continuité. Avec une petite équipe interne et l'appui d'un prestataire, elle doit bâtir en dix-huit mois une organisation de sécurité crédible : audit, projets de sécurisation, SOC, gestion de crise et conformité. Elle doit aussi convaincre un comité de direction attentif aux coûts.

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 cartographie le SI d'Hydrelis, conduit l'audit EBIOS RM, sélectionne un SIEM par benchmark, structure son équipe et présente sa feuille de route au comité de pilotage.
2. Bloc 2 : Inès refond le filtrage entre les réseaux industriels et bureautiques, déploie l'IAM avec SSO et MFA, organise la gestion des vulnérabilités et protège le centre de relation clients contre les attaques DDoS sur la téléphonie IP.
3. Bloc 3 : Inès formalise le PCRA, met en service le SOC et affronte une attaque par rançongiciel qu'elle qualifie, investigue, communique et analyse en post-mortem.
4. Bloc 4 : Inès installe une veille sur les menaces, établit le registre de conformité RGPD et NIS2, déploie la charte et la sensibilisation, puis défend le budget cyber pluriannuel devant la direction générale.

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
RNCP41445BC01 · Concevoir des projets de sécurité des systèmes d'information		**132 h**
1	Cartographier le SI et définir le périmètre de sécurité	22 h
2	Auditer le SI et analyser les risques avec EBIOS RM	22 h
3	Benchmarker et sélectionner des solutions de sécurité	22 h
4	Définir les paramètres techniques et prioriser les projets de sécurité	22 h
5	Encadrer une équipe cyber, piloter les projets et en rendre compte	22 h
6	Exploiter un cahier des charges et sécuriser dès la conception (STRIDE)	22 h
RNCP41445BC02 · Mettre en œuvre et administrer des solutions de sécurité du système d'information		**132 h**
7	Filtrage et sécurité périmétrique : pare-feu, proxy, VPN et WAF	22 h
8	Protocoles de sécurité, cloisonnement et maintien en condition de sécurité	22 h
9	Concevoir et déployer une architecture IAM	22 h
10	Identifier les vulnérabilités et rédiger des rapports de faille	22 h
11	DevSecOps, supervision et indicateurs de sécurité	22 h
12	Détecter les attaques réseau et y répondre	22 h
RNCP41445BC03 · Gérer les incidents et les situations de crise		**110 h**
13	Établir et tester un plan de continuité et de reprise d'activité (PCRA)	22 h
14	Piloter le SOC et classifier les incidents	22 h
15	Analyser les incidents de sécurité et corriger les intrusions	22 h
16	Gérer une crise cyber et communiquer auprès des parties prenantes	22 h
17	Investigation forensics et capitalisation du retour d'expérience	22 h
RNCP41445BC04 · Garantir la veille, le conseil et l'information en matière de sécurité des systèmes d'information		**66 h**
18	Organiser et animer une veille active sur les menaces et la réglementation	22 h
19	Cartographier les obligations et piloter la conformité (RGPD, NIS2, ISO 27001)	22 h
20	Ancrer la culture de sécurité et conseiller la direction	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

RNCP41445BC01 · 132 h

Concevoir des projets de sécurité des systèmes d'information

Cours 1 · Cartographier le SI et définir le périmètre de sécurité

22 h

OBJECTIFS

- Inventorier et classifier les actifs du SI (données, infrastructures, applications, matériels, facteur humain)
- Construire une matrice de criticité fondée sur les critères CID et les exigences NIS2 et ISO 2700x

ÉVALUATION FORMATIVE

QCM de validation des acquis et production guidée d'une matrice de criticité commentée

CONTENUS

- Panorama des référentiels : ISO 27001 et 27002, NIST CSF, NIS2, guides de l'ANSSI
- Méthodes d'inventaire des actifs et cartographie du SI (vues métier, applicative, infrastructure)
- Classification des informations et des données sensibles
- Critères CID et construction d'une matrice de criticité
- Spécificités des SI industriels et des objets connectés
- Prise en compte du facteur humain dans le périmètre
- Formaliser le périmètre de sécurité et la liste des éléments à surveiller

Fil rouge · Inès dresse la première cartographie des actifs d'Hydrelis, des automates des usines au portail clients, puis classe chaque actif dans une matrice de criticité qu'elle soumet au DSI.

