

SCHOOL FOR MATE

LIVRET PÉDAGOGIQUE

Expert en cybersécurité (MS)

RNCP39837 · Certification RNCP · Niveau 7

Ce parcours de 440 heures prépare au titre RNCP39837 Expert en cybersécurité (MS), de niveau 7, en couvrant l'ensemble du cycle de vie de la sécurité d'un système d'information : analyse de risques, architecture, exploitation, audit, veille et réponse à incident. Construit bloc par bloc sur le référentiel France Compétences, il fait progresser l'apprenant au sein d'un opérateur fictif de services d'eau, confronté à des enjeux réglementaires, industriels et de protection des données.

VOLUME HORAIRE	COURS	BLOCS
440 h	20	5

01 · PRÉSENTATION

La formation en bref

Intitulé	Expert en cybersécurité (MS)
Code	RNCP39837
Type	Certification RNCP
Niveau	Niveau 7
Certificateur	CENTRALESUPELEC, INSTITUT MINES TELECOM - IMT ATLANTIQUE - BRETAGNE - PAYS DE LA LOIRE
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	28/11/2027

Le métier et les compétences visées

L'expert en cybersécurité conçoit, déploie et maintient la sécurité des systèmes d'information d'une organisation. Il conduit des analyses de risques selon des méthodes reconnues (EBIOS Risk Manager, ISO/IEC 27005) et définit les stratégies de traitement associées. Il conçoit des architectures sécurisées et met en place la supervision des équipements. Il contrôle la conformité aux référentiels et à la réglementation (LPM, NIS, RGPD, LCEN). Il audite le SI, assure une veille continue sur les menaces et les technologies, puis pilote la réponse aux incidents et la gestion de crise. En relation avec la DSI, les équipes d'exploitation, le SOC, le CERT et la direction, il traduit les enjeux techniques en décisions argumentées et assure la sécurité de la reprise d'activité.

Public visé

- Ingénieurs et cadres informatiques souhaitant se spécialiser en sécurité des systèmes d'information
- Administrateurs systèmes et réseaux expérimentés visant une fonction d'expertise ou d'architecture sécurité
- Chefs de projet SI, consultants et auditeurs souhaitant structurer une pratique SSI de niveau expert
- Professionnels en reconversion disposant d'un diplôme de niveau 7 ou d'une expérience significative en lien avec le numérique
- Agents des organismes publics et des opérateurs de services essentiels exerçant des missions de sécurité numérique

Prérequis

- Être titulaire d'un diplôme de niveau 7 : diplôme d'ingénieur habilité par la CTI, Master 2 universitaire ou international, diplôme d'école de management conférant le grade de master, diplôme d'IEP, titre RNCP de niveau 7 ou diplôme équivalent listé par le référentiel (médecine, pharmacie, écoles vétérinaires, écoles d'architecture)
- Ou être titulaire d'un Master 1 universitaire ou d'un Bachelor en 4 ans, avec trois ans d'expérience professionnelle post-diplôme
- À titre dérogatoire (dans la limite fixée par le certificateur) : Master 1 ou Bachelor en 4 ans avec moins de trois ans d'expérience, Licence 3 ou Bachelor en 3 ans avec trois ans d'expérience en lien avec la formation visée
- Par validation des acquis professionnels et personnels (VAPP) : cinq ans d'expérience professionnelle ayant un lien avéré avec les compétences visées

Objectifs pédagogiques

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

- Conduire une analyse de risques complète selon EBIOS Risk Manager, de la cartographie des biens essentiels et supports jusqu'aux scénarios opérationnels
- Évaluer la vraisemblance des scénarios de menace et le coût comparé des incidents, des mesures préventives et des remédiations
- Concevoir une stratégie de traitement du risque articulant mesures techniques, organisationnelles et procédures d'exploitation
- Identifier les obligations légales et normatives applicables (LPM, NIS, LCEN, RGPD, ISO/IEC 27001/27002, IEC 62443, RGS, guides ANSSI) et délimiter les responsabilités
- Déployer une architecture sécurisée et une supervision adaptée, puis qualifier et hiérarchiser les alertes de sécurité
- Exploiter le SI en sécurité en garantissant la conformité des configurations et l'usage pertinent des mécanismes cryptographiques
- Contrôler la conformité des traitements de données à caractère personnel et rendre compte aux décideurs et aux autorités compétentes
- Concevoir, conduire et restituer un audit SSI, y compris un test d'intrusion d'application web et l'analyse d'un produit de sécurité

- Mettre en œuvre une veille continue et actualiser l'analyse de risques en fonction des évolutions techniques, organisationnelles et législatives
- Détecter, caractériser et diagnostiquer un incident, coordonner la gestion de crise et rédiger un rapport d'incident assorti de préconisations

02 · FIL ROUGE PÉDAGOGIQUE

Hydrelia Services

CF

Camille Ferrand

Ingénieure cybersécurité, puis experte cybersécurité référente auprès du RSSI

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

Hydrelia Services gère la production et la distribution d'eau potable ainsi que l'assainissement pour une quarantaine de communes. Son système d'information combine un SI de gestion (facturation, relation abonnés, ressources humaines), un SI industriel de télégestion pilotant usines et stations de pompage, un portail web abonnés et un parc de compteurs communicants. L'exploitation repose en partie sur un infogéreur et sur des prestataires de maintenance industrielle disposant d'accès distants. Soumise aux exigences de la directive NIS et au RGPD, l'entreprise doit structurer sa sécurité après plusieurs alertes. Camille Ferrand rejoint l'équipe du RSSI, Laurent Méric. Elle travaille avec Sonia Lambert, déléguée à la protection des données, et Hugo Tessier, responsable de l'exploitation, ainsi qu'avec un SOC externalisé. Sa mission : faire passer Hydrelia d'une sécurité réactive à une sécurité pilotée par les risques.

