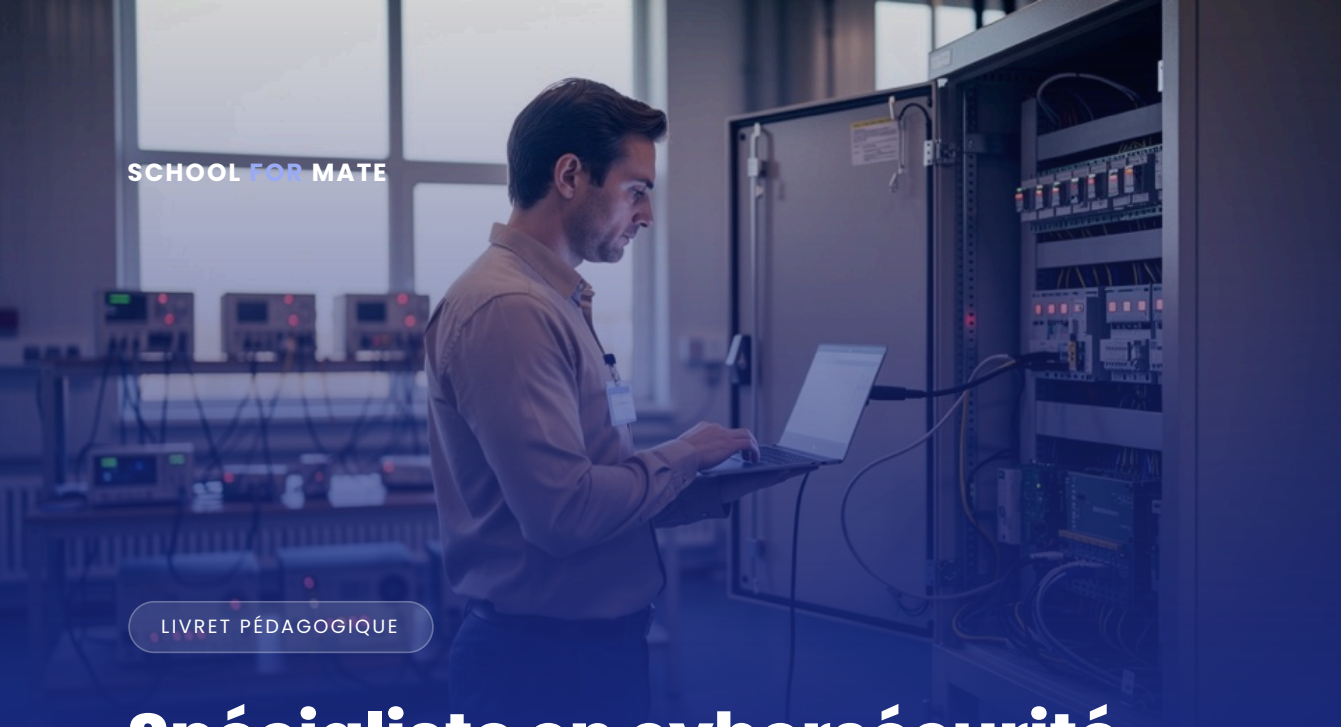


SCHOOL FOR MATE

LIVRET PÉDAGOGIQUE

Spécialiste en cybersécurité (MS)

RNCP38434 · Certification RNCP · Niveau 7

Ce parcours de 440 heures prépare les futurs spécialistes en cybersécurité à construire, piloter et faire vivre la sécurité d'un système d'information, de la gouvernance du SMSI jusqu'aux tests d'intrusion et à la continuité d'activité. Construit bloc par bloc sur le référentiel RNCP38434 (niveau 7), il suit le quotidien d'une responsable cybersécurité au sein d'un industriel ferroviaire fictif. Chaque cours correspond ainsi à une situation professionnelle réelle.

VOLUME HORAIRE	COURS	BLOCS
440 h	**20**	**3**

01 · PRÉSENTATION

La formation en bref

Intitulé	Spécialiste en cybersécurité (MS)
Code	RNCP38434
Type	Certification RNCP
Niveau	Niveau 7
Certificateur	INSTITUT NATIONAL SCIENCES APPLIQUEES LYON
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	21/12/2028

Le métier et les compétences visées

Le spécialiste en cybersécurité conçoit ou améliore les fonctions de sécurité d'un système d'information afin de protéger les actifs informationnels d'une organisation contre les malveillances. Il définit la stratégie de gouvernance de la sécurité, met en place et pilote le SMSI, apprécie les risques selon la méthode EBIOS RM et structure la gestion des identités et des accès. Il conçoit des architectures de sécurité adaptées aux réseaux, systèmes et applications, et intègre la sécurité dans le développement de produits industriels complexes. Interlocuteur privilégié de la DG, de la DSI et des métiers, il organise des tests d'intrusion et des analyses forensiques. Il garantit enfin la continuité de service grâce aux dispositifs PCA et PRA.

