

SCHOOL FOR MATE

LIVRET PÉDAGOGIQUE

Manager de la cybersécurité

RNCP40246 · Certification RNCP · Niveau 7

Ce parcours de 440 heures prépare les professionnels de l'informatique à piloter la cybersécurité d'une organisation, de l'analyse stratégique des cyber-risques jusqu'à la gestion budgétaire des projets de sécurité. Il est construit sur les cinq blocs de compétences de la certification RNCP40246 « Manager de la cybersécurité » (niveau 7) et suit tout au long des cours le fil rouge d'une entreprise industrielle soumise à la directive NIS2.

VOLUME HORAIRE	COURS	BLOCS
440 h	20	5

01 · PRÉSENTATION

La formation en bref

Intitulé	Manager de la cybersécurité
Code	RNCP40246
Type	Certification RNCP
Niveau	Niveau 7
Certificateur	ADE HOLDING, DE VINCI HIGHER EDUCATION (DVHE)
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	28/02/2030

Le métier et les compétences visées

Le manager de la cybersécurité définit et pilote la stratégie de protection des systèmes d'information et des réseaux d'une organisation. Il analyse les menaces (géopolitiques, criminelles, concurrentielles), audite les vulnérabilités, conçoit une architecture de sécurité adaptée au niveau de risque et rédige les appels d'offres destinés aux prestataires. Il déploie la politique de sécurité des systèmes d'information (PSSI) en s'appuyant sur les recommandations de l'ANSSI, sécurise les infrastructures physiques et organise la continuité d'activité. Il développe une culture de la cybersécurité auprès des équipes, anticipe et gère les crises, et assure le pilotage budgétaire des projets ainsi que le suivi des sous-traitants. Il exerce avec une large autonomie, dans un environnement fortement réglementé.

Public visé

- Administrateurs systèmes et réseaux souhaitant évoluer vers des fonctions de management de la sécurité
- Ingénieurs ou techniciens supérieurs en informatique visant un poste de RSSI ou d'ingénieur cybersécurité
- Consultants en systèmes d'information souhaitant se spécialiser dans le conseil en sécurité
- Chefs de projet informatique ou DSI adjoints en charge de la conformité NIS2 et de la sécurité
- Titulaires d'une certification de niveau 6 en informatique, réseaux ou management des SI

Prérequis

- Être titulaire d'une certification professionnelle de niveau 6 minimum
- Ou être titulaire d'une certification professionnelle de niveau 5 avec une expérience professionnelle, après validation du dossier par la Commission d'autorisation de candidature (CAC) du certificateur
- Disposer de connaissances de base en systèmes d'information et en réseaux (architecture, protocoles, administration)
- Disposer d'un poste informatique et d'une connexion internet permettant de suivre les contenus vidéo et les activités en ligne

Objectifs pédagogiques

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

- Cartographier les menaces cyber pesant sur un pays, une industrie ou une entreprise à partir d'une analyse géopolitique et de l'historique des cyberattaques
- Conduire un audit de vulnérabilité du système d'information et des réseaux et établir le catalogue des risques d'intrusion selon les principes du hacking éthique
- Évaluer les dommages potentiels sur les données numériques et rédiger un cahier des charges de cybersécurité conforme à l'ISO/IEC 27032 et à la directive NIS2
- Concevoir le schéma général de cybersécurité et une architecture cible, puis piloter l'appel d'offres et la sélection des prestataires
- Élaborer et diffuser une PSSI fondée sur les recommandations de l'ANSSI, intégrant la protection des données, la sécurité physique et la sûreté de fonctionnement
- Évaluer les usages offensifs et défensifs de l'intelligence artificielle en cybersécurité
- Concevoir un plan de formation, conduire le changement et préparer la communication de crise en tenant compte de l'accessibilité et de la multiculturalité
- Construire le budget et le plan de financement d'un projet de cybersécurité, puis piloter les écarts à l'aide de tableaux de bord
- Organiser la veille réglementaire, technologique et concurrentielle et assurer le suivi contractuel et financier des sous-traitants

02 · FIL ROUGE PÉDAGOGIQUE

Hydralys

CA

Camille Arnaud

Manager de la cybersécurité, nouvellement recrutée et rattachée à la direction générale

Conception et maintenance d'équipements de traitement de l'eau pour les collectivités et les industriels (ETI d'environ 900 salariés, trois sites en France et une filiale au Ma

Hydralys fournit et télé-exploite des stations de traitement de l'eau pour des collectivités et des industriels. Son activité la place dans le périmètre de la directive NIS2, et la direction générale a pris conscience de son exposition après une tentative d'hameçonnage ciblé visant le service comptable. Le système d'information s'est construit par strates : ERP hébergé en interne, messagerie et outils collaboratifs en SaaS, supervision industrielle connectée à distance, sauvegardes hétérogènes selon les sites. Aucune PSSI formalisée n'existe et les équipes, réparties entre la France et le Maroc, ont des pratiques très variées. Camille Arnaud est recrutée pour structurer la cybersécurité de l'entreprise : elle dispose d'un budget à construire, d'un comité de direction attentif mais exigeant, et d'une équipe informatique de huit personnes qu'elle doit fédérer autour d'un projet de transformation.

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 analyse le contexte géopolitique du secteur de l'eau, audite le SI d'Hydralys, évalue les dommages possibles sur les données et met en place une cellule de veille concurrentielle.
2. Bloc 2 : elle conçoit le schéma général de cybersécurité, rédige avec les achats l'appel d'offres pour un centre de supervision externalisé, refond la stratégie de sauvegarde cloud et organise la veille réglementaire.
3. Bloc 3 : elle fait réaliser un test d'intrusion, rédige et diffuse la PSSI, évalue les outils de détection fondés sur l'IA, sécurise les sites physiques et l'alimentation électrique, puis formalise le plan de continuité d'activité.
4. Bloc 4 : elle mesure les compétences des salariés, pilote le projet de nouvelle organisation, accompagne le changement sur les sites français et marocain, prépare la communication de crise et rend le dispositif accessible à tous.
5. Bloc 5 : elle chiffre le programme pluriannuel, négocie son financement avec