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

La progression

1. Bloc 1 : Camille conduit l'analyse de risques EBIOS Risk Manager d'Hydrelia, chiffre les options de traitement et défend sa stratégie de sécurisation du nouveau portail abonnés devant la direction.
2. Bloc 2 : elle cartographie les obligations légales, conçoit la segmentation entre SI de gestion et SI industriel, déploie la supervision avec le SOC et forme les équipes techniques au vocabulaire commun.
3. Bloc 3 : elle prend en charge l'exploitation sécurisée, contrôle les configurations et la cryptographie, collecte les preuves d'application des mesures et sécurise, avec la DPO, la conformité des traitements de données des abonnés.
4. Bloc 4 : lors du rachat d'une régie voisine, elle audite un SI inconnu, réalise un test d'intrusion du portail, analyse une passerelle VPN industrielle et intègre sa veille dans une analyse de risques actualisée.
5. Bloc 5 : face à un rançongiciel touchant la facturation, elle caractérise l'incident, coordonne la cellule de crise, contrôle la sécurité de la reprise et rédige le rapport d'incident qui fait évoluer l'analyse de risques.

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
RNCP39837BC01 · Concevoir la sécurité d'un système d'information		**110 h**
1	Cadrer une étude de risques : périmètre, biens essentiels et biens supports	22 h
2	Analyser les enjeux de la sécurité du SI : dimensions technique, économique et juridique	22 h
3	Construire des scénarios de menace et évaluer leur vraisemblance	22 h
4	Évaluer les coûts de la sécurité et définir la stratégie de traitement du risque	22 h
5	Restituer l'analyse de risques et défendre une stratégie de sécurisation de service	22 h
RNCP39837BC02 · Déployer les mesures techniques et organisationnelles répondant aux exigences de sécurité du SI		**88 h**
6	Cadre légal, normes et référentiels de la sécurité des données et services numériques	22 h
7	Concevoir et déployer une architecture sécurisée	22 h
8	Déployer la supervision de sécurité et qualifier les alertes	22 h
9	Rendre compte des mesures de sécurité aux équipes techniques (SI, SOC, CERT)	22 h
RNCP39837BC03 · Exploiter en sécurité un SI		**88 h**
10	Exploitation sécurisée et conformité des configurations	22 h
11	Cryptographie appliquée à l'exploitation du SI	22 h
12	Collecter des preuves d'audit et des indicateurs de compromission en exploitation	22 h
13	Conformité des traitements de données personnelles et restitution aux décideurs	22 h
RNCP39837BC04 · Maintenir de manière continue la sécurité d'un SI		**88 h**
14	Concevoir et conduire un audit de la sécurité d'un SI	22 h
15	Test d'intrusion web et analyse de sécurité d'un produit	22 h
16	Rédiger et restituer un rapport d'audit et de test d'intrusion	22 h
17	Veille continue et actualisation de l'analyse de risques	22 h
RNCP39837BC05 · Réagir à un incident de sécurité du SI		**66 h**
18	Détecter et caractériser un incident de sécurité	22 h
19	Coordonner la réponse à incident, la gestion de crise et la reprise d'activité	22 h
20	Diagnostiquer un incident et rédiger le rapport d'incident	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

Contenu des cours

RNCP39837BC01 · 110 h

Concevoir la sécurité d'un système d'information

Cours 1 · Cadrer une étude de risques : périmètre, biens essentiels et biens supports — 22 h

OBJECTIFS

- Délimiter le périmètre d'une étude de risques et identifier les parties prenantes
- Recenser les biens essentiels, les biens supports et leurs relations fonctionnelles
- Formaliser le socle de sécurité et les procédures d'exploitation existantes

ÉVALUATION FORMATIVE

Étude de cas : production d'une cartographie des biens essentiels et supports à partir d'un dossier d'entreprise, complétée d'un QCM sur les notions de l'atelier 1

CONTENUS

- Panorama des méthodes de gestion des risques : ISO/IEC 27005, EBIOS Risk Manager, EIVP/PIA, BIA
- Atelier 1 d'EBIOS Risk Manager : cadrage, missions et valeurs métier
- Identification et cartographie des biens essentiels et des biens supports
- Modélisation des relations fonctionnelles et des dépendances entre biens
- Événements redoutés, besoins de sécurité et échelles de gravité
- Socle de sécurité : référentiels applicables et écarts constatés
- Recensement des procédures d'exploitation et de leurs points de fragilité

Fil rouge · Camille cadre l'étude de risques d'Hydrelia sur le périmètre de la télégestion et de la facturation : elle anime des entretiens avec Hugo Tessier et les responsables métier pour cartographier biens essentiels, biens supports et dépendances.

