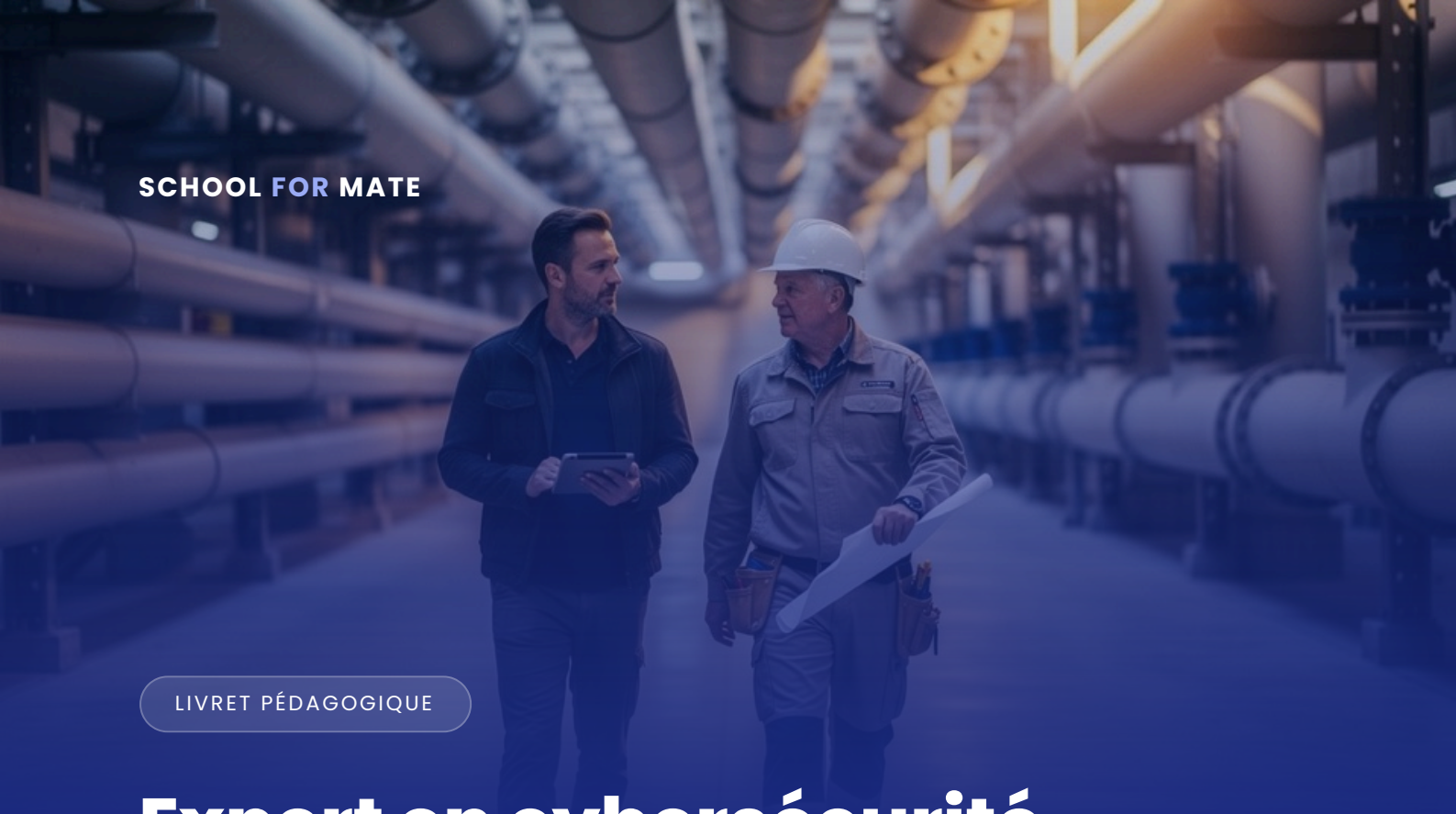


SCHOOL FOR MATE

LIVRET PÉDAGOGIQUE

Expert en cybersécurité

RNCP39999 · Certification RNCP · Niveau 7

Ce parcours de 440 heures prépare vos apprenants à exercer comme expert en cybersécurité, de l'analyse de risques au pilotage de la conformité, en passant par l'audit, la sécurité opérationnelle et l'intégration d'outils de sécurité en environnement hétérogène. Construit bloc par bloc sur le référentiel RNCP39999 de niveau 7, il suit pas à pas Camille Vasseur, chargée de mission cybersécurité chez Hydrelis Énergies, un opérateur multi-sites confronté à des menaces bien réelles.

VOLUME HORAIRE	COURS	BLOCS
440 h	20	7

01 · PRÉSENTATION

La formation en bref

Intitulé	Expert en cybersécurité
Code	RNCP39999
Type	Certification RNCP
Niveau	Niveau 7
Certificateur	IKAI
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	18/12/2027

Le métier et les compétences visées

L'expert en cybersécurité protège le système d'information d'une organisation et en garantit la résilience face aux cybermenaces. Il identifie les actifs critiques, conduit des analyses de risques selon des méthodes reconnues comme EBIOS Risk Manager, définit et met en œuvre les mesures de protection techniques et organisationnelles, et veille à la conformité au RGPD, à NIS2 et aux normes applicables. Il pilote des projets de sécurité, sensibilise les équipes et rend compte à la direction. Selon sa spécialisation, il conduit des audits de sécurité, opère la détection et le traitement des incidents au sein d'un SOC ou intègre des solutions de sécurité dans des environnements hybrides mêlant cloud, systèmes industriels et objets connectés.