Public visé

- Ingénieurs et titulaires d'un Bac+5 en informatique, réseaux ou systèmes souhaitant se spécialiser en cybersécurité
- Administrateurs systèmes et réseaux, ingénieurs d'exploitation ou développeurs expérimentés visant un poste d'expert ou de pilote sécurité
- Chefs de projet SI et consultants en maîtrise d'ouvrage souhaitant évoluer vers le conseil, l'audit ou la gouvernance cybersécurité
- Professionnels de l'industrie (ferroviaire, aéronautique, énergie) chargés de la sécurité de produits ou de systèmes embarqués
- Personnes en reconversion justifiant d'une expérience significative, admises par une procédure de validation des acquis personnels et professionnels

Prérequis

- Être titulaire d'un diplôme d'ingénieur habilité CTI, d'un diplôme d'école de management conférant le grade de Master, d'un diplôme Bac+5 ou d'un titre RNCP de niveau 7, ou d'un diplôme étranger équivalent
- Ou être titulaire d'un M1 ou équivalent et justifier d'au moins trois années d'expérience professionnelle
- Par dérogation, dans les limites fixées par le règlement de la Conférence des Grandes Écoles : justifier d'au moins 5 années d'expérience professionnelle après une procédure de VAPP, ou être titulaire d'un M1 sans expérience, ou d'une L3 avec au moins 3 ans d'expérience adaptée
- Maîtriser les fondamentaux des réseaux, des systèmes d'exploitation et des architectures applicatives. Les conditions d'admission définitives relèvent de l'établissement certificateur.

Objectifs pédagogiques

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

- Définir le périmètre et la politique de sécurité d'un SMSI conforme à l'ISO/IEC 27001, validés par la direction générale

- Conduire une appréciation des risques selon la méthode EBIOS RM et établir un plan de traitement des risques assorti de seuils d'acceptabilité
- Sélectionner, budgéter et piloter des mesures de sécurité techniques et organisationnelles, puis mesurer leur efficacité à l'aide d'indicateurs
- Concevoir et piloter une architecture de gestion des identités et des accès (IAM, SSO, fédération, PAM) et le cycle de vie des habilitations
- Concevoir une architecture de sécurité d'infrastructure durable et conforme aux exigences réglementaires, puis la défendre auprès d'un donneur d'ordre
- Intégrer la sécurité dans le cycle de développement d'un produit industriel complexe et dans sa chaîne d'approvisionnement
- Planifier et réaliser des tests d'intrusion et des audits techniques, puis rédiger un rapport de vulnérabilités exploitable par les métiers
- Mener une analyse post-mortem en respectant les exigences des différents types d'investigation
- Élaborer, organiser et maintenir en condition opérationnelle un PCA/PRA fondé sur une analyse d'impact métier

02 · FIL ROUGE PÉDAGOGIQUE

Alvéon Mobilité

CR

Camille Rousseau

Cheffe de projet cybersécurité, puis RSSI adjointe

Industrie ferroviaire : conception et fabrication de systèmes de signalisation et d'équipements embarqués pour trains régionaux

Alvéon Mobilité est une entreprise de taille intermédiaire d'environ 1 800 salariés, implantée sur trois sites en Auvergne-Rhône-Alpes. Elle conçoit des calculateurs embarqués et des systèmes de signalisation pour les exploitants ferroviaires européens. Sa croissance rapide s'est faite par l'acquisition d'une PME de maintenance, ce qui a hérité d'un système d'information hétérogène : annuaires multiples, applications métier non documentées, sauvegardes peu testées. Un client exploitant exige désormais une démarche de sécurité formalisée sur les produits livrés. Un incident de rançongiciel évité de justesse sur un poste d'atelier a par ailleurs alerté la direction générale. Camille Rousseau, ingénieure réseaux de formation, est recrutée pour structurer la cybersécurité de l'entreprise. Elle rapporte au DSI, Olivier Marchand, et travaille avec la direction produit, les responsables d'usine et les achats.

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 cadre le SMSI d'Alvéon Mobilité, conduit l'analyse EBIOS RM avec les métiers, fait valider le plan de traitement par la direction et lance le chantier IAM pour unifier les identités issues de l'acquisition.
2. Bloc 2 : Camille conçoit la nouvelle architecture de sécurité des usines et du SI de gestion, convainc le comité de direction de la financer et intègre la sécurité dans le développement du nouveau calculateur embarqué ainsi que chez les fournisseurs.
3. Bloc 3 : devenue RSSI adjointe, Camille pilote une campagne de tests d'intrusion et l'analyse forensique d'un incident, puis bâtit et éprouve le PCA/PRA de l'entreprise lors d'un exercice de crise.

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
RNCP38434BC01 · Elaborer la stratégie et gouvernance de la sécurité de l'information		**154 h**
1	Cadrer le SMSI : contexte, périmètre et politique de sécurité	22 h
2	Apprécier les risques avec la méthode EBIOS Risk Manager	22 h
3	Choisir et déployer les mesures de sécurité techniques et organisationnelles	22 h
4	Piloter et améliorer en continu le SMSI	22 h
5	Cartographier les accès et concevoir les modèles d'autorisation	22 h
6	Gérer le cycle de vie des identités et analyser les habilitations	22 h
7	Concevoir une architecture IAM et piloter le projet	22 h
RNCP38434BC02 · Concevoir et mettre en service d'infrastructures de cybersécurité		**132 h**
8	Concevoir une architecture de sécurité d'infrastructure	22 h
9	Intégrer et déployer les solutions de sécurité du marché	22 h
10	Convaincre un donneur d'ordre et piloter un projet de sécurisation	22 h
11	Intégrer la sécurité dans le développement d'un produit industriel	22 h
12	Analyser le code et évaluer le niveau de sécurité d'un produit	22 h
13	Maintenir la sécurité du produit et sécuriser la supply chain	22 h
RNCP38434BC03 · Maintenir en continuité de service		**154 h**
14	Cadrer un test d'intrusion et mener la reconnaissance	22 h
15	Réaliser des tests d'intrusion et des audits techniques	22 h
16	Rédiger le rapport de vulnérabilités et piloter les campagnes de tests	22 h
17	Mener une analyse post-mortem (forensic)	22 h
18	Identifier les applications critiques et définir la continuité de service	22 h
19	Organiser la gestion de crise et l'équipe PCA/PRA	22 h
20	Maintenir le PCA/PRA en condition opérationnelle et piloter le projet	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