Cours 2 · Auditer le SI et analyser les risques avec EBIOS RM

22 h

OBJECTIFS

- Mener un audit organisationnel et technique du SI au regard de la PSSI, des normes ISO 27001 et NIST et du RGPD
- Conduire les cinq ateliers EBIOS RM et qualifier les risques en gravité et en vraisemblance

ÉVALUATION FORMATIVE

Étude de cas EBIOS RM avec rapport d'analyse de risques et grille d'autoévaluation

CONTENUS

- Typologie des audits : organisationnel, de conformité, d'architecture, de configuration, tests d'intrusion
- Préparer un audit : périmètre, référentiel, plan d'audit, entretiens et preuves
- EBIOS RM, atelier 1 : cadrage et socle de sécurité
- EBIOS RM, ateliers 2 et 3 : sources de risque et scénarios stratégiques
- EBIOS RM, ateliers 4 et 5 : scénarios opérationnels et traitement du risque
- Échelles de gravité et de vraisemblance, cartographie des risques
- Préconisations techniques et organisationnelles, plan de traitement et risques résiduels

Fil rouge · Inès anime les ateliers EBIOS RM avec les directions métier d'Hydrelis et identifie un scénario critique : l'altération des consignes de traitement de l'eau via un accès distant de maintenance mal protégé.

Cours 3 · Benchmarker et sélectionner des solutions de sécurité

22 h

OBJECTIFS

- Réaliser un benchmark détaillé de solutions (endpoints, identités, détection, surveillance)
- Justifier un choix technologique par un modèle de notation pondérée adapté aux besoins métier

ÉVALUATION FORMATIVE

Exercice de benchmark noté sur grille et QCM

CONTENUS

- Panorama des familles de solutions : EDR et XDR, IAM, SIEM, SOAR, NDR, gestion des vulnérabilités
- Recueillir les besoins métier et les traduire en critères de sélection
- Critères d'évaluation : fonctionnalités clés, compatibilité, ergonomie, fréquence de mise à jour, évolutivité, intégration, coût
- Construire un Weighted Scoring Model et analyser la sensibilité des pondérations
- Preuves de concept, essais et retours d'utilisateurs
- Labels et qualifications de l'ANSSI comme critère de confiance
- Rédiger une note de recommandation argumentée

Fil rouge · Inès compare trois solutions SIEM fictives pour Hydrelis et présente une grille de notation pondérée qui justifie son choix au regard des contraintes budgétaires et de l'intégration avec les systèmes industriels.

Cours 4 · Définir les paramètres techniques et prioriser les projets de sécurité

22 h

OBJECTIFS

- Définir les paramètres d'architecture réseau, de politique d'accès et de chiffrement selon la criticité de la menace
- Prioriser un portefeuille de projets SI et gérer leurs interdépendances

ÉVALUATION FORMATIVE

Mise en situation de priorisation avec production d'une feuille de route commentée

CONTENUS

- Principes d'architecture sécurisée : défense en profondeur, zonage, Zero Trust
- Politiques d'accès et de chiffrement selon les critères CID
- Tableau de bord de priorisation de la menace
- Calcul du ROI de résolution et arbitrage coût et risque
- Gestion de portefeuille : jalons critiques, livrables, dépendances
- Analyse des interdépendances entre projets en cours et à venir
- Construire une feuille de route de sécurité pluriannuelle

Fil rouge · Inès doit arbitrer entre la segmentation du réseau industriel, le déploiement du MFA et la refonte des sauvegardes : elle construit un tableau de priorisation et une feuille de route qui tient compte des dépendances entre ces chantiers.

Cours 5 · Encadrer une équipe cyber, piloter les projets et en rendre compte

22 h

OBJECTIFS

- Constituer et encadrer une équipe en affectant les tâches selon les compétences (Skill Matrix, NIST NICE, ECSF)
- Piloter les projets en cascade ou en agilité et produire des rapports synthétiques pour la hiérarchie et les comités

ÉVALUATION FORMATIVE

Production d'une matrice RACI et d'un rapport d'avancement, évalués sur grille critériée

CONTENUS

- Référentiels de compétences cyber : NIST NICE et ECSF
- Construire une Skill Matrix et un plan de développement des compétences
- Responsabilités hiérarchiques et fonctionnelles, matrice RACI
- Méthodes de gestion de projet : cycle en V, Scrum, Kanban, approches hybrides
- Outils de planification et de suivi des livrables
- Rapports d'avancement, notes d'analyse des choix opérationnels et rapports d'audit au format ISO
- Préparer et animer un comité de pilotage

Fil rouge · Inès répartit les rôles entre deux administrateurs, une analyste junior et le prestataire grâce à une Skill Matrix et une matrice RACI, puis présente l'état d'avancement du programme au premier comité de pilotage.