Public visé

- Alternants titulaires d'une certification de niveau 5 ou 6 en informatique, mathématiques ou domaine connexe souhaitant se spécialiser en cybersécurité
- Administrateurs systèmes et réseaux souhaitant évoluer vers des fonctions d'expertise en sécurité
- Développeurs et techniciens informatiques justifiant d'une expérience professionnelle en informatique
- Professionnels en reconversion disposant de solides bases en réseau, système et programmation
- Salariés de DSI ou d'ESN visant des fonctions de RSSI, consultant ou analyste SOC

Prérequis

- Maîtriser les compétences de base en réseau, programmation et système informatique
- Ou être titulaire d'une certification de niveau 5 ou 6 en informatique, mathématiques ou domaines connexes à la cybersécurité
- Ou justifier d'une expérience professionnelle en informatique d'au moins 530 heures
- Une seule de ces conditions suffit pour intégrer la formation en alternance

Objectifs pédagogiques

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

- Conduire une analyse de risques complète d'un système d'information selon la méthode EBIOS Risk Manager et proposer un plan de traitement priorisé
- Cartographier un système d'information et mettre en place une veille sur les menaces et vulnérabilités
- Durcir les infrastructures et paramétrer la sécurité des composants logiques (hyperviseurs, containers, orchestrateurs, applications)
- Classifier les données sensibles et appliquer des mesures de confidentialité et d'intégrité adaptées à leur criticité
- Évaluer la conformité d'une organisation au RGPD, à NIS2 et aux normes de sécurité, puis piloter la correction des écarts
- Piloter un projet de cybersécurité, du cahier des charges à la soutenance, en communiquant auprès de toutes les parties prenantes de manière accessible
- Planifier, conduire et restituer un audit de sécurité d'un système d'information
- Déployer une chaîne de détection et un processus de gestion des incidents conforme à la norme ISO 27035
- Intégrer et contrôler des solutions de sécurité dans un environnement hétérogène mêlant cloud, IoT et systèmes industriels

02 · FIL ROUGE PÉDAGOGIQUE

Hydrelis Énergies

CV

Camille Vasseur

Chargée de mission cybersécurité, puis RSSI adjointe

Production et distribution d'énergie (réseaux de chaleur urbains et petite hydroélectricité)

Hydrelis Énergies exploite 14 réseaux de chaleur urbains et 6 microcentrales hydroélectriques répartis sur trois régions, avec 620 salariés et un siège à Grenoble. Son système d'information est hétérogène : ERP hébergé dans un cloud public, portail client traitant des données personnelles et de facturation, supervision industrielle SCADA sur les sites de production, capteurs connectés sur les sous-stations et nombreux prestataires de maintenance à distance. Une tentative de rançongiciel sur un site, l'entrée dans le champ de la directive NIS2 et une forte croissance externe poussent la direction générale à structurer sa cybersécurité. Camille Vasseur, ancienne administratrice systèmes, rejoint la direction des systèmes d'information pour construire la démarche. Elle doit convaincre, prioriser, sécuriser et rendre des comptes, avec un budget et des équipes limités.

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 inventorie les actifs d'Hydrelis, anime les ateliers EBIOS RM avec les métiers et fait valider par le comité de direction un plan de traitement des risques priorisé.
2. Bloc 2 : elle cartographie le SI, monte une veille sur les vulnérabilités, durcit l'annuaire, les serveurs et la plateforme de containers du portail client, et classifie les données sensibles.
3. Bloc 3 : elle conduit l'étude d'écarts NIS2 et RGPD, rédige la politique de sécurité et les procédures, gère une violation de données et produit le premier rapport de conformité.
4. Bloc 4 : elle pilote le projet de mise en place d'un SOC mutualisé, de la note de cadrage à la soutenance devant la direction, avec une campagne de sensibilisation accessible à tous les salariés.
5. Bloc 5 : devenue RSSI adjointe, elle construit le programme d'audit de la filiale récemment acquise, coordonne un test d'intrusion et présente ses conclusions au comité d'audit.
6. Bloc 6 : elle déploie le SIEM, formalise le processus de gestion des incidents selon ISO 27035 et dirige le traitement d'une compromission sur le portail client, jusqu'au test du PRA.
7. Bloc 7 : elle sécurise l'interconnexion entre le SCADA des microcentrales, les capteurs IoT et le cloud, en intégrant pare-feu industriel, NAC et diode de données sans interrompre la production.

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
RNCP39999BC01 · Gérer les risques liés à la sécurité de l'information		**66 h**
1	Identifier les actifs et les sources de menaces	22 h
2	Évaluer, estimer et classifier les risques	22 h
3	Traiter, suivre et réévaluer les risques	22 h
RNCP39999BC02 · Protéger un système d'information face à la cyber-menace		**88 h**
4	Cartographier le SI et organiser la veille sur les menaces	22 h
5	Durcir l'infrastructure et évaluer les mesures de sécurité	22 h
6	Sécuriser les composants logiques : virtualisation, containers et applications	22 h
7	Protéger les données et les identités	22 h
RNCP39999BC03 · Assurer la conformité du traitement de l'information au cadre réglementaire et normatif en vigueur dans l'organisation		**66 h**
8	Maîtriser le cadre légal, réglementaire et normatif de la cybersécurité	22 h
9	Évaluer la conformité et construire les politiques et procédures	22 h
10	Faire vivre la conformité : sensibilisation, suivi et gestion des non-conformités	22 h
RNCP39999BC04 · Piloter un projet et communiquer en cybersécurité		**66 h**
11	Cadrer un projet de cybersécurité et rédiger le cahier des charges	22 h
12	Planifier, sécuriser et piloter le projet et son équipe	22 h
13	Communiquer, sensibiliser et restituer les résultats	22 h
RNCP39999BC05 · Mener un audit de sécurité d'un système d'information (spécialisation)		**44 h**
14	Construire le programme d'audit et préparer la mission	22 h
15	Conduire, suivre et restituer l'audit de sécurité	22 h
RNCP39999BC06 · Opérer et surveiller les mesures de sécurité d'un SI (spécialisation)		**66 h**
16	Déployer un système de surveillance de la sécurité	22 h
17	Concevoir le processus de gestion des incidents et qualifier les alertes	22 h
18	Traiter les incidents et éprouver la résilience	22 h
RNCP39999BC07 · Intégrer des outils de sécurité dans un environnement hétérogène (spécialisation)		**44 h**