RNCP38434BC01 · 154 h

Elaborer la stratégie et gouvernance de la sécurité de l'information

Cours 1 · Cadrer le SMSI : contexte, périmètre et politique de sécurité

22 h

OBJECTIFS

- Établir le contexte de l'organisation et définir le périmètre du SMSI selon l'ISO/IEC 27001
- Recenser les actifs informationnels et les biens supports concernés par l'appréciation des risques
- Rédiger une politique de sécurité de l'information et la faire valider par la direction générale

ÉVALUATION FORMATIVE

QCM de validation des acquis et rédaction commentée d'un extrait de PSSI à partir du cas Alvéon Mobilité

CONTENUS

- Panorama de la gouvernance cybersécurité : rôles du RSSI, de la DSI, de la DG et des métiers
- Famille ISO/IEC 27000 : structure de l'ISO/IEC 27001 et articulation avec l'ISO/IEC 27002
- Cadre réglementaire applicable : RGPD, directive NIS 2, exigences sectorielles
- Analyse du contexte interne et externe, des parties intéressées et de leurs attentes
- Définition du périmètre et déclaration d'applicabilité
- Inventaire et valorisation des actifs informationnels et des biens supports
- Rédaction de la PSSI et des principes d'action, circuit de validation par la direction
- Organisation de la gouvernance : comité sécurité, feuille de route de mise en œuvre du SMSI

Fil rouge · Camille arrive chez Alvéon Mobilité et doit présenter au comité de direction, sous trois semaines, une note de cadrage du SMSI. Celle-ci précise le périmètre retenu (bureau d'études et SI de gestion) et un premier inventaire des actifs.

Cours 2 · Apprécier les risques avec la méthode EBIOS Risk Manager

22 h

OBJECTIFS

- Conduire les cinq ateliers de la méthode EBIOS RM sur un périmètre défini
- Définir les seuils d'acceptabilité des risques en cohérence avec la politique de sécurité
- Établir un plan de traitement des risques conforme au cadre normatif

ÉVALUATION FORMATIVE

Étude de cas : production d'une cartographie des risques et d'un plan de traitement, autocorrigée à l'aide d'une grille critériée

CONTENUS

- Fondamentaux de la gestion des risques : ISO/IEC 27005 et ISO 31000
- Atelier 1 de la méthode EBIOS RM : socle de sécurité, valeurs métier et événements redoutés
- Atelier 2 : sources de risques et objectifs visés
- Atelier 3 : scénarios stratégiques et cartographie de l'écosystème
- Atelier 4 : scénarios opérationnels et évaluation de la vraisemblance
- Atelier 5 : stratégie de traitement, seuils d'acceptabilité et risques résiduels
- Animation des ateliers avec les métiers et restitution à la direction

Fil rouge · Camille anime avec la direction produit et la direction industrielle les ateliers EBIOS RM sur le bureau d'études. Elle doit faire arbitrer par la DG les seuils d'acceptabilité du risque de vol de propriété intellectuelle.

Cours 3 · Choisir et déployer les mesures de sécurité techniques et organisationnelles

22 h

OBJECTIFS

- Sélectionner les mesures de sécurité adaptées aux risques à traiter
- Allouer les moyens budgétaires et humains nécessaires à leur mise en œuvre
- Planifier et suivre le déploiement effectif des mesures

ÉVALUATION FORMATIVE

Mise en situation : élaboration d'un plan d'action budgété et QCM sur les mesures de l'ISO/IEC 27002

CONTENUS

- Catalogue des mesures de l'ISO/IEC 27002 : organisationnelles, humaines, physiques et technologiques
- Guides de bonnes pratiques de l'ANSSI : hygiène informatique et mesures prioritaires
- Du plan de traitement au plan d'action : priorisation par le risque et par le coût
- Construction d'un budget sécurité : investissement, fonctionnement, ressources internes et externes
- Sensibilisation et accompagnement au changement des collaborateurs
- Pilotage du déploiement : jalons, responsabilités, suivi de l'avancement
- Gestion des prestataires et des exigences contractuelles de sécurité

Fil rouge · À partir du plan de traitement validé, Camille doit construire un plan d'action sur 18 mois et défendre l'enveloppe budgétaire associée devant le DSI Olivier Marchand. Elle dispose d'un effectif limité à deux ingénieurs.