Cours 6 · Exploiter un cahier des charges et sécuriser dès la conception (STRIDE)

22 h

OBJECTIFS

- Analyser un cahier des charges technique et fonctionnel au regard des objectifs, des contraintes et de l'existant
- Modéliser les menaces avec STRIDE et proposer une architecture HLD sécurisée, par exemple pour le déploiement d'un SIEM

ÉVALUATION FORMATIVE

Étude de cas avec rapport de déploiement et architecture HLD, préparatoire à la mise en situation certificative

CONTENUS

- Lire et challenger un cahier des charges : objectifs, exigences, contraintes temporelles, budgétaires et réglementaires
- Compatibilité avec l'existant et limites des systèmes legacy
- Security by design et exigences de sécurité dans les spécifications
- Modélisation des menaces avec STRIDE
- Concevoir une architecture HLD (High Level Design)
- Étapes de déploiement d'un SIEM : sources de logs, collecte, règles de corrélation, montée en charge
- Rédiger un rapport de déploiement étape par étape

Fil rouge · À partir du cahier des charges du projet SIEM d'Hydrelis, Inès conduit une analyse STRIDE, conçoit l'architecture HLD et rédige le plan de déploiement en justifiant la composition de son équipe.

RNCP41445BC02 · 132 h

Mettre en œuvre et administrer des solutions de sécurité du système d'information

Cours 7 · Filtrage et sécurité périmétrique : pare-feu, proxy, VPN et WAF — 22 h

OBJECTIFS

- Concevoir et appliquer une politique de filtrage et de routage fondée sur le moindre privilège et le blocage par défaut
- Déployer pare-feu, proxy sécurisé, VPN et WAF sans dégrader l'activité de l'entreprise

ÉVALUATION FORMATIVE

Travaux pratiques en laboratoire virtuel avec compte rendu de configuration

CONTENUS

- Principes de filtrage : moindre privilège, blocage par défaut, filtrage à états
- Configuration de pare-feu et politique de routage
- Inspection profonde des paquets et inspection des protocoles courants
- Proxy sécurisé et filtrage web
- Réseaux privés virtuels : IPsec, TLS, accès distants
- Pare-feu applicatif (WAF) et protection des applications exposées
- Concilier sécurité et performance : tests, supervision, gestion des exceptions

Fil rouge · Inès fait cloisonner les réseaux industriels et bureautiques d'Hydrelis, remplace l'accès de maintenance à distance par un VPN filtré et protège le portail clients par un WAF.

Cours 8 · Protocoles de sécurité, cloisonnement et maintien en condition de sécurité — 22 h

OBJECTIFS

- Déployer et maintenir les protocoles de sécurité : chiffrement, certificats, cloisonnement, authentification forte
- Organiser le maintien en condition de sécurité : patch management, journaux, sécurité physique, documentation

ÉVALUATION FORMATIVE

QCM et exercice de rédaction d'une procédure de patch management

CONTENUS

- Cryptographie appliquée : chiffrement symétrique et asymétrique, hachage, signature
- Infrastructure à clés publiques et gestion du cycle de vie des certificats
- Cloisonnement des réseaux et des systèmes, durcissement des postes et serveurs
- Sécurité physique des équipements et des locaux techniques
- Patch management et gestion des mises à jour
- Journalisation, conservation et exploitation des journaux de sécurité
- Audits internes, écarts, mesures correctives et mise à jour des procédures

Fil rouge · Inès découvre des certificats expirés sur le portail de télérelève et des serveurs non mis à jour depuis des mois : elle instaure un processus de gestion des certificats et un cycle de patch management documenté.