19	Analyser un environnement hétérogène avant intégration	22 h
20	Déployer, superviser et contrôler les solutions de sécurité	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

RNCP39999BC01 · 66 h

Gérer les risques liés à la sécurité de l'information

Cours 1 · Identifier les actifs et les sources de menaces

22 h

OBJECTIFS

- Réaliser un inventaire exhaustif des actifs informationnels et évaluer leur criticité
- Identifier les sources de menaces et leurs objectifs visés à l'aide d'une méthode d'analyse appropriée

ÉVALUATION FORMATIVE

QCM de validation par sous-chapitre et production guidée d'un registre des actifs avec cotation de criticité

CONTENUS

- Fondamentaux de la gestion des risques : vocabulaire, ISO 27005 et place de l'analyse de risques dans un SMSI
- Présentation de la méthode EBIOS Risk Manager et de ses cinq ateliers
- Atelier 1 : cadrage, valeurs métier, biens supports et socle de sécurité
- Évaluation de la criticité des actifs : besoins de disponibilité, intégrité, confidentialité et traçabilité
- Atelier 2 : identification des sources de risque et des objectifs visés
- Panorama des menaces : cybercriminalité, espionnage, hacktivisme, menace interne
- Évaluation de la pertinence des couples source de risque et objectif visé

Fil rouge · Camille anime un atelier de cadrage avec les directions exploitation, clientèle et finance d'Hydrelis pour lister les valeurs métier et leurs biens supports, puis qualifie les sources de risque susceptibles de cibler la supervision des réseaux de chaleur.

Cours 2 · Évaluer, estimer et classifier les risques

22 h

OBJECTIFS

- Construire et évaluer des scénarios stratégiques et opérationnels selon EBIOS RM
- Estimer l'impact des risques et les hiérarchiser selon des critères de gravité et de vraisemblance

ÉVALUATION FORMATIVE

Étude de cas notée : rédaction de deux scénarios opérationnels et d'une matrice de risques commentée, complétée par un QCM

CONTENUS

- Atelier 3 : cartographie de la menace de l'écosystème et des parties prenantes
- Construction des scénarios stratégiques et chemins d'attaque
- Atelier 4 : scénarios opérationnels et modes opératoires (référentiel MITRE ATT&CK)
- Évaluation de la vraisemblance des scénarios opérationnels
- Estimation des impacts : opérationnels, financiers, juridiques, réputationnels et humains
- Échelles de gravité et de vraisemblance, matrice des risques
- Hiérarchisation des risques et présentation à la direction

Fil rouge · Camille modélise le scénario d'un prestataire de maintenance compromis utilisé comme point d'entrée vers le SCADA d'une microcentrale, en estime l'impact sur la continuité de fourniture et le positionne dans la matrice des risques.

Cours 3 · Traiter, suivre et réévaluer les risques

22 h

OBJECTIFS

- Élaborer une stratégie de traitement des risques et un plan de remédiation adaptés aux contraintes de l'organisation
- Mettre en œuvre et piloter le plan de traitement avec des indicateurs de performance et de conformité

ÉVALUATION FORMATIVE

Mise en situation de restitution : présentation orale enregistrée d'un plan de traitement des risques, évaluée sur grille critériée

CONTENUS

- Atelier 5 : stratégies de traitement (réduction, transfert, refus, acceptation)
- Choix des mesures de sécurité en cohérence avec la stratégie retenue et les normes applicables
- Construction du plan d'amélioration continue de la sécurité (PACS) et du plan de remédiation
- Arbitrages budgétaires, risques résiduels et acceptation formelle par la direction
- Mise en œuvre du plan : jalons, responsables, intégration aux politiques internes
- Indicateurs de suivi des risques et tableaux de bord
- Réévaluation périodique et cycle d'amélioration continue

Fil rouge · Camille présente au comité de direction d'Hydrelis un plan de traitement en trois vagues, négocie le transfert d'une partie du risque à l'assurance cyber et définit les indicateurs trimestriels de suivi.

Protéger un système d'information face à la cyber-menace

Cours 4 · Cartographier le SI et organiser la veille sur les menaces

22 h

OBJECTIFS

- Cartographier les composants physiques et logiques d'un SI, leurs interconnexions, dépendances et criticité
- Mettre en place un dispositif de veille sur les menaces et vulnérabilités et en exploiter les résultats

ÉVALUATION FORMATIVE

Exercice pratique : réalisation d'une cartographie multi-vues à partir d'un dossier technique et d'une fiche de veille qualifiée

CONTENUS

- Les vues de la cartographie du SI : écosystème, métier, applicative, infrastructure logique et physique
- Identification, classification et documentation des composants et de leurs dépendances
- Outils et formats de cartographie, maintien à jour dans le temps
- Sources de veille : CERT-FR, bulletins éditeurs, bases CVE, flux de renseignement sur la menace
- Qualification des vulnérabilités : scores CVSS, exploitabilité, exposition
- Organisation d'un processus de veille et diffusion aux équipes concernées

Fil rouge · Camille produit la première cartographie complète du SI d'Hydrelis, découvre des flux non documentés entre la supervision et la bureautique, et met en place une veille hebdomadaire sur les vulnérabilités des équipements industriels utilisés.