Cours 4 · Piloter et améliorer en continu le SMSI

22 h

OBJECTIFS

- Mettre en place des indicateurs de sécurité pertinents et un tableau de bord de pilotage
- Organiser l'audit interne et la revue de direction dans une logique d'amélioration continue
- Piloter les projets SMSI en mobilisant leadership, communication et gestion des délais et budgets

ÉVALUATION FORMATIVE

Production d'un tableau de bord d'indicateurs commenté et quiz de mise en situation sur la revue de direction

CONTENUS

- Cycle PDCA appliqué au SMSI : surveillance, mesure, analyse et évaluation
- Conception d'indicateurs techniques, financiers et organisationnels
- Tableau de bord sécurité à destination de la direction générale
- Audit interne du SMSI : programme, conduite, constats et non-conformités
- Revue de direction et actions correctives
- Évaluation de la maturité cybersécurité et alignement avec la stratégie de l'entreprise
- Conduite de projet SMSI : gestion des parties prenantes, du stress, des délais et du budget
- Communication orale et écrite : synthèse pour la direction, animation d'équipe inclusive

Fil rouge · Six mois après le lancement, Camille prépare la première revue de direction du SMSI. Elle doit présenter un tableau de bord d'indicateurs et proposer un réajustement de la feuille de route après un retard du chantier de sensibilisation.

Cours 5 · Cartographier les accès et concevoir les modèles d'autorisation

22 h

OBJECTIFS

- Réaliser un audit préalable de l'ensemble des accès internes, cloud et fédérés aux actifs
- Concevoir un modèle de contrôle d'accès et une matrice des rôles avec les managers métier

ÉVALUATION FORMATIVE

Cas pratique : réalisation d'une matrice des rôles et identification des conflits de séparation des tâches

CONTENUS

- Enjeux de la gestion des identités et des accès dans la gouvernance de la sécurité
- Méthodologie d'audit des accès auprès des responsables d'application
- Environnements utilisateurs : annuaires internes, services cloud, identités fédérées et partenaires
- Modèles de contrôle d'accès : DAC, MAC, RBAC, ABAC
- Construction d'une matrice des rôles et séparation des tâches
- Gouvernance des autorisations et responsabilités des directions métier
- Gestion de l'évolution des accès : mobilité interne, arrivées, départs

Fil rouge · L'acquisition de la PME de maintenance a laissé deux annuaires et de nombreux comptes partagés. Camille conduit des entretiens avec les responsables d'application pour cartographier les accès, puis construit avec le directeur des achats la première matrice des rôles.

Cours 6 · Gérer le cycle de vie des identités et analyser les habilitations

22 h

OBJECTIFS

- Organiser le provisionnement, le dé-provisionnement et les revues des accès
- Analyser les données d'identités et d'habilitations à l'aide d'un outillage logiciel pour les faire évoluer

ÉVALUATION FORMATIVE

Exercice d'analyse d'un jeu de données d'habilitations fictif et QCM sur le cycle de vie des identités

CONTENUS

- Cycle de vie des identités : création, modification, suspension, suppression
- Processus de provisionnement et de dé-provisionnement automatisés
- Comptes de service, comptes techniques et comptes d'accès système
- Campagnes de revue des accès : périmètre, fréquence, certification par les managers
- Outils de gouvernance des identités (IGA) : fonctions et critères d'évaluation
- Analyse des habilitations : détection des comptes orphelins, des droits excessifs et des anomalies
- Rôle mining et rationalisation des profils applicatifs

Fil rouge · Camille lance la première campagne de revue des accès sur l'ERP d'Alvéon Mobilité. L'analyse des extractions révèle des comptes d'anciens salariés encore actifs, et elle doit proposer un processus de dé-provisionnement fiable avec les ressources humaines.

Cours 7 · Concevoir une architecture IAM et piloter le projet

22 h

OBJECTIFS

- Choisir une solution IAM adaptée au contexte et aux besoins de l'organisation
- Concevoir l'architecture technique et fonctionnelle (SSO, fédération, gestion des comptes à privilèges)
- Piloter le projet IAM en maîtrisant délais, budget et relations avec les parties prenantes

ÉVALUATION FORMATIVE

Rendu d'un schéma d'architecture IAM argumenté et d'un planning projet, accompagné d'un QCM sur les protocoles de fédération

CONTENUS

- Architecture IAM de référence : annuaire, référentiel d'identités, moteur de provisionnement
- Authentification forte et authentification multifacteur
- Single Sign-On et protocoles de fédération : SAML, OAuth 2.0, OpenID Connect
- Gestion des comptes à privilèges (PAM) : coffre-fort, bastion, traçabilité
- Expression de besoin, cahier des charges et choix de solution
- Déploiement progressif et conduite du changement auprès des utilisateurs
- Pilotage du projet IAM : planning, budget, comité de suivi, communication

Fil rouge · Le DSI demande à Camille de recommander une solution IAM unifiant les deux annuaires et intégrant un bastion pour les administrateurs. Elle doit rédiger le cahier des charges, comparer trois offres fictives et planifier le déploiement.