Cours 9 · Concevoir et déployer une architecture IAM

22 h

OBJECTIFS

- Identifier l'ensemble des accès internes et externes et sélectionner une solution IAM adaptée
- Implémenter SSO, MFA, RBAC et ABAC et gérer les mécanismes d'autorisation

ÉVALUATION FORMATIVE

Étude de cas IAM avec démonstration commentée et soutenance blanche

CONTENUS

- Fondamentaux de l'IAM : identification, authentification, autorisation, traçabilité
- Revue des accès existants, comptes à privilèges et comptes de service
- Authentification forte et MFA, identification biométrique
- SSO et fédération d'identités : SAML, OAuth 2.0, OpenID Connect
- Modèles de contrôle d'accès RBAC et ABAC
- Cycle de vie des identités : arrivées, mobilités, départs
- Gestion des accès à privilèges (PAM) et recertification périodique

Fil rouge · Inès lance la revue des droits d'Hydrelis, supprime les comptes orphelins, définit des rôles métier et déploie un portail SSO avec MFA pour les techniciens d'astreinte.

Cours 10 · Identifier les vulnérabilités et rédiger des rapports de faille

22 h

OBJECTIFS

- Détecter les vulnérabilités d'un système par scans automatisés et simulations d'attaque
- Rédiger des rapports d'analyse standardisés et préconiser des mesures correctives et préventives

ÉVALUATION FORMATIVE

Travaux pratiques avec rapport de vulnérabilités évalué sur grille

CONTENUS

- Processus de gestion des vulnérabilités : découverte, qualification, traitement, vérification
- Scanners de vulnérabilités de type Nessus ou Qualys
- Tests d'intrusion applicatifs avec Burp Suite
- Méthodologie de pentest et cadre contractuel
- Scores CVSS et priorisation selon le contexte métier
- Templates de rapport de faille critique
- Adapter la restitution aux équipes techniques et aux métiers

Fil rouge · Une campagne de scans révèle une faille critique sur l'application de facturation d'Hydrelis : Inès rédige le rapport de faille et coordonne la correction avec l'éditeur et les métiers.

Cours 11 · DevSecOps, supervision et indicateurs de sécurité

22 h

OBJECTIFS

- Superviser la mise en œuvre de solutions de sécurité selon les principes du DevSecOps
- Définir des indicateurs de suivi et les présenter dans un tableau de bord

ÉVALUATION FORMATIVE

Construction guidée d'un tableau de bord KPI et QCM

CONTENUS

- Principes du DevSecOps et intégration de la sécurité dans les chaînes CI/CD
- Analyse de code et des dépendances, gestion des secrets
- Exploitation d'un SIEM pour la surveillance continue
- Indicateurs clés : MTTR, taux de faux positifs et de faux négatifs, couverture des journaux
- Construire un tableau de bord de KPI de sécurité
- Mesurer l'efficacité des dispositifs et ajuster les règles
- Inventaire des éléments de sécurité à protéger

Fil rouge · L'équipe de développement du portail clients d'Hydrelis livre chaque semaine : Inès intègre des contrôles de sécurité dans la chaîne de déploiement et présente un premier tableau de bord de KPI au DSI.

Cours 12 · Détecter les attaques réseau et y répondre

22 h

OBJECTIFS

- Identifier les principaux types d'attaques réseau (DDoS, phishing, exploitation de failles)
- Implémenter des mécanismes de détection et de protection adaptés, y compris en environnement SDN

ÉVALUATION FORMATIVE

Mise en situation en laboratoire avec rapport documenté des décisions

CONTENUS

- Panorama des attaques réseau et des techniques adverses (référentiel MITRE ATT&CK)
- Phishing et compromission de messagerie
- Attaques DDoS et dispositifs anti-DDoS
- Détection et prévention d'intrusion : IDS et IPS
- Analyse comportementale UEBA, surveillance des adresses IP et détection de trafic inhabituel
- Monitoring des terminaux et des réseaux
- Cas pratique : détection et remédiation d'attaques DDoS sur la VoIP SIP en environnement SDN

Fil rouge · Le centre de relation clients d'Hydrelis subit une saturation de sa téléphonie IP : Inès caractérise une attaque DDoS SIP et conçoit une architecture de détection et de remédiation dans l'environnement SDN.