Cours 5 · Durcir l'infrastructure et évaluer les mesures de sécurité

22 h

OBJECTIFS

- Mettre en œuvre des mesures de durcissement pour réduire la surface d'attaque
- Auditer les mesures de sécurité en place et évaluer leur impact sur la sécurité du SI

ÉVALUATION FORMATIVE

Étude de cas : rapport d'évaluation des mesures existantes et plan de durcissement priorisé, complété par un QCM

CONTENUS

- Principes de défense en profondeur et de moindre privilège
- Durcissement des systèmes Windows et Linux selon les guides de l'ANSSI et les benchmarks CIS
- Sécurisation de l'annuaire Active Directory et modèle d'administration en tiers
- Durcissement réseau : segmentation, filtrage, sécurisation des accès distants
- Gestion des correctifs et des configurations
- Évaluation de la pertinence des solutions de sécurité : revue de configuration, scans, indicateurs d'efficacité

Fil rouge · Après la tentative de rançongiciel, Camille audite la configuration de l'annuaire et des postes d'Hydrelis, constate des comptes à privilèges excessifs et déploie un plan de durcissement par paliers.

Cours 6 · Sécuriser les composants logiques : virtualisation, containers et applications

22 h

OBJECTIFS

- Définir les paramètres de sécurité des hyperviseurs, containers et orchestrateurs à partir de référentiels reconnus
- Sécuriser les applications et services critiques conformément aux politiques de l'organisation

ÉVALUATION FORMATIVE

Exercice pratique : rédaction d'une fiche de paramétrage sécurisé d'un orchestrateur et d'une application, évaluée sur grille

CONTENUS

- Sécurité des hyperviseurs : isolation, administration, sauvegarde
- Sécurité des containers : images, registres, exécution
- Sécurité des orchestrateurs : contrôle d'accès, secrets, politiques réseau
- Sécurité applicative : principales vulnérabilités du web (OWASP Top 10) et mesures associées
- Sécurisation des services critiques : messagerie, DNS, sauvegardes, bases de données
- Utilisation des référentiels de sécurité : guides ANSSI, benchmarks CIS, politiques internes

Fil rouge · Camille définit la configuration de sécurité de la plateforme de containers qui héberge le nouveau portail client d'Hydrelis et impose une politique de gestion des secrets à l'équipe de développement.

Cours 7 · Protéger les données et les identités

22 h

OBJECTIFS

- Classifier les données sensibles et garantir la conformité des usages aux politiques de gestion des identités et des données
- Appliquer des mesures de confidentialité et d'intégrité proportionnées à la criticité des données

ÉVALUATION FORMATIVE

Mise en situation : plan d'action de sécurisation des données à partir d'un registre fourni, préparatoire à l'épreuve du bloc

CONTENUS

- Classification des données : niveaux de sensibilité, marquage, registre des données
- Gestion des identités et des accès : cycle de vie, habilitations, revue des droits
- Authentification forte et gestion des comptes à privilèges
- Chiffrement au repos et en transit, gestion des clés et certificats
- Intégrité et traçabilité : signatures, journalisation, sauvegardes protégées
- Prévention des fuites de données et contrôle des usages
- Évaluation de l'efficience des mesures appliquées aux données

Fil rouge · Camille classifie les données de facturation et de consommation des clients d'Hydrelis, impose l'authentification forte aux accès distants et vérifie que les droits des prestataires correspondent à leurs missions.

Assurer la conformité du traitement de l'information au cadre réglementaire et normatif en vigueur dans l'organisation

Cours 8 · Maîtriser le cadre légal, réglementaire et normatif de la cybersécurité

22 h

OBJECTIFS

- Identifier les lois, règlements et normes applicables à une organisation
- Organiser une veille juridique et normative en sécurité des données

ÉVALUATION FORMATIVE

QCM par sous-chapitre et production d'une matrice des exigences légales et normatives applicables à un cas fourni

CONTENUS

- Le RGPD : principes, rôles, obligations de sécurité et droits des personnes
- Les directives NIS et NIS2 : entités concernées, obligations, gouvernance
- Le Cybersecurity Act et la certification européenne de cybersécurité
- La LCEN et la responsabilité des acteurs du numérique
- Le code pénal : atteintes aux systèmes de traitement automatisé de données
- Normes et référentiels : famille ISO 27000, référentiels sectoriels (HDS, PCI-DSS)
- Mettre en place une veille réglementaire et normative

Fil rouge · Camille détermine si Hydrelis relève de NIS2 en tant qu'opérateur du secteur de l'énergie, identifie les obligations RGPD liées au portail client et construit la matrice des exigences applicables.

Cours 9 · Évaluer la conformité et construire les politiques et procédures

22 h

OBJECTIFS

- Réaliser une étude d'écarts par audit et revue documentaire
- Rédiger des politiques et procédures de conformité claires et un plan d'action correctif

ÉVALUATION FORMATIVE

Étude de cas : rapport d'écarts et extrait de politique de sécurité rédigé, évalués sur grille critériée

CONTENUS

- Méthodologie d'étude de conformité : périmètre, référentiel, preuves
- Revue documentaire et entretiens, cotation de la maturité
- Rédaction de la politique de sécurité des systèmes d'information (PSSI)
- Procédures de conformité : gestion des droits, sous-traitance, conservation des données
- Registre des traitements et analyse d'impact relative à la protection des données (AIPD)
- Construction du plan d'action de mise en conformité et suivi en amélioration continue

Fil rouge · Camille conduit l'étude d'écarts NIS2 d'Hydrelis, révise la PSSI devenue obsolète et lance l'analyse d'impact sur le traitement des données de télérelève des compteurs.