Cours 2 · Analyser les enjeux de la sécurité du SI : dimensions technique, économique et juridique — 22 h

OBJECTIFS

- Analyser le contexte d'une organisation pour qualifier ses enjeux de sécurité
- Relier les impacts techniques, financiers, juridiques et d'image d'un événement redouté
- Identifier les sources de risque et leurs objectifs visés

ÉVALUATION FORMATIVE

Mise en situation écrite : note d'analyse des enjeux SSI d'une organisation et cartographie de l'écosystème, corrigée selon une grille critériée

CONTENUS

- Étude du contexte : métier, organisation, écosystème, contraintes réglementaires
- Typologie des impacts : continuité de service, financier, juridique, sanitaire, réputation
- Responsabilités juridiques de l'organisation et de ses dirigeants en matière de SSI
- Atelier 2 d'EBIOS Risk Manager : sources de risque et objectifs visés
- Atelier 3 : cartographie de la menace numérique de l'écosystème et parties prenantes critiques
- Spécificités des systèmes industriels et des opérateurs de services essentiels

Fil rouge · À la demande de la direction générale, Camille analyse les conséquences d'une interruption de distribution d'eau : impacts techniques sur la télégestion, coûts financiers, exposition juridique d'Hydrelia et dépendance vis-à-vis de l'infogéreur.

Cours 3 · Construire des scénarios de menace et évaluer leur vraisemblance

22 h

OBJECTIFS

- Élaborer des scénarios stratégiques et opérationnels réalistes
- Évaluer la vraisemblance d'un scénario au regard du potentiel des sources de menace, de l'exposition et de la facilité d'exploitation des vulnérabilités
- Déterminer la nature de la réponse à apporter à chaque risque

ÉVALUATION FORMATIVE

Étude de cas : rédaction de deux scénarios opérationnels cotés et positionnés sur une cartographie des risques, avec QCM sur les critères de vraisemblance

CONTENUS

- Scénarios stratégiques : chemins d'attaque par l'écosystème
- Atelier 4 d'EBIOS Risk Manager : scénarios opérationnels et modes opératoires
- Référentiels de techniques d'attaque et modélisation de la chaîne d'attaque
- Critères de vraisemblance : potentiel de la source, exposition, facilité d'exploitation
- Identification et qualification des vulnérabilités des biens supports
- Cartographie des risques et matrice gravité vraisemblance
- Choix de la réponse : réduire, transférer, éviter ou accepter le risque

Fil rouge · Camille construit le scénario d'une intrusion dans la télégestion via l'accès distant d'un prestataire de maintenance, puis évalue sa vraisemblance en confrontant le potentiel des attaquants aux faiblesses réelles de cet accès.

Cours 4 · Évaluer les coûts de la sécurité et définir la stratégie de traitement du risque

22 h

OBJECTIFS

- Comparer le coût d'un incident, d'une mesure préventive et d'une remédiation
- Évaluer la pertinence d'une mesure technique au regard du contexte technique, légal et organisationnel
- Articuler mesures techniques, organisationnelles et procédures d'exploitation dans un plan de traitement

ÉVALUATION FORMATIVE

Livrable professionnel : plan de traitement du risque priorisé avec budget estimatif et une procédure d'exploitation, évalué sur grille

CONTENUS

- Estimation du coût d'un incident : pertes d'exploitation, remédiation, sanctions, réputation
- Coût complet d'une mesure : acquisition, déploiement, exploitation, maintien
- Atelier 5 d'EBIOS Risk Manager : stratégie de traitement et risques résiduels
- Évaluation de la pertinence d'une mesure technique selon le contexte
- Mesures organisationnelles : gouvernance, sensibilisation, gestion des tiers
- Rédaction de procédures d'exploitation et d'utilisation des équipements
- Priorisation des remédiations et construction d'un budget estimatif

Fil rouge · Camille compare le coût estimé d'un rançongiciel bloquant la facturation d'Hydrelia avec celui d'un bastion d'administration et de sauvegardes déconnectées, puis rédige la procédure d'accès distant des prestataires.

Cours 5 · Restituer l'analyse de risques et défendre une stratégie de sécurisation de service

22 h

OBJECTIFS

- Rédiger un rapport d'analyse de risques adapté au donneur d'ordre
- Présenter oralement une analyse de risques et une architecture sécurisée pour obtenir des arbitrages
- Adapter supports et discours à toutes les parties prenantes, dont les personnes en situation de handicap

ÉVALUATION FORMATIVE

Mise en situation orale : soutenance enregistrée d'un rapport d'analyse de risques et d'architecture, évaluée sur grille par le formateur

CONTENUS

- Structure d'un rapport d'analyse de risques : synthèse, cartographies, mesures, priorités, budget
- Rapport d'architecture d'un service fourni : choix fonctionnels, architecture SI et analyse de risques associée
- Techniques de présentation orale à un comité de direction ou à un jury
- Argumentation et aide à l'arbitrage : présenter des options et des risques résiduels
- Accessibilité des documents et des présentations : lisibilité, contrastes, alternatives textuelles, sous-titrage
- Sensibilisation des parties prenantes et conduite du changement

Fil rouge · Camille présente l'analyse de risques au comité de direction d'Hydrelia et défend l'architecture sécurisée du nouveau portail abonnés devant Laurent Méric et le DSI, avec des supports accessibles à un administrateur malvoyant.