RNCP38434BC02 · 132 h

Concevoir et mettre en service d'infrastructures de cybersécurité

Cours 8 · Concevoir une architecture de sécurité d'infrastructure

22 h

OBJECTIFS

- Concevoir une architecture de sécurité intégrant contraintes techniques, organisationnelles, réglementaires et financières
- Garantir la durabilité, la performance et l'évolutivité de l'architecture

ÉVALUATION FORMATIVE

Cas pratique : production d'un dossier d'architecture cible et auto-évaluation à l'aide d'une grille de critères

CONTENUS

- Principes d'architecture sécurisée : défense en profondeur, moindre privilège, zero trust
- Segmentation et cloisonnement des réseaux : zones, DMZ, réseaux d'administration
- Sécurité des systèmes et durcissement des serveurs et postes de travail
- Sécurité des applications et des environnements cloud et hybrides
- Spécificités des systèmes industriels (OT) et cloisonnement IT/OT selon l'IEC 62443
- Exigences réglementaires et recommandations de l'ANSSI pour les architectures
- Dossier d'architecture : choix, alternatives, coûts et trajectoire d'évolution

Fil rouge · Les usines d'Alvéon Mobilité partagent le même réseau que les bureaux. Camille conçoit une architecture cible qui cloisonne les réseaux industriels, sécurise les accès des mainteneurs et reste compatible avec le budget validé.

Cours 9 · Intégrer et déployer les solutions de sécurité du marché

22 h

OBJECTIFS

- Organiser une veille technologique approfondie sur les équipements et solutions de sécurité
- Intégrer des solutions de sécurité en maîtrisant les techniques de déploiement et de migration

ÉVALUATION FORMATIVE

Étude de cas sur un plan de migration et QCM sur les familles de solutions de sécurité

CONTENUS

- Méthodes et sources de veille technologique et de veille sur les menaces
- Familles de solutions : pare-feu, passerelles, EDR, SIEM, sondes de détection, chiffrement
- Critères de choix : qualification et certification des produits, interopérabilité, coût total
- Supervision de la sécurité et centralisation des journaux
- Stratégies de déploiement : maquette, pilote, généralisation
- Migration d'un existant sans interruption de service et plan de retour arrière
- Conformité réglementaire lors du déploiement et documentation d'exploitation

Fil rouge · Camille doit remplacer les pare-feu vieillissants des usines et déployer une solution de supervision. Elle prépare un plan de migration qui évite tout arrêt de la ligne de production pendant la bascule.

Cours 10 · Convaincre un donneur d'ordre et piloter un projet de sécurisation

22 h

OBJECTIFS

- Argumenter un projet de sécurisation pour obtenir les ressources budgétaires et humaines nécessaires
- Piloter un projet de conception et de mise en œuvre de fonctions de sécurité avec des équipes pluridisciplinaires

ÉVALUATION FORMATIVE

Préparation d'un support de présentation et d'un pitch argumenté, évalués par une grille de critères oraux

CONTENUS

- Identifier les attentes et les contraintes du donneur d'ordre : DG, DSI, chef de projet, autorité
- Construire un dossier d'opportunité : risques couverts, coûts, bénéfices, scénarios d'investissement
- Techniques de présentation et d'argumentation à destination de non-spécialistes
- Gestion des objections et négociation des arbitrages
- Méthodes de conduite de projet : cycle en V, approches agiles, gestion hybride
- Pilotage des délais, des coûts et des risques projet
- Leadership, travail en équipe inclusive et communication écrite dans un projet sécurité

Fil rouge · Camille présente au comité de direction le projet de sécurisation des usines. Face à un directeur financier réticent, elle doit défendre le budget en reliant chaque investissement aux risques identifiés par l'analyse EBIOS RM.

Cours 11 · Intégrer la sécurité dans le développement d'un produit industriel

22 h

OBJECTIFS

- Réaliser les études de sécurité d'un produit industriel complexe
- Intégrer l'analyse de risque, la réduction des risques et l'évaluation dans le cycle de développement du produit

ÉVALUATION FORMATIVE

Cas pratique : rédaction d'un extrait de spécification d'exigences de sécurité produit et QCM sur les référentiels sectoriels

CONTENUS

- Spécificités de la sécurité des produits industriels complexes : ferroviaire, aéronautique, automobile
- Référentiels sectoriels : IEC 62443, CLC/TS 50701 pour le ferroviaire, ED-202A/DO-326A pour l'aéronautique
- Articulation entre sûreté de fonctionnement et cybersécurité
- Analyse de risque produit et définition des niveaux de sécurité cibles
- Exigences de sécurité et fonctions de sécurité permettant une exploitation sûre par l'utilisateur
- Intégration des activités de sécurité dans chaque phase du cycle de développement
- Plan de management de la sécurité produit

Fil rouge · La direction produit lance un nouveau calculateur embarqué pour trains régionaux. Camille rejoint l'équipe projet pour conduire l'analyse de risque produit et traduire ses résultats en exigences de sécurité intégrées aux spécifications.

Cours 12 · Analyser le code et évaluer le niveau de sécurité d'un produit

22 h

OBJECTIFS

- Mettre en œuvre des méthodologies adaptées, dont l'analyse de code, pour mettre en conformité le niveau de sécurité du produit
- Évaluer le niveau de maturité à chaque étape et établir les risques résiduels à l'issue de l'intégration finale

ÉVALUATION FORMATIVE

Exercice d'interprétation d'un rapport d'analyse de code fictif et rédaction d'une synthèse des risques résiduels

CONTENUS

- Développement sécurisé : règles de codage et vulnérabilités logicielles courantes
- Analyse statique et dynamique du code, revues de code manuelles
- Gestion des composants logiciels tiers et nomenclature logicielle
- Vérification et validation de la sécurité : tests, évaluation, preuves attendues
- Indicateurs de maturité sécurité par phase de développement
- Évaluation des risques résiduels et dossier de sécurité à l'intégration finale
- Préparation aux évaluations et certifications de produit

Fil rouge · Avant la phase d'intégration du calculateur, Camille fait réaliser une analyse de code qui révèle plusieurs défauts. Elle doit établir le niveau de sécurité atteint et formaliser les risques résiduels à présenter au client exploitant.