Cours 10 · Faire vivre la conformité : sensibilisation, suivi et gestion des non-conformités

22 h

OBJECTIFS

- Former et sensibiliser les collaborateurs avec des ressources accessibles et mesurer l'efficacité des actions
- Suivre la conformité, gérer les incidents de non-conformité et documenter les efforts réalisés

ÉVALUATION FORMATIVE

Mise en situation : gestion d'un incident de non-conformité et rédaction d'un rapport de conformité, préparatoires à l'épreuve du bloc

CONTENUS

- Concevoir un programme de formation et de sensibilisation aux exigences légales et normatives
- Accessibilité des supports pour les personnes en situation de handicap (sous-titrage, contraste, formats adaptés)
- Mesurer l'efficacité des campagnes de sensibilisation
- Indicateurs de conformité et programme d'audits internes réguliers
- Gestion des incidents de non-conformité et des violations de données, notification à l'autorité de contrôle
- Rapports de conformité à destination de la direction et des autorités
- Mise en œuvre et suivi des mesures correctives

Fil rouge · Une erreur d'envoi expose des factures clients d'Hydrelis : Camille qualifie la violation, prépare la notification dans les délais prévus par le RGPD, puis intègre l'événement dans son rapport de conformité semestriel.

RNCP39999BC04 · 66 h

Piloter un projet et communiquer en cybersécurité

Cours 11 · Cadrer un projet de cybersécurité et rédiger le cahier des charges

22 h

OBJECTIFS

- Identifier une problématique de cybersécurité à partir des besoins de l'organisation et d'une veille sur les solutions existantes
- Rédiger un cahier des charges normalisant le cadre de gestion et les livrables du projet

ÉVALUATION FORMATIVE

Exercice pratique : rédaction d'une note de cadrage et d'un cahier des charges, évalués sur grille

CONTENUS

- Formuler une problématique de sécurité : besoins métier, contraintes, enjeux
- Veille et benchmark des solutions du marché, critères de comparaison
- Note de cadrage et étude d'opportunité
- Structure d'un cahier des charges : exigences fonctionnelles, techniques et de sécurité
- Définition des livrables, critères d'acceptation et gouvernance du projet
- Prise en compte de l'accessibilité dans les exigences du projet

Fil rouge · Camille formule la problématique de détection tardive des incidents chez Hydrelis, compare les options SOC interne et SOC externalisé et rédige le cahier des charges du projet.

Cours 12 · Planifier, sécuriser et piloter le projet et son équipe

22 h

OBJECTIFS

- Concevoir un plan de gestion de projet définissant objectifs, calendrier, budget et livrables
- Identifier les risques du projet et piloter l'équipe par des techniques de communication et de leadership inclusives

ÉVALUATION FORMATIVE

Étude de cas : plan de gestion de projet complet avec registre des risques, complété par un QCM

CONTENUS

- Méthodes de gestion de projet : cycle en V, méthodes agiles, approches hybrides
- Planification : découpage, jalons, diagramme de Gantt, chemin critique
- Budget, ressources et suivi des coûts
- Analyse des risques projet et mesures de sécurité associées
- Pilotage de l'avancement : comités, indicateurs, gestion des écarts
- Leadership, communication d'équipe et gestion des conflits
- Prise en compte des situations de handicap dans l'organisation du travail de l'équipe

Fil rouge · Camille construit le planning et le budget du projet SOC d'Hydrelis, anticipe le risque d'indisponibilité de l'équipe réseau et adapte l'organisation des réunions pour un collaborateur malentendant.

Cours 13 · Communiquer, sensibiliser et restituer les résultats

22 h

OBJECTIFS

- Développer un plan de communication adapté aux parties prenantes et sensibiliser l'ensemble de l'organisation
- Synthétiser les résultats d'un projet dans un rapport écrit et une présentation orale accessibles

ÉVALUATION FORMATIVE

Mise en situation : soutenance blanche enregistrée d'un projet, évaluée sur la grille préparatoire à l'épreuve du bloc

CONTENUS

- Cartographie des parties prenantes et implication de la direction
- Construction d'un plan de communication projet
- Conception d'une campagne de sensibilisation : messages, formats, simulations d'hameçonnage
- Adaptation des supports et méthodes aux personnes en situation de handicap
- Rédaction d'un rapport de projet : structure, synthèse, indicateurs d'impact
- Préparation et conduite d'une soutenance orale convaincante et accessible

Fil rouge · Camille déploie une campagne de sensibilisation multi-format auprès des techniciens de terrain et du siège d'Hydrelis, puis présente le bilan du projet SOC au comité de direction.