RNCP39837BC02 · 88 h

Déployer les mesures techniques et organisationnelles répondant aux exigences de sécurité du SI

Cours 6 · Cadre légal, normes et référentiels de la sécurité des données et services numériques

22 h

OBJECTIFS

- Identifier les obligations légales applicables à une organisation et à ses prestataires
- Mobiliser les référentiels nationaux et internationaux pour définir des exigences de sécurité
- Délimiter les périmètres de responsabilité en matière de sécurité informatique

ÉVALUATION FORMATIVE

QCM réglementaire et étude de cas : matrice des obligations et des responsabilités pour une organisation donnée

CONTENUS

- Loi de programmation militaire de 2013, loi renseignement de 2015 et directive NIS
- Responsabilité des intermédiaires techniques (LCEN) et régime de la sous-traitance
- RGPD et loi Informatique et Libertés : principes et obligations de sécurité
- Recherche et divulgation de vulnérabilités, propriété intellectuelle (Hadopi, jurisprudence VideoLan)
- ISO/IEC 27001 et 27002, série ISA-99 / IEC 62443, guides NIST
- Référentiels nationaux : RGS, II901, guides ANSSI et guides CNIL
- Contractualisation de la sécurité avec les tiers et matrice des responsabilités

Fil rouge · Camille établit pour Hydrelia la cartographie des obligations issues de NIS, du RGPD et de la LCEN, et formalise la répartition des responsabilités de sécurité avec l'infogéreur dans une annexe contractuelle.

Cours 7 · Concevoir et déployer une architecture sécurisée

22 h

OBJECTIFS

- Concevoir une architecture segmentée conforme à l'état de l'art
- Déployer et configurer équipements et protocoles de sécurité
- Définir les procédures et les tests de validation d'une architecture

ÉVALUATION FORMATIVE

Travaux pratiques guidés : dossier d'architecture avec schéma, règles de filtrage et plan de tests, évalué sur grille

CONTENUS

- Principes d'architecture : défense en profondeur, cloisonnement, moindre privilège
- Segmentation réseau, filtrage et zones démilitarisées
- Zones et conduits pour les systèmes industriels selon IEC 62443
- Accès distants sécurisés : VPN, bastion d'administration, authentification forte
- Gestion des identités et des accès, annuaires et comptes à privilèges
- Protocoles sécurisés et durcissement des équipements
- Plan de tests de l'architecture et procédures d'exploitation associées

Fil rouge · Camille conçoit la segmentation entre le SI de gestion et le SI industriel d'Hydrelia, déploie un bastion pour les prestataires de maintenance et rédige le plan de tests de la nouvelle architecture.

Cours 8 · Déployer la supervision de sécurité et qualifier les alertes

22 h

OBJECTIFS

- Placer et configurer des sondes pour produire des indicateurs utiles
- Organiser la collecte et la conservation des journaux pour la réponse à incident et l'investigation
- Estimer la criticité d'une alerte et hiérarchiser son traitement

ÉVALUATION FORMATIVE

Exercice de qualification : tri et cotation d'un lot d'alertes simulées avec justification écrite, complété d'un QCM

CONTENUS

- Stratégie de journalisation : sources, contenus, horodatage, conservation
- Sondes de détection réseau et système : positionnement et configuration
- Centralisation et corrélation des événements (SIEM)
- Supervision spécifique des environnements industriels
- Critères de criticité : contexte, architecture, lien aux biens essentiels
- Hiérarchisation des alertes, réduction des faux positifs et recherche de corrélations
- Indicateurs de pilotage de la supervision

Fil rouge · Camille positionne les sondes aux frontières de la télégestion d'Hydrelia, définit les règles de corrélation avec le SOC externalisé et qualifie une alerte de connexion nocturne sur un automate de station de pompage.

Cours 9 · Rendre compte des mesures de sécurité aux équipes techniques (SI, SOC, CERT)

22 h

OBJECTIFS

- Produire une documentation technique claire des mesures mises en œuvre
- Adapter la communication écrite et orale à l'audience, y compris aux profils singuliers
- Construire un vocabulaire et une connaissance partagés des processus de sécurité

ÉVALUATION FORMATIVE

Étude de cas : audit critique d'un rapport d'architecture et rédaction d'un compte rendu destiné aux équipes techniques

CONTENUS

- Documentation d'architecture et dossiers d'exploitation sécurité
- Comptes rendus techniques et fiches réflexes pour le SOC et le CERT
- Vocabulaire SSI de référence et glossaire partagé
- Communication orale technique : réunions de passation, revues de sécurité
- Adaptation aux situations de handicap et à l'interculturalité
- Audit d'architecture de sécurité à partir d'un rapport produit
- Mesure de l'appropriation par les équipes

Fil rouge · Camille présente la nouvelle architecture et les règles de supervision au SOC externalisé et à l'équipe d'Hugo Tessier, qui compte un technicien malentendant et des intervenants d'une équipe d'infogérance internationale.