Cours 13 · Maintenir la sécurité du produit et sécuriser la supply chain

22 h

OBJECTIFS

- Adapter le processus de gestion du changement pour maintenir le niveau de sécurité du produit dans le temps
- Définir et mettre en œuvre un système d'assurance sécurité dans la chaîne d'approvisionnement

ÉVALUATION FORMATIVE

Étude de cas sur une demande de changement et élaboration d'un plan d'assurance sécurité fournisseur

CONTENUS

- Gestion de configuration et gestion du changement d'un produit en service
- Analyse d'impact sécurité d'une modification et décision de requalification
- Gestion des vulnérabilités en exploitation et diffusion des correctifs
- Cartographie de la supply chain et des fournisseurs critiques
- Exigences de sécurité contractuelles et plans d'assurance sécurité fournisseurs
- Évaluation et audit des fournisseurs, suivi des écarts
- Système d'assurance sécurité : organisation, revues, preuves de conformité

Fil rouge · Un fournisseur de cartes électroniques d'Alvéon Mobilité annonce un changement de composant. Camille doit évaluer l'impact sur la sécurité du calculateur et intégrer des exigences d'assurance sécurité dans les contrats fournisseurs.

Maintenir en continuité de service

Cours 14 · Cadrer un test d'intrusion et mener la reconnaissance — 22 h

OBJECTIFS

- Définir et analyser le périmètre d'intervention d'un audit technique
- Rechercher des informations directes et indirectes sur l'organisation cible pour identifier des vulnérabilités

ÉVALUATION FORMATIVE

Rédaction d'une convention d'audit et quiz sur le cadre légal des tests d'intrusion

CONTENUS

- Cadre légal et éthique des tests d'intrusion : autorisation, convention d'audit, responsabilités
- Référentiel PASSI et bonnes pratiques de conduite d'audit
- Définition du périmètre, des règles d'engagement et des contraintes de production
- Recherche passive d'informations en sources ouvertes (OSINT)
- Reconnaissance active : découverte des services accessibles et de l'infrastructure
- Cartographie de la surface d'attaque
- Planification de la campagne et coordination avec les équipes exploitées

Fil rouge · Devenue RSSI adjointe, Camille prépare une campagne de tests d'intrusion sur le portail fournisseurs et le réseau d'une usine. Elle rédige la convention d'audit et mène une première phase de reconnaissance en sources ouvertes.

Cours 15 · Réaliser des tests d'intrusion et des audits techniques — 22 h

OBJECTIFS

- Élaborer et planifier des scénarios d'attaques adaptés au périmètre
- Réaliser des tests d'intrusion, des audits de code et de configuration pour qualifier les vecteurs de risque

ÉVALUATION FORMATIVE

Travaux pratiques guidés en environnement de laboratoire et QCM sur la qualification des vulnérabilités

CONTENUS

- Méthodologies de test : boîte noire, grise, blanche, tests internes et externes
- Élaboration de scénarios d'attaques à partir de l'analyse de risque
- Tests d'intrusion réseau et systèmes : ports ouverts, services vulnérables, élévation de privilèges
- Tests d'intrusion applicatifs : référentiel OWASP et vulnérabilités web
- Audit de configuration : annuaires, systèmes, équipements réseau
- Audit de code orienté sécurité
- Qualification des vulnérabilités et évaluation de leur criticité

Fil rouge · Dans un environnement de laboratoire reproduisant le SI d'Alvéon Mobilité, Camille déroule les scénarios d'attaques prévus. Elle doit qualifier une faille de configuration de l'annuaire permettant une élévation de privilèges.

Cours 16 · Rédiger le rapport de vulnérabilités et piloter les campagnes de tests — 22 h

OBJECTIFS

- Rédiger pour les métiers un rapport d'analyse des vulnérabilités documenté et assorti de preuves
- Préconiser des mesures correctives priorisées
- Piloter les projets de tests d'intrusion en maîtrisant délais, budgets et relations avec les équipes

ÉVALUATION FORMATIVE

Rédaction d'une synthèse managériale et d'une fiche de vulnérabilité, évaluées par une grille de critères

CONTENUS

- Structure d'un rapport d'audit : synthèse managériale, détail technique, preuves
- Cotation des vulnérabilités : méthode CVSS et contextualisation métier
- Formulation de recommandations correctives réalistes et priorisées
- Restitution orale aux métiers et à la direction
- Suivi du plan de remédiation et contre-audit
- Pilotage d'un programme annuel de tests : planning, budget, prestataires
- Communication, rigueur et gestion des relations avec les équipes auditées

Fil rouge · Camille doit restituer les résultats de la campagne à deux publics : le directeur industriel, qui attend une synthèse claire, et l'équipe d'exploitation, qui doit corriger les failles sans arrêter la production.