RNCP41445BC03 · 110 h

Gérer les incidents et les situations de crise

Cours 13 · Établir et tester un plan de continuité et de reprise d'activité (PCRA)

22 h

OBJECTIFS

- Construire un PCRA en définissant processus, ressources techniques et humaines et moyens nécessaires
- Planifier et conduire des tests de continuité, par exemple une panne simulée de data center

ÉVALUATION FORMATIVE

Étude de cas avec rédaction d'un extrait de PCRA et compte rendu d'exercice

CONTENUS

- Bilan d'impact sur l'activité (BIA) et activités critiques
- Objectifs de reprise : RTO, RPO et niveaux de service dégradés
- Redondance des serveurs et architectures de haute disponibilité
- Stratégie de sauvegarde : fréquence, externalisation, sauvegardes hors ligne
- Ressources humaines, astreintes et cellule de continuité
- Scénarios de test et exercices de reprise
- Maintien en condition opérationnelle du PCRA

Fil rouge · Inès réalise le BIA de la distribution d'eau et de la facturation, puis organise un exercice de bascule simulant la perte de la salle serveurs principale.

Cours 14 · Piloter le SOC et classifier les incidents

22 h

OBJECTIFS

- Organiser et coordonner l'activité d'un SOC exploitant un SIEM
- Classifier les incidents selon des matrices de gravité, de vraisemblance et de criticité CID

ÉVALUATION FORMATIVE

Exercice de classification d'une série d'alertes et QCM

CONTENUS

- Organisation d'un SOC : niveaux d'analyse, rôles, processus
- Exploitation du SIEM et cas d'usage de détection
- Matrices de classification : gravité, vraisemblance, niveaux de menace
- Mesure d'impact des incidents et lien avec la cartographie des risques EBIOS RM
- Workflows automatisés et orchestration (SOAR)
- Playbooks et bibliothèque de crise à destination du SOC

Fil rouge · Le SOC d'Hydrelis remonte des dizaines d'alertes par jour : Inès définit la matrice de classification, rédige les premiers playbooks et automatise le traitement des alertes récurrentes.

Cours 15 · Analyser les incidents de sécurité et corriger les intrusions

22 h

OBJECTIFS

- Identifier les patterns malveillants dans les journaux et corréler les événements
- Détecter, caractériser et corriger des intrusions et des anomalies réseau

ÉVALUATION FORMATIVE

Travaux pratiques d'analyse de journaux avec rapport détaillé

CONTENUS

- Sources de données : journaux système, réseau, applicatifs, EDR
- Corrélation d'événements et recherche d'indicateurs de compromission
- Analyse de trafic avec des débogueurs et analyseurs réseau
- Threat hunting et monitorage en direct
- Coopération avec un CERT et les dispositifs nationaux
- Confinement, éradication et remédiation
- Rapport d'analyse d'incident

Fil rouge · Une connexion nocturne anormale sur un serveur de supervision alerte le SOC : Inès reconstitue le chemin d'attaque à partir des journaux, confine la machine et corrige la faille exploitée.

Cours 16 · Gérer une crise cyber et communiquer auprès des parties prenantes

22 h

OBJECTIFS

- Cartographier les acteurs et organiser la gestion d'une crise cyber
- Communiquer en interne et en externe avec des supports adaptés et accessibles, y compris aux personnes en situation de handicap

ÉVALUATION FORMATIVE

Simulation de cellule de crise avec production de supports de communication

CONTENUS

- Cartographie des acteurs internes et externes en amont de la crise
- Organisation de la cellule de crise : rôles, rythme, main courante
- Classification de la criticité d'une crise selon les CID et EBIOS RM
- Obligations de notification : CNIL, ANSSI au titre de NIS2, autorités sectorielles
- Communication de crise interne et externe, éléments de langage
- Supports visuels et infographies inspirés des recommandations de l'ANSSI
- Accessibilité des supports pour les personnes en situation de handicap

Fil rouge · Un rançongiciel chiffre une partie du SI de gestion d'Hydrelis : Inès active la cellule de crise, prépare les notifications réglementaires et diffuse des messages accessibles aux salariés, aux collectivités clientes et aux abonnés.