RNCP39837BC03 · 88 h

Exploiter en sécurité un SI

Cours 10 · Exploitation sécurisée et conformité des configurations

22 h

OBJECTIFS

- Assurer la conformité des configurations aux référentiels et à la réglementation
- Intervenir en sécurité sur les équipements et ressources du SI
- Contrôler l'application des procédures qualité et sécurité par les opérateurs techniques

ÉVALUATION FORMATIVE

Travaux pratiques : contrôle de conformité d'un jeu de configurations et rédaction d'une fiche d'écarts

CONTENUS

- Maintien en condition de sécurité : principes et organisation
- Référentiels de durcissement et contrôle de conformité des configurations
- Gestion des correctifs et des changements
- Administration sécurisée et poste d'administration dédié
- Sauvegardes, restauration et tests associés
- Contrôle des pratiques des opérateurs techniques et des prestataires
- Procédures qualité et sécurité dans un SI hétérogène

Fil rouge · Avant la mise en production des nouveaux serveurs de facturation d'Hydrelia, Camille contrôle leur conformité aux référentiels de durcissement et vérifie que l'infogéreur applique la procédure de gestion des correctifs.

Cours 11 · Cryptographie appliquée à l'exploitation du SI

22 h

OBJECTIFS

- Mobiliser les principes fondamentaux des outils cryptographiques
- Assurer l'adéquation entre configurations cryptographiques et évolutions techniques
- Piloter le cycle de vie des clés et des certificats

ÉVALUATION FORMATIVE

QCM technique et exercice pratique d'audit d'une configuration TLS avec recommandations

CONTENUS

- Fondamentaux : chiffrement symétrique et asymétrique, hachage, signature
- Infrastructures de gestion de clés et cycle de vie des certificats
- Configuration sécurisée des protocoles (TLS, SSH, VPN)
- Chiffrement des données au repos et des sauvegardes
- Recommandations nationales sur les mécanismes cryptographiques
- Obsolescence des algorithmes et anticipation des évolutions, dont la cryptographie post-quantique

Fil rouge · Camille organise le renouvellement des certificats du portail abonnés, met en place le chiffrement des sauvegardes et planifie le remplacement de suites cryptographiques obsolètes sur la télégestion.

Cours 12 · Collecter des preuves d'audit et des indicateurs de compromission en exploitation

22 h

OBJECTIFS

- Collecter des preuves en respectant les procédures qualité et sécurité
- Vérifier l'adéquation entre le plan de sécurité initial et sa mise en œuvre effective
- Identifier et exploiter des indicateurs de compromission

ÉVALUATION FORMATIVE

Étude de cas : dossier de preuves constitué à partir d'un environnement simulé et tableau d'écarts commenté

CONTENUS

- Notion de preuve : intégrité, traçabilité, chaîne de conservation
- Sources de preuves : journaux, configurations, entretiens, documents
- Indicateurs de compromission : typologie et exploitation
- Méthodes de collecte non intrusive en production
- Comparaison plan de traitement et réalité opérationnelle
- Formalisation des constats et suivi des écarts

Fil rouge · Six mois après le plan de traitement, Camille collecte des preuves pour vérifier que l'authentification forte des prestataires et la journalisation du bastion sont réellement appliquées chez Hydrelia.

Cours 13 · Conformité des traitements de données personnelles et restitution aux décideurs

22 h

OBJECTIFS

- Contrôler la conformité des traitements de données à caractère personnel
- Gérer le registre des traitements et l'interface avec la CNIL
- Rendre compte des écarts aux décideurs et aux autorités dans un format adapté

ÉVALUATION FORMATIVE

Livrable : extrait de registre, synthèse d'AIPD et note de restitution aux décideurs, évalués sur grille

CONTENUS

- Registre des traitements : constitution, mise à jour, contrôle
- Analyse d'impact relative à la protection des données (AIPD/PIA)
- Sécurité des traitements et contrôle des sous-traitants
- Violations de données : qualification, documentation, notification
- Relations avec la CNIL et autres autorités compétentes
- Rapports et présentations orales accessibles pour un public juridique ou décisionnaire

Fil rouge · Avec Sonia Lambert, Camille met à jour le registre des traitements d'Hydrelia, conduit l'analyse d'impact de la télérelève des compteurs communicants et présente les écarts constatés au comité de direction.

RNCP39837BC04 · 88 h

Maintenir de manière continue la sécurité d'un SI

Cours 14 · Concevoir et conduire un audit de la sécurité d'un SI

22 h

OBJECTIFS

- Rédiger un programme d'audit définissant périmètre, critères et objectifs
- Intervenir dans un système complexe et inconnu pour collecter des preuves
- Documenter les procédures de collecte pour pouvoir les rejouer

ÉVALUATION FORMATIVE

Livrable : programme d'audit et fiches de procédures de collecte, corrigés selon une grille critériée

CONTENUS

- Typologie des audits : organisationnel, architecture, configuration, code, intrusion
- Lignes directrices de l'audit de systèmes de management et référentiels d'audit SSI
- Programme d'audit : périmètre, critères, objectifs, convention d'audit
- Prise de connaissance d'un SI inconnu : reconnaissance et entretiens
- Techniques de collecte de preuves et documentation reproductible
- Analyse des preuves et établissement des constatations

Fil rouge · Hydrelia rachète une régie voisine : Camille rédige le programme d'audit de ce SI qu'elle ne connaît pas, puis documente chaque procédure de collecte afin qu'elle puisse être rejouée lors de l'audit de suivi.