RNCP39999BC05 · 44 h

Mener un audit de sécurité d'un système d'information (spécialisation)

Cours 14 · Construire le programme d'audit et préparer la mission

22 h

OBJECTIFS

- Définir un contrat et un programme d'audit en fixant le périmètre, les rôles et les responsabilités
- Mettre en place le système de suivi du programme d'audit et préparer les activités par la revue documentaire

ÉVALUATION FORMATIVE

Exercice pratique : rédaction d'un programme et d'un plan d'audit à partir d'un cas, complétée par un QCM

CONTENUS

- Typologie des audits : organisationnel, intrusif, réseau, vulnérabilités, code, conformité
- Lignes directrices de l'audit (ISO 19011) et référentiel d'exigences des prestataires d'audit de l'ANSSI
- Contrat d'audit, convention et autorisations, cadre juridique des tests
- Programme et plan d'audit : objectifs, périmètre, critères, calendrier
- Système de management du programme d'audit : analyse des résultats, gestion et conservation des enregistrements
- Revue documentaire et répartition des tâches au sein de l'équipe d'audit

Fil rouge · Devenue RSSI adjointe, Camille rédige le programme d'audit de la filiale récemment acquise par Hydrelis et la convention signée avec le cabinet chargé du test d'intrusion.

Cours 15 · Conduire, suivre et restituer l'audit de sécurité

22 h

OBJECTIFS

- Mettre en œuvre et suivre les activités d'audit, dont tests d'intrusion et évaluations de vulnérabilités
- Rédiger le rapport et la synthèse d'audit, puis présenter des conclusions objectives à la direction

ÉVALUATION FORMATIVE

Mise en situation : rédaction d'un rapport d'audit et soutenance blanche, préparatoires à l'épreuve du bloc

CONTENUS

- Méthodologie de test d'intrusion : reconnaissance, exploitation, post-exploitation
- Évaluation de vulnérabilités et audit de configuration : outils et techniques
- Suivi des activités : journal d'audit, communication avec l'audité, revue des informations produites
- Qualification des constats et cotation des vulnérabilités
- Rédaction du rapport d'audit et de la synthèse managériale
- Présentation des conclusions, indicateurs de maturité et recommandations

Fil rouge · Camille coordonne le test d'intrusion de la filiale, arbitre une découverte critique en cours de mission et présente au comité d'audit d'Hydrelis une synthèse de maturité assortie de recommandations.

RNCP39999BC06 · 66 h

Opérer et surveiller les mesures de sécurité d'un SI (spécialisation)

Cours 16 · Déployer un système de surveillance de la sécurité

22 h

OBJECTIFS

- Déployer une chaîne de collecte et de détection des événements de sécurité
- Intégrer la détection dans un processus de gestion d'incident en tenant compte des utilisateurs en situation de handicap

ÉVALUATION FORMATIVE

Exercice pratique : conception d'une architecture de collecte et de trois règles de détection documentées

CONTENUS

- Organisation et missions d'un SOC
- Sources de journaux : systèmes, réseau, applications, cloud
- Architecture et déploiement d'un SIEM sur une infrastructure web
- Conception de cas d'usage et de règles de détection
- Indicateurs de supervision et tableaux de bord
- Accessibilité des consoles, alertes et procédures pour les opérateurs et utilisateurs en situation de handicap

Fil rouge · Camille raccorde au SIEM les journaux de l'annuaire, du portail client et des passerelles industrielles d'Hydrelis, puis définit les premiers cas d'usage de détection.

Cours 17 · Concevoir le processus de gestion des incidents et qualifier les alertes

22 h

OBJECTIFS

- Concevoir un processus et un flux de traitement des incidents conforme à la norme ISO 27035
- Identifier, classifier et prioriser les alertes issues des outils SIEM, XDR, EDR et IDS

ÉVALUATION FORMATIVE

Étude de cas : modélisation d'un processus ISO 27035 et priorisation d'un lot d'alertes, complétées par un QCM

CONTENUS

- La norme ISO 27035 : phases et principes de la gestion des incidents
- Modélisation du flux de traitement des événements et des incidents
- Typologie des alertes par outil : SIEM, EDR, XDR, IDS
- Classification et priorisation selon criticité et impact
- Automatisation du traitement : playbooks et orchestration (SOAR)
- Rôles, escalade et interfaces avec les métiers et la direction

Fil rouge · Confrontée à un afflux d'alertes peu qualifiées, Camille construit la grille de classification d'Hydrelis et automatise le traitement des alertes de connexion suspecte sur le portail client.

Cours 18 · Traiter les incidents et éprouver la résilience

22 h

OBJECTIFS

- Définir une stratégie et un plan de traitement des incidents cohérents avec les dispositifs PRA/PCA
- Suivre le traitement des incidents et vérifier l'efficacité de la stratégie par des tests réguliers

ÉVALUATION FORMATIVE

Simulation d'incident : rédaction du plan de traitement et du retour d'expérience, préparatoires à l'épreuve du bloc

CONTENUS

- Stratégie de traitement des incidents et articulation avec le PRA et le PCA
- Analyse d'impact et identification des sous-systèmes touchés
- Plan de résolution : confinement, éradication, restauration
- Fondamentaux de l'investigation numérique et préservation des preuves
- Indicateurs d'efficacité du traitement et retour d'expérience
- Exercices de crise et tests du PRA/PCA
- Intégration des enseignements dans l'amélioration continue

Fil rouge · Camille dirige le traitement d'une compromission du portail client d'Hydrelis, documente le plan de résolution, puis organise un exercice de crise testant le PRA du site de supervision.

RNCP39999BC07 · 44 h

Intégrer des outils de sécurité dans un environnement hétérogène (spécialisation)

Cours 19 · Analyser un environnement hétérogène avant intégration

22 h

OBJECTIFS

- Identifier les actifs matériels, logiciels et humains ainsi que les interconnexions des sous-systèmes (SCADA, IoT, cloud)
- Évaluer les impacts d'une mise en production pour éviter régressions et pannes

ÉVALUATION FORMATIVE

Étude de cas : dossier d'analyse d'environnement et de stratégie de déploiement, complété par un QCM

CONTENUS

- Spécificités des environnements industriels, IoT et cloud
- Inventaire des actifs et des compétences humaines nécessaires à l'intégration
- Analyse des interconnexions et des flux entre sous-systèmes
- Modèles de référence pour les systèmes industriels (zones et conduits)
- Stratégie de déploiement en environnement hybride
- Analyse d'impact de mise en production : tests, recette, plan de retour arrière

Fil rouge · Camille recense les automates, capteurs et passerelles cloud des microcentrales d'Hydrelis et identifie les créneaux d'intervention compatibles avec la continuité de production.