Cours 17 · Investigation forensics et capitalisation du retour d'expérience

22 h

OBJECTIFS

- Réaliser des analyses forensics à froid, à chaud et en temps réel, incluant l'analyse mémoire et le carving de données
- Animer le post-mortem et la capitalisation de l'expérience dans une logique d'amélioration continue

ÉVALUATION FORMATIVE

Travaux pratiques en binôme avec dossier synthétique d'analyse post-mortem

CONTENUS

- Cadre de l'investigation numérique : préservation de la preuve, chaîne de custody
- Analyse à froid et acquisition de supports
- Analyse à chaud, en temps réel et analyse de la mémoire vive
- Carving de données et reconstitution de chronologies
- Investigations administratives, civiles, pénales et réglementaires
- Analyse des causes racines : méthode des 5 pourquoi, diagramme d'Ishikawa
- Indicateurs MTTD, MTTR, MTTC et coût des interruptions
- Espace de documentation partagée et gestion des connaissances

Fil rouge · Après la crise, Inès conduit l'analyse forensics des postes compromis, anime le débriefing avec la méthode des 5 pourquoi et publie dans l'espace documentaire de l'équipe les enseignements et le plan d'amélioration.

RNCP41445BC04 · 66 h

Garantir la veille, le conseil et l'information en matière de sécurité des systèmes d'information

Cours 18 · Organiser et animer une veille active sur les menaces et la réglementation

22 h

OBJECTIFS

- Structurer un dispositif de veille technique, technologique et réglementaire
- Diffuser régulièrement une information accessible, par exemple un rapport mensuel sur les menaces émergentes

ÉVALUATION FORMATIVE

Production d'un bulletin de veille évalué sur grille

CONTENUS

- Sources de référence : ANSSI, CERT-FR, éditeurs, prestataires, collectifs professionnels
- Agrégation de flux RSS et outils de veille
- Plateformes de Threat Intelligence (TIP) et partage d'indicateurs
- Veille collaborative et participation à des collectifs
- Veille réglementaire sur les textes en vigueur et à venir
- Rédiger un rapport mensuel sur les menaces émergentes

Fil rouge · Inès met en place une veille partagée avec son équipe et publie le premier bulletin mensuel des menaces visant le secteur de l'eau à destination de la DSI et de la direction des opérations.

Cours 19 · Cartographier les obligations et piloter la conformité (RGPD, NIS2, ISO 27001) 22 h

OBJECTIFS

- Identifier les droits, obligations et normes applicables et les consigner dans un registre de conformité
- Comparer les exigences à l'état des lieux du SI à l'aide d'un outil GRC et vérifier l'application des normes ISO 2700x et du RGPD

ÉVALUATION FORMATIVE

Étude de cas de cadrage réglementaire avec rapport synthétique

CONTENUS

- Cadre juridique de la cybersécurité en France et en Europe
- RGPD : principes, registre des traitements, analyse d'impact, violations de données
- Directive NIS2 : entités concernées, mesures de gestion des risques, notification
- Famille ISO 2700x : système de management de la sécurité de l'information, déclaration d'applicabilité
- Construire et tenir un registre de conformité
- Analyse d'écarts et plan de mise en conformité avec un logiciel GRC
- Recherche bibliographique et cadrage réglementaire d'un cas

Fil rouge · Inès établit le registre de conformité d'Hydrelis, mesure les écarts avec les exigences NIS2 et ISO 27001 et vérifie le traitement des données des abonnés au regard du RGPD.

Cours 20 · Ancrer la culture de sécurité et conseiller la direction 22 h

OBJECTIFS

- Rédiger une charte de sécurité et organiser des sessions de sensibilisation à l'hygiène cyber
- Conseiller la direction sur les investissements cyber à l'aide d'études ROI et TCO, de tableaux de bord stratégiques et d'une analyse SWOT

ÉVALUATION FORMATIVE

Étude de cas en groupe avec supports de sensibilisation et note de conseil à la direction

CONTENUS

- Rédaction d'une charte de sécurité et de règles d'usage du SI
- Conception de supports de sensibilisation adaptés aux publics
- Organisation de sessions de formation à l'hygiène cyber et campagnes de simulation
- Audits internes périodiques de l'application de la charte
- Études de rentabilité : ROI et TCO des projets de sécurité
- Tableaux de bord stratégiques et analyse SWOT
- Présenter les risques, les impacts métier et les conséquences réglementaires à la direction

Fil rouge · Inès déploie la nouvelle charte auprès des agents d'exploitation et des équipes administratives, puis défend devant le comité de direction un budget cyber pluriannuel appuyé par une étude TCO et une analyse SWOT.