Cours 15 · Test d'intrusion web et analyse de sécurité d'un produit

22 h

OBJECTIFS

- Identifier les vulnérabilités d'une application web et évaluer leur exploitabilité
- Coter la criticité des vulnérabilités et proposer des contre-mesures
- Analyser la sécurité d'un produit de sécurité

ÉVALUATION FORMATIVE

Travaux pratiques sur application vulnérable de démonstration : fiches de vulnérabilités cotées avec preuves et contre-mesures

CONTENUS

- Cadre juridique et contractuel du test d'intrusion
- Méthodologie de test d'intrusion et principales familles de vulnérabilités web
- Outils de test et preuves d'exploitation
- Cotation des vulnérabilités et évaluation de la criticité
- Analyse de sécurité d'un produit de sécurité : surface d'attaque, configuration, mises à jour
- Contre-mesures et recommandations de correction

Fil rouge · Camille réalise le test d'intrusion du portail abonnés d'Hydrelia et analyse la passerelle VPN utilisée par les prestataires industriels, en cotant chaque vulnérabilité découverte.

Cours 16 · Rédiger et restituer un rapport d'audit et de test d'intrusion

22 h

OBJECTIFS

- Structurer un rapport d'audit ou de pentest conforme aux attentes professionnelles
- Formuler des préconisations techniques et organisationnelles et un plan de remédiation
- Restituer l'audit à un public technique et décisionnaire, de manière accessible

ÉVALUATION FORMATIVE

Mise en situation : rédaction complète d'un rapport de pentest et restitution orale enregistrée, évaluées sur grille

CONTENUS

- Résumé exécutif : vue d'ensemble des découvertes et recommandations
- Méthodologie : description des méthodes et outils utilisés
- Découvertes : vulnérabilités, implications et preuves
- Recommandations et plan de remédiation détaillé
- Restitution orale aux équipes techniques et aux donneurs d'ordre
- Accessibilité des rapports et des supports de restitution

Fil rouge · Camille remet le rapport d'audit de la régie rachetée et le rapport de pentest du portail, puis les restitue successivement à l'équipe d'Hugo Tessier et à la direction générale d'Hydrelia.

Cours 17 · Veille continue et actualisation de l'analyse de risques

22 h

OBJECTIFS

- Organiser une veille sur les technologies, les vulnérabilités, les menaces et les produits de sécurité
- Évaluer l'impact et le coût d'une évolution ou d'une menace en termes de SSI
- Actualiser l'analyse de risques en fonction des évolutions techniques, structurelles et législatives

ÉVALUATION FORMATIVE

Livrable : bulletin de veille argumenté et mise à jour commentée d'une analyse de risques

CONTENUS

- Organisation de la veille : sources institutionnelles, bulletins, communautés
- Veille technologique : cloud, objets connectés, réseaux et télécommunications
- Veille vulnérabilités et menaces : qualification et diffusion aux acteurs concernés
- Évaluation des impacts et des coûts d'une évolution
- Veille réglementaire et normative
- Cycle opérationnel et cycle stratégique d'EBIOS Risk Manager : mise à jour de l'analyse
- Comptes rendus de veille et force de proposition

Fil rouge · Une vulnérabilité critique est publiée sur des automates utilisés par Hydrelia : Camille évalue son impact, coordonne la réponse avec les administrateurs, puis actualise l'analyse de risques en intégrant le projet de migration de la facturation vers le cloud.

RNCP39837BC05 · 66 h

Réagir à un incident de sécurité du SI

Cours 18 · Détecter et caractériser un incident de sécurité

22 h

OBJECTIFS

- Proposer une architecture de détection d'intrusion et ses phases de tests
- Identifier la portée temporelle et fonctionnelle d'un incident
- Collecter les indicateurs de compromission et caractériser la menace

ÉVALUATION FORMATIVE

Exercice sur scénario simulé : chronologie de l'incident et liste d'indicateurs de compromission justifiés

CONTENUS

- Architecture de détection d'intrusion et plan de tests
- Exploitation des sources : documents d'architecture, alertes, analyse de risques courante
- Qualification d'un événement en incident
- Détermination de la portée temporelle et fonctionnelle
- Collecte et partage des indicateurs de compromission
- Caractérisation de la menace et de l'attaquant

Fil rouge · Un vendredi soir, le SOC signale le chiffrement de serveurs de facturation d'Hydrelia : Camille s'appuie sur les documents d'architecture et l'analyse de risques pour déterminer depuis quand l'attaquant est présent et quels services sont touchés.