Cours 20 · Déployer, superviser et contrôler les solutions de sécurité

22 h

OBJECTIFS

- Intégrer des mesures et services de sécurité interopérables dans un système hybride en respectant les contraintes métiers
- Mettre en place le contrôle des flux et mesurer l'efficacité des solutions déployées

ÉVALUATION FORMATIVE

Mise en situation : proposition argumentée de solutions de sécurité pour une infrastructure hétérogène, préparatoire à l'épreuve du bloc

CONTENUS

- Panorama des solutions : pare-feu, IDS, XDR, WAF, NAC, diode de données
- Intégration en cloud privé et public, hyperviseurs et containers
- Segmentation et cloisonnement pour limiter la propagation d'une attaque
- Sécurité de la chaîne d'approvisionnement et des prestataires
- Contrôle et surveillance des flux sous contraintes métiers
- Indicateurs d'efficacité et audits réguliers des mesures

Fil rouge · Camille installe une diode de données entre le SCADA d'une microcentrale et le cloud d'Hydrelis, déploie un NAC sur les sous-stations et définit les indicateurs de contrôle des flux.

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 actifs informationnels et évaluer leur criticité	RNCP39999BC01	1
Identifier les sources de menaces et déterminer leur probabilité	RNCP39999BC01	1
Évaluer les scénarios stratégiques et opérationnels (EBIOS RM)	RNCP39999BC01	1, 2
Estimer l'impact potentiel des risques	RNCP39999BC01	2
Classifier et prioriser les risques	RNCP39999BC01	2
Élaborer des stratégies de traitement des risques	RNCP39999BC01	3
Mettre en œuvre le plan de traitement des risques	RNCP39999BC01	3
Suivre et réévaluer les risques en continu	RNCP39999BC01	3
Proposer un plan de remédiation	RNCP39999BC01	3
Cartographier un système d'information	RNCP39999BC02	4
Mettre en place un système de veille menaces et vulnérabilités	RNCP39999BC02	4
Évaluer la pertinence des solutions de sécurité	RNCP39999BC02	5, 7
Mettre en œuvre des mesures de durcissement du SI	RNCP39999BC02	5
Définir les paramètres de sécurité des composants logiques	RNCP39999BC02	6
Classifier les données sensibles et contrôler les usages	RNCP39999BC02	7
Appliquer des mesures de sécurité sur les données	RNCP39999BC02	7
Identifier les lois, règlements et normes applicables	RNCP39999BC03	8
Évaluer la conformité actuelle des pratiques	RNCP39999BC03	9
Développer des politiques et procédures de conformité	RNCP39999BC03	9
Mettre en œuvre les mesures de conformité	RNCP39999BC03	9, 10
Former et sensibiliser les employés aux exigences légales et normatives	RNCP39999BC03	10
Suivre la conformité de manière continue	RNCP39999BC03	10
Gérer les incidents de non-conformité	RNCP39999BC03	10
Documenter et communiquer les efforts de conformité	RNCP39999BC03	10
Identifier une problématique en cybersécurité	RNCP39999BC04	11
Rédiger un cahier des charges du projet	RNCP39999BC04	11

Concevoir un plan de gestion de projet	RNCP39999BC04	12
Identifier les risques liés au projet	RNCP39999BC04	12
Assurer le suivi de l'équipe projet	RNCP39999BC04	12
Sensibiliser les membres de l'organisation aux enjeux de la cybersécurité	RNCP39999BC04	13
Développer un plan de communication adapté aux parties prenantes	RNCP39999BC04	13
Synthétiser et présenter les résultats de la démarche	RNCP39999BC04	13
Définir un contrat et un programme d'audit	RNCP39999BC05	14
Définir un système de management de suivi du programme d'audit	RNCP39999BC05	14
Préparer les activités d'audit	RNCP39999BC05	14
Mettre en œuvre les activités d'audit (tests d'intrusion, vulnérabilités)	RNCP39999BC05	15
Suivre les activités d'audit	RNCP39999BC05	15
Élaborer les documents de restitution de l'audit	RNCP39999BC05	15
Présenter les conclusions de l'audit	RNCP39999BC05	15
Déployer un système de surveillance de la sécurité	RNCP39999BC06	16
Concevoir un processus de traitement des incidents (ISO 27035)	RNCP39999BC06	17
Identifier et classifier les alertes (SIEM, XDR, EDR, IDS)	RNCP39999BC06	17
Définir une stratégie de traitement des incidents (PRA/PCA)	RNCP39999BC06	18
Définir un plan de traitement d'un incident	RNCP39999BC06	18
Suivre le traitement des incidents	RNCP39999BC06	18
Vérifier l'efficacité de la stratégie de traitement des incidents	RNCP39999BC06	18
Identifier les actifs nécessaires à l'intégration d'une solution de sécurité	RNCP39999BC07	19
Identifier les interconnexions des sous-systèmes	RNCP39999BC07	19
Identifier les impacts de la mise en production d'une solution	RNCP39999BC07	19
Mettre en œuvre des stratégies de déploiement interopérables	RNCP39999BC07	20
Intégrer des mesures de sécurité dans un système hybride	RNCP39999BC07	20
Mettre en place le contrôle et la surveillance des flux	RNCP39999BC07	20
Contrôler l'efficacité des mesures et services de sécurité	RNCP39999BC07	20

Évaluations formatives

Chaque sous-chapitre se conclut par un QCM de validation des acquis permettant à l'apprenant de se positionner et au formateur de suivre la progression. Chaque cours comporte une mise en situation dans le fil rouge Hydrelis Énergies, donnant lieu à une production évaluée sur grille critériée : registre,

cartographie, rapport, plan d'action, fiche de paramétrage ou soutenance enregistrée selon le cours. Le dernier cours de chaque bloc propose une évaluation préparatoire construite sur le format de l'épreuve de certification correspondante. Les résultats sont tracés sur la plateforme et exploitables par l'organisme de formation pour ses bilans de progression.