05 · CONFORMITÉ AU RÉFÉRENTIEL

Couverture des compétences

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

Compétence	Bloc	Cours
Auditer l'infrastructure du SI et mesurer sa conformité (EBIOS RM, PSSI, ISO 27001, NIST, RGPD)	RNCP41445BC01	1, 2
Définir le périmètre de sécurité du SI par classification des actifs et matrice de criticité	RNCP41445BC01	1
Analyser et comparer des solutions technologiques par benchmark	RNCP41445BC01	3
Définir des paramètres techniques et opérationnels et prioriser les projets SI selon la menace et les CID	RNCP41445BC01	4
Encadrer une équipe et piloter les projets cyber (Skill Matrix, NICE, ECSF, RACI, cascade ou agilité)	RNCP41445BC01	5
Concevoir des rapports synthétiques justifiés par des Weighted Scoring Models	RNCP41445BC01	3, 5
Analyser les cahiers des charges techniques et fonctionnels pour sécuriser le produit final (STRIDE)	RNCP41445BC01	6
Mettre en œuvre les règles de filtrage et les solutions de sécurité périmétrique	RNCP41445BC02	7, 12
Définir, déployer et maintenir les protocoles et outils de sécurité, y compris la sécurité physique	RNCP41445BC02	8
Sélectionner et mettre en place une architecture IAM (SSO, MFA, RBAC, ABAC)	RNCP41445BC02	9
Rédiger des rapports d'analyse et des rapports de faille à l'aide de scanners	RNCP41445BC02	10
Superviser les solutions de cybersécurité selon le DevSecOps avec indicateurs et outils de surveillance	RNCP41445BC02	11
Identifier les attaques réseau et implémenter les mécanismes de sécurité adaptés	RNCP41445BC02	12
Établir un plan de continuité et de reprise d'activités (PCRA)	RNCP41445BC03	13
Animer la capitalisation de l'expérience au sein des équipes IT	RNCP41445BC03	17
Classifier les incidents détectés à l'aide des outils de surveillance et de matrices	RNCP41445BC03	14
Analyser les incidents de sécurité détectés (logs, corrélation, CERT)	RNCP41445BC03	15
Communiquer auprès des parties prenantes, y compris en situation de handicap	RNCP41445BC03	16
Réaliser des analyses forensics	RNCP41445BC03	17
Organiser l'animation d'un système de veille active	RNCP41445BC04	18
Définir une charte de sécurité et organiser la sensibilisation à l'hygiène cyber	RNCP41445BC04	20
Conseiller la direction sur les projets et investissements cyber (ROI, TCO, SWOT)	RNCP41445BC04	20
Identifier les droits, obligations et normes applicables via un registre de conformité	RNCP41445BC04	19

Évaluations formatives

Chaque sous-chapitre se conclut par un QCM d'ancrage qui donne un retour immédiat et commenté. Chaque cours comporte une évaluation formative alignée sur les compétences visées : étude de cas, travaux pratiques en laboratoire virtuel, production d'un livrable professionnel (matrice de criticité, rapport de faille, PCRA, bulletin de veille) ou simulation. Ces productions sont évaluées sur des grilles critériées reprenant les attendus du référentiel, ce qui permet à l'apprenant et au formateur de l'organisme de formation de suivre la progression et d'identifier les besoins de remédiation.