Cours 19 · Coordonner la réponse à incident, la gestion de crise et la reprise d'activité

22 h

OBJECTIFS

- Coordonner la gestion de crise en tenant compte des contextes technique et organisationnel
- Adopter une posture adaptée en mesurant les coûts associés à l'incident
- Contrôler la sécurité de la reprise d'activité

ÉVALUATION FORMATIVE

Exercice de crise sur table : rôle de coordinateur, main courante et note de décision évaluées sur grille

CONTENUS

- Organisation d'une cellule de crise : rôles, rythme, main courante
- Choix de posture : confinement, surveillance, éradication
- Évaluation des coûts de l'incident pour orienter les décisions
- Communication de crise interne et externe, notifications réglementaires
- Coordination avec les prestataires, le CERT et les autorités
- Plan de continuité, plan de reprise et contrôle de la sécurité de la reprise

Fil rouge · Camille coordonne la cellule de crise d'Hydrelia, arbitre entre isolement immédiat et surveillance de l'attaquant, prépare avec Sonia Lambert les notifications et vérifie la sécurité des systèmes avant leur remise en service.

Cours 20 · Diagnostiquer un incident et rédiger le rapport d'incident

22 h

OBJECTIFS

- Diagnostiquer en sécurité la nature et l'origine d'un incident
- Reconstituer le scénario d'attaque effectif et faire évoluer l'analyse de risques
- Rédiger un rapport d'incident avec actions curatives et formatives

ÉVALUATION FORMATIVE

Étude de cas finale : diagnostic et rapport d'incident complet à partir d'un jeu de traces, évalués sur grille

CONTENUS

- Principes de l'investigation numérique et préservation des preuves
- Analyse de journaux, de systèmes et d'artefacts
- Reconstitution du scénario d'attaque effectif
- Confrontation avec les scénarios de l'analyse de risques
- Structure du rapport d'incident et préconisations curatives et formatives
- Retour d'expérience et plan d'amélioration

Fil rouge · Camille reconstitue le scénario de l'attaque, constate qu'il emprunte un compte de prestataire non révoqué, rédige le rapport d'incident pour Laurent Méric et intègre ce chemin d'attaque dans l'analyse de risques d'Hydrelia.

05 · CONFORMITÉ AU RÉFÉRENTIEL

Couverture des compétences

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

Compétence	Bloc	Cours
Identifier les biens essentiels, les biens supports et les procédures d'exploitation	RNCP39837BC01	1, 3
Analyser les enjeux SSI en termes technique, économique et juridique	RNCP39837BC01	1, 2
Évaluer la vraisemblance d'un scénario de menace	RNCP39837BC01	3
Évaluer les coûts liés à la sécurité (incident, prévention, remédiation)	RNCP39837BC01	4
Restituer l'analyse de risques et les moyens de remédiation à un donneur d'ordre	RNCP39837BC01	5
Évaluer la pertinence d'une mesure technique de sécurité	RNCP39837BC01	4, 5
Proposer une articulation de moyens techniques et organisationnels et des procédures d'exploitation	RNCP39837BC01	4, 5
Identifier le contexte légal et les référentiels de sécurité	RNCP39837BC02	6
Déployer les équipements et protocoles d'une architecture sécurisée	RNCP39837BC02	7
Rendre compte des mesures SSI auprès des équipes techniques (SI, SOC, CERT)	RNCP39837BC02	9
Déployer un juste niveau de supervision et configurer des sondes	RNCP39837BC02	8
Estimer la criticité d'une alerte de sécurité et hiérarchiser les alertes	RNCP39837BC02	8
Collecter des preuves d'audit ou des indicateurs de compromission	RNCP39837BC03	12
Assurer la conformité des configurations et fonctionnalités des composants du SI	RNCP39837BC03	10
Assurer l'adéquation des configurations aux évolutions techniques en mobilisant la cryptographie	RNCP39837BC03	11
S'assurer du respect du cadre législatif par les opérateurs techniques	RNCP39837BC03	10, 13
Rendre compte de la conformité des traitements de données personnelles aux décideurs et autorités	RNCP39837BC03	13
Rédiger un programme d'audit dans un système complexe et inconnu	RNCP39837BC04	14
Documenter les procédures de collecte de preuves d'audit	RNCP39837BC04	14, 16
Restituer un audit et formuler des préconisations	RNCP39837BC04	15, 16
Réaliser une veille sur les évolutions technologiques, SI et télécommunications	RNCP39837BC04	17
Réaliser une veille sur les vulnérabilités, menaces et produits de sécurité	RNCP39837BC04	15, 17
Adapter l'analyse de risques aux évolutions des menaces, techniques, structurelles et législatives	RNCP39837BC04	17
Identifier la portée temporelle et fonctionnelle d'un incident	RNCP39837BC05	18

Collecter des indicateurs de compromission et mesurer les coûts de l'incident	RNCP39837BC05	18, 19
Coordonner la gestion de crise et la réponse à incident	RNCP39837BC05	19
Diagnostiquer la nature et l'origine d'un incident et faire évoluer l'analyse de risques	RNCP39837BC05	20
Établir un rapport d'incident avec actions curatives et formatives	RNCP39837BC05	20

Évaluations formatives

Chaque cours intègre des évaluations formatives régulières : QCM de fin de sous-chapitre pour vérifier l'acquisition des notions, études de cas et mises en situation dans le fil rouge Hydrelia Services, livrables professionnels (cartographies, plans de traitement, dossiers d'architecture, rapports d'audit et d'incident) corrigés selon des grilles critériées alignées sur les attendus des épreuves. Des restitutions orales enregistrées permettent de travailler la communication auprès de publics techniques et décisionnaires, en intégrant les exigences d'accessibilité. Les résultats sont tracés sur la plateforme, ce qui permet à l'organisme de formation de suivre la progression de chaque apprenant et de proposer des remédiations ciblées.