Cours 17 · Mener une analyse post-mortem (forensic)

22 h

OBJECTIFS

- Réaliser une analyse forensique en préservant l'intégrité des preuves
- Intégrer les exigences des investigations administratives, criminelles, civiles et réglementaires dans les campagnes de tests

ÉVALUATION FORMATIVE

Étude de cas forensique : reconstitution d'une chronologie d'incident à partir de journaux fictifs

CONTENUS

- Gestion d'incident de sécurité et place de l'investigation numérique
- Types d'investigation et exigences associées : administrative, criminelle, civile, réglementaire
- Collecte et préservation des preuves : chaîne de custody, horodatage, empreintes
- Analyse de systèmes de fichiers, de mémoire et de journaux
- Reconstitution de la chronologie d'une attaque
- Obligations de notification et relations avec les autorités
- Retour d'expérience et adaptation des campagnes de tests

Fil rouge · Un poste d'atelier présente un comportement suspect évoquant une compromission. Camille coordonne la collecte des preuves et l'analyse de la chronologie, en tenant compte d'un éventuel dépôt de plainte.

Cours 18 · Identifier les applications critiques et définir la continuité de service

22 h

OBJECTIFS

- Classifier les applications et serveurs pour identifier les actifs critiques
- Définir avec les métiers et la DSI les critères de continuité de service (DMIA, PDMA)

ÉVALUATION FORMATIVE

Cas pratique : réalisation d'un BIA et d'une classification des applications à partir d'entretiens simulés

CONTENUS

- Fondamentaux de la continuité d'activité : ISO 22301, distinction PCA, PRA, PCI
- Méthode de questionnement structuré des métiers : entretiens, ateliers, visites sur site
- Exploitation des documents existants et des résultats des tests d'intrusion
- Bilan d'impact sur l'activité (BIA) et classification des applications et serveurs
- Durée maximale d'interruption admissible (DMIA) et perte de données maximale admissible (PDMA)
- Dépendances techniques, fournisseurs et ressources critiques
- Choix des stratégies de continuité et de reprise

Fil rouge · Camille rencontre les responsables de production, de la logistique et de la maintenance pour mener le bilan d'impact. Elle découvre que l'application de planification de l'atelier ne supporte pas plus de quelques heures d'interruption.

Cours 19 · Organiser la gestion de crise et l'équipe PCA/PRA

22 h

OBJECTIFS

- Définir une organisation dédiée à la gestion d'un sinistre
- Formaliser les procédures de crise et de reprise d'activité

ÉVALUATION FORMATIVE

Participation à un exercice de crise simulé et rédaction d'une fiche réflexe

CONTENUS

- Organisation de crise : cellules décisionnelle, opérationnelle et technique
- Rôles et responsabilités de l'équipe PCA/PRA
- Procédures d'alerte, d'escalade et de déclenchement
- Communication de crise interne et externe
- Procédures de reprise : sauvegardes, sites de secours, ordre de redémarrage
- Spécificités de la cyber-crise : rançongiciel, compromission de l'annuaire
- Préparation et conduite d'un exercice de crise

Fil rouge · Camille constitue la cellule de crise d'Alvéon Mobilité et organise un exercice simulant un rançongiciel. Les sauvegardes du SI de gestion s'avèrent indisponibles pendant le scénario.

Cours 20 · Maintenir le PCA/PRA en condition opérationnelle et piloter le projet

22 h

OBJECTIFS

- Inscrire le PCA/PRA dans une boucle d'amélioration continue grâce à un plan de maintien en condition opérationnelle
- Piloter le projet PCA/PRA pour accroître la résilience de l'organisation

ÉVALUATION FORMATIVE

Rendu d'un retour d'expérience structuré et d'un plan de maintien en condition opérationnelle, complété par un QCM de synthèse

CONTENUS

- Plan de maintien en condition opérationnelle : mises à jour, tests, formation
- Programme d'exercices et de tests de reprise
- Retour d'expérience et identification des évolutions à apporter
- Anticipation des futures cyber-crises et veille sur les menaces
- Indicateurs de résilience et reporting à la direction
- Pilotage du projet PCA/PRA : planning, budget, parties prenantes
- Leadership, communication et travail en équipe dans un projet de résilience

Fil rouge · À l'issue de l'exercice de crise, Camille présente au comité de direction le retour d'expérience. Elle y joint une feuille de route de maintien en condition opérationnelle du PCA/PRA, avec le budget et les jalons associés.