Modalités de certification

Bloc	Modalité d'évaluation
RNCP39999BC01	Mise en situation professionnelle, analyse de risque d'un SI : à partir de la documentation d'une entreprise réelle ou fictive (activité, ressources, système d'information), le candidat réalise et présente une analyse de risque adaptée aux besoins et contraintes de l'organisation et propose un plan de traitement des risques.
RNCP39999BC02	Mise en situation professionnelle, renforcer la sécurité technique d'un SI : à partir du système d'information d'une organisation réelle ou fictive (schéma d'infrastructure, caractéristiques techniques, registre des données, cahier des charges), le candidat propose un plan d'action de sécurisation conforme aux normes et standards applicables à l'activité et au cahier des charges.
RNCP39999BC03	Mise en situation professionnelle, étude de conformité légale, réglementaire ou normative : le candidat présente un projet d'étude de conformité mené de bout en bout sur la sécurité des données personnelles ou des systèmes d'information, au regard d'une loi, d'une réglementation ou d'une norme.
RNCP39999BC04	Mise en situation professionnelle, gestion de projet en cybersécurité : le candidat, seul ou en groupe, mène un projet répondant à une problématique de cybersécurité qu'il choisit et clairement définie ; l'évaluation finale prend la forme d'une soutenance présentant les résultats et l'impact du projet au regard de la problématique initiale.
RNCP39999BC05	Mise en situation professionnelle, réalisation d'un audit de sécurité : à partir des données mises à disposition sur une organisation réelle ou fictive, le candidat réalise un audit (organisationnel, intrusif, réseau, de vulnérabilités, de code ou de conformité), produit un rapport conforme au plan d'audit donnant une vision claire de la maturité de l'organisation et le défend lors d'une soutenance orale.
RNCP39999BC06	Mise en situation professionnelle, mise en œuvre d'un SOC : à partir de l'étude d'une organisation réelle ou fictive, le candidat crée une preuve de concept comprenant une infrastructure web avec un SIEM déployé, des indicateurs, des processus et procédures de résolution d'incidents établis, suivis et évalués ; le système est testé par la simulation d'un incident de sécurité.
RNCP39999BC07	Mise en situation professionnelle, intégration d'un outil de sécurité : à partir d'une infrastructure hétérogène réelle ou fictive (industrielle, logistique, IoT embarqué), le candidat propose et met en œuvre des solutions de sécurité (pare-feu, IDS, XDR, WAF, NAC, diode de données) pour renforcer la sécurité du traitement et des échanges d'informations.

Le parcours reproduit, cours après cours, les productions attendues aux épreuves : analyse de risques EBIOS RM, plan de sécurisation technique, étude de conformité, projet soutenu, rapport d'audit, preuve de concept de SOC et dossier d'intégration. Le fil rouge Hydrelis Énergies fournit à l'apprenant une organisation documentée sur laquelle s'entraîner avant de traiter le cas proposé lors de la certification. Les évaluations préparatoires de fin de bloc utilisent des grilles alignées sur les compétences du référentiel. Les trois blocs de spécialisation (BC05, BC06, BC07) sont tous couverts : l'organisme de formation sélectionne celui ou ceux correspondant au parcours de certification de ses apprenants. SFM

fournit le contenu pédagogique ; l'organisme de formation reste responsable de l'inscription, de l'organisation et du passage de la certification auprès du certificateur.

Moyens pédagogiques et débouchés

Moyens pédagogiques et techniques

- Plateforme e-learning en marque blanche accessible 24h/24, avec suivi de progression, traçabilité des connexions et des résultats exploitables pour Qualiopi
- Une vidéo de 3 à 5 minutes par sous-chapitre, représentant 30 % du volume horaire (132 heures sur 440), sous-titrée pour l'accessibilité
- Cours texte enrichi, infographies et fiches méthodes téléchargeables (EBIOS RM, ISO 27035, plan d'audit, cahier des charges)
- Études de cas et mises en situation dans le fil rouge Hydrelis Énergies, avec dossiers documentaires réalistes (schémas d'infrastructure, registres, journaux d'événements)
- QCM de validation par sous-chapitre et grilles critériées d'évaluation des productions
- Modèles de livrables professionnels : registre des actifs, matrice des risques, PSSI, rapport d'audit, plan de traitement d'incident
- Supports conçus selon des principes d'accessibilité numérique (contrastes, structure, formats alternatifs) pour les apprenants en situation de handicap

Débouchés et évolutions

- Responsable de la sécurité des systèmes d'information (RSSI)
- Consultant en cybersécurité
- Chef de projet cybersécurité
- Responsable d'audit de sécurité ou pentester
- Opérateur de sécurité (analyste SOC) ou analyste DFIR
- Intégrateur de solutions de sécurité ou architecte de la sécurité des 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 RNCP39999 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.