Modalités de certification

Bloc	Modalité d'évaluation
RNCP39837BC01	Mise en situation professionnelle portant sur une analyse de risques : étude d'un cas pratique représentatif de cas réels selon la méthodologie EBIOS Risk Manager, donnant lieu à un rapport écrit présentant la cartographie des biens essentiels et supports, la cartographie des risques, des scénarios de menace opérationnels vraisemblables, des mesures de sécurité complémentaires, la priorité des remédiations et un budget estimatif. Mise en situation professionnelle portant sur la sécurisation d'un service fourni : rapport d'architecture (choix fonctionnels, architecture SI et analyse de risques) et restitution orale devant un jury de professionnels de la SSI.
RNCP39837BC02	Mise en situation professionnelle portant sur la mise en place d'une architecture physique : le candidat conçoit l'architecture, met en place des procédures répondant aux exigences de sécurité et réalise les tests, les solutions étant évaluées par des professionnels de la SSI. Étude de cas portant sur la maîtrise des fondamentaux du déploiement d'une architecture de sécurité, au travers d'un audit d'architecture fondé sur le rapport produit, avec emploi du vocabulaire adapté aux comptes rendus destinés aux équipes techniques.
RNCP39837BC03	Mise en situation professionnelle simulée portant sur l'exploitation d'un SI proposé au candidat : il exploite l'architecture, met en place des procédures répondant aux exigences de sécurité et réalise les tests, les solutions étant évaluées par des professionnels de la SSI. Les travaux sont présentés lors d'une restitution orale individuelle.
RNCP39837BC04	Quatre mises en situation professionnelles simulées : audit d'un SI à partir d'un programme d'audit (collecte et analyse des preuves, constats recensés dans un rapport) ; test d'intrusion d'une application web réaliste donnant lieu à un rapport de pentest (résumé exécutif, méthodologie, découvertes, recommandations, plan de remédiation) évalué par des professionnels en activité ; analyse de risques fondée sur une étude bibliographique et formalisée dans un rapport ; analyse de sécurité d'un produit de sécurité donnant lieu à un rapport technique détaillant et cotant les vulnérabilités identifiées.

RNCP39837BC05	Mise en situation professionnelle simulée portant sur un incident de sécurité : le candidat propose une architecture de détection d'intrusion et ses phases de tests, collecte et analyse les informations de l'incident, collecte des indicateurs de compromission, coordonne la gestion de crise, rédige le diagnostic et émet des préconisations.

Le parcours reproduit la logique des épreuves officielles : chaque bloc se conclut par des livrables de même nature que ceux attendus en certification (rapport EBIOS Risk Manager avec budget, rapport d'architecture et soutenance, dossier d'exploitation, rapport d'audit, rapport de pentest structuré, analyse de produit de sécurité, rapport d'incident). Le fil rouge Hydrelia Services offre un cas continu, réaliste et cohérent, qui entraîne l'apprenant à mobiliser simultanément compétences techniques, réglementaires et de communication. Les grilles d'évaluation formative reprennent les critères des modalités officielles, et les restitutions orales préparent aux soutenances devant jury. School For Mate fournit le contenu pédagogique ; l'organisme de formation reste responsable de l'inscription des candidats, de l'organisation des épreuves et des relations avec les certificateurs habilités, selon les modalités qu'ils définissent.

06 · MOYENS ET PERSPECTIVES

Moyens pédagogiques et débouchés

Moyens pédagogiques et techniques

- Plateforme e-learning en marque blanche accessible 24 h/24, avec suivi de progression et traçabilité des activités
- Une vidéo de 3 à 5 minutes par sous-chapitre, représentant 30 % du volume horaire du parcours
- Cours textes enrichis, infographies, fiches méthodes et glossaire SSI partagé, conçus pour être accessibles (sous-titrage, contrastes, compatibilité avec les lecteurs d'écran)
- Études de cas, mises en situation et livrables professionnels ancrés dans le fil rouge Hydrelia Services
- Modèles et trames professionnelles : rapport d'analyse de risques, dossier d'architecture, programme d'audit, rapport de pentest, rapport d'incident, main courante de crise
- Énoncés de travaux pratiques et scénarios techniques à déployer dans l'environnement de laboratoire de l'organisme de formation
- QCM et grilles d'évaluation critériées alignées sur les modalités de certification de chaque bloc

Débouchés et évolutions

- Expert cybersécurité, ingénieur cybersécurité ou ingénieur sécurité des systèmes d'information
- Architecte cybersécurité ou ingénieur sécurité système et réseau
- Analyste en cybersécurité
- Consultant cybersécurité ou auditeur SSI
- Ingénieur projet cybersécurité
- Officier SSI

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 RNCP39837 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.