05 · CONFORMITÉ AU RÉFÉRENTIEL

Couverture des compétences

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

Compétence	Bloc	Cours
Définir le périmètre d'application et la politique de sécurité	RNCP38434BC01	1
Identifier, apprécier les risques, définir les seuils d'acceptabilité et le plan de traitement	RNCP38434BC01	2
Choisir et piloter la mise en place des mesures de sécurité techniques et organisationnelles	RNCP38434BC01	3
Contrôler le SMSI dans une boucle d'amélioration continue par des indicateurs	RNCP38434BC01	4
Piloter les projets de définition et de mise en œuvre du SMSI	RNCP38434BC01	1, 4
Identifier les accès internes et externes aux actifs par un audit préalable	RNCP38434BC01	5
Implémenter et gérer les mécanismes d'autorisation et la matrice des rôles	RNCP38434BC01	5
Gérer le cycle de vie des identités et le provisionnement des accès	RNCP38434BC01	6
Choisir des solutions et mettre en place des architectures IAM (fédération, SSO, PAM)	RNCP38434BC01	7
Analyser les données d'identités et d'habilitations par un outillage logiciel	RNCP38434BC01	6
Piloter les projets de gestion des accès et des identités	RNCP38434BC01	7
Concevoir une architecture durable, performante et évolutive	RNCP38434BC02	8
Intégrer les équipements et solutions de sécurité du marché (veille, déploiement, migration)	RNCP38434BC02	9
Conseiller et convaincre un donneur d'ordre pour mobiliser les ressources	RNCP38434BC02	10
Piloter les projets de conception et de mise en œuvre des fonctions de sécurité	RNCP38434BC02	9, 10
Réaliser les études de sécurité dans le développement d'un produit industriel	RNCP38434BC02	11
Intégrer la gestion des risques dans le développement d'un produit industriel complexe (analyse de code)	RNCP38434BC02	11, 12
Évaluer le niveau de maturité et les risques résiduels du produit	RNCP38434BC02	12
Adapter le processus de gestion du changement du produit	RNCP38434BC02	13
Définir et mettre en œuvre un système d'assurance sécurité dans la supply chain	RNCP38434BC02	13
Définir et analyser le périmètre d'intervention et rechercher des informations sur la cible	RNCP38434BC03	14
Réaliser des tests d'intrusion, audits de code et de configuration	RNCP38434BC03	15
Rédiger un rapport d'analyse des vulnérabilités et préconiser des mesures correctives	RNCP38434BC03	16
Réaliser des analyses post-mortem (forensic)	RNCP38434BC03	17
Piloter les projets de tests d'intrusion	RNCP38434BC03	14, 16
Classifier les applications et serveurs critiques	RNCP38434BC03	18
Définir la continuité de service et ses critères (DMIA, PDMA)	RNCP38434BC03	18
Définir une organisation et une équipe dédiée PCA/PRA	RNCP38434BC03	19
Identifier les évolutions du PCA/PRA et assurer son maintien en condition opérationnelle	RNCP38434BC03	20
Piloter le projet de PCA/PRA	RNCP38434BC03	19, 20

Évaluations formatives

Chaque sous-chapitre se termine par un QCM de validation des acquis, qui permet à l'apprenant de mesurer sa progression en continu. Chaque cours comporte en outre une évaluation formative ancrée dans le fil rouge Alvéon Mobilité : étude de cas, production d'un livrable professionnel (PSSI, cartographie des risques, matrice des rôles, dossier d'architecture, rapport d'audit, BIA, plan de maintien en condition opérationnelle) ou préparation d'une présentation orale. Des grilles de critères accompagnent les livrables pour faciliter l'auto-évaluation et, le cas échéant, la correction par le formateur de l'organisme de formation. Les résultats restent consultables sur la plateforme et permettent à l'OF d'assurer un suivi individualisé de la progression.

Modalités de certification

Bloc	Modalité d'évaluation
RNCP38434BC01	Cas pratiques, rendu de livrables et soutenance orale
RNCP38434BC02	Cas pratiques, rendu de livrables et soutenance orale
RNCP38434BC03	Cas pratiques, rendu de livrables et soutenance orale

Le parcours reproduit le format des épreuves officielles : les cas pratiques du fil rouge amènent l'apprenant à produire, bloc après bloc, les livrables attendus d'un spécialiste en cybersécurité. Les cours de pilotage et de conviction (cours 4, 7, 10, 16 et 20) entraînent spécifiquement à la synthèse et à la présentation orale devant un public de direction, en préparation des soutenances. Chaque compétence du référentiel étant reliée à un ou plusieurs cours dans la matrice de couverture, l'organisme de formation peut vérifier que tous les attendus sont travaillés avant la présentation aux épreuves. School For Mate fournit le contenu pédagogique : l'organisation des épreuves et l'inscription des candidats relèvent de l'organisme de formation, en lien avec le certificateur.

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 connexions et des résultats
- Une vidéo de 3 à 5 minutes par sous-chapitre, représentant 30 % du volume horaire du parcours
- Cours texte enrichi, infographies et schémas d'architecture téléchargeables
- Études de cas et mises en situation professionnelles construites autour du fil rouge Alvéon Mobilité
- Modèles de livrables professionnels : PSSI, plan de traitement des risques, matrice des rôles, convention d'audit, rapport de vulnérabilités, BIA, fiches réflexes de crise
- QCM de validation par sous-chapitre et grilles de critères pour l'auto-évaluation des livrables
- Environnements de laboratoire et jeux de données fictifs pour les travaux pratiques techniques (tests d'intrusion, analyse d'habilitations, forensic), mis à disposition selon l'équipement de l'organisme de formation

Débouchés et évolutions

- RSSI
- Consultant ou auditeur organisationnel en cybersécurité
- Consultant technique en cybersécurité
- Ingénieur-intégrateur de solutions en cybersécurité
- Analyste cybersécurité
- Chef de projet cybersécurité ou auditeur technique d'infrastructures de cybersécurité

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 RNCP38434 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.