Modalités de certification

Bloc	Modalité d'évaluation
RNCP41445BC01	Étude de cas : à partir d'une situation donnée et avec la méthodologie EBIOS RM, mener un audit organisationnel, fournir une analyse de risques (types, gravité, vraisemblance) et émettre des préconisations et mesures de traitement, avec un rapport écrit défendu à l'oral (travail de groupe, notation individuelle). Mise en situation professionnelle : déployer un SIEM à partir d'un cahier des charges, proposer une architecture HLD et rédiger un rapport de déploiement étape par étape précisant la méthode managériale et justifiant la constitution de l'équipe SI, avec un rapport défendu en soutenance (rendu de groupe, notation individuelle).
RNCP41445BC02	Travaux pratiques : déployer des méthodes d'authentification, gérer une identification biométrique, inventorier les éléments de sécurité à protéger, identifier des KPI présentés en tableau de bord, identifier et lister les vulnérabilités d'un système, avec plusieurs rapports et comptes rendus techniques (travail individuel ou de groupe, notation individuelle). Étude de cas : déployer une identité numérique IAM, avec démonstration et soutenance orale illustrée (travail et notation individuels). Mise en situation professionnelle : configurer des pare-feu, définir et implémenter une politique de filtrage et de routage, configurer une politique d'authentification, mettre en place un VPN et configurer un proxy, avec compte rendu écrit individuel. Mise en situation professionnelle : concevoir, déployer et configurer une architecture logicielle et matérielle de détection et de remédiation d'attaques DDoS VoIP SIP en environnement SDN, avec rapport écrit documenté analysant et illustrant les décisions (travail de groupe, notation individuelle).
RNCP41445BC03	Travaux pratiques : détecter, caractériser et corriger des intrusions et anomalies réseau, avec un rapport écrit détaillé et illustré des choix (travail et notation individuels). Étude de cas : à partir d'une situation réelle ou fictive, cartographier les acteurs en amont d'une crise, classifier les niveaux de criticité selon les CID et EBIOS RM, organiser la gestion de crise, communiquer en interne et en externe et constituer des éléments d'une bibliothèque de crise pour le SOC, avec livrables présentés en soutenance orale (travail de groupe, notation individuelle). Travaux pratiques : analyser une série d'incidents sous l'angle du digital forensics post-mortem, avec un dossier synthétique (travail en binôme, notation individuelle).
RNCP41445BC04	Étude de cas : dans le cadre d'une recherche bibliographique analytique et à partir de cas réels ou fictifs, cadrer la réglementation applicable et vérifier l'application du contexte normatif, avec un rapport synthétique argumenté et illustré (travail et notation individuels). Étude de cas : dans une situation réelle ou fictive, analyser l'application des normes ISO 2700x, vérifier la conformité au RGPD, identifier les enjeux juridiques et réglementaires de l'entreprise et créer des supports de sensibilisation pour les employés, avec un rapport détaillé et argumenté (travail de groupe, notation individuelle).

Le parcours reproduit le format des épreuves certificatives : chaque évaluation formative est conçue comme un entraînement à une modalité officielle (étude de cas EBIOS RM au cours 2, rapport de déploiement SIEM au cours 6, IAM au cours 9, filtrage et VPN au cours 7, DDoS SIP en SDN au cours 12, gestion de crise au cours 16, forensics au cours 17, cadrage réglementaire et conformité aux cours 19 et

20). Le fil rouge Hydrelis Services fournit un contexte continu qui permet de constituer progressivement des livrables réutilisables et de s'exercer à leur défense orale. Des grilles d'autoévaluation alignées sur les attendus du référentiel complètent le dispositif. SFM fournit le contenu pédagogique ; l'organisme de formation reste responsable de l'organisation des épreuves et de la relation avec le certificateur.

Moyens pédagogiques et débouchés

Moyens pédagogiques et techniques

- Plateforme e-learning en marque blanche accessible 24 h sur 24, avec suivi de progression et traçabilité des connexions
- Vidéos de 3 à 5 minutes par sous-chapitre, représentant 30 % du volume horaire, complétées par des cours texte enrichis
- Infographies, fiches méthodes et modèles de livrables professionnels (matrice de criticité, rapport de faille, PCRA, registre de conformité, charte)
- Études de cas et mises en situation scénarisées autour du fil rouge Hydrelis Services
- Scénarios de travaux pratiques conçus pour être réalisés dans un laboratoire virtuel mis à disposition par l'organisme de formation
- QCM d'ancrage auto-corrigés et grilles d'évaluation critériées alignées sur le référentiel
- Supports conçus selon les principes d'accessibilité numérique (sous-titrage des vidéos, transcriptions, contrastes)

Débouchés et évolutions

- Expert en cybersécurité
- Consultant en cybersécurité
- Responsable cybersécurité ou responsable de la sécurité des systèmes d'information (RSSI)
- Architecte sécurité et réseaux
- Chief Information Security Officer (CISO)
- Manager de la sécurité et des risques de l'information (MSRI)

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 RNCP41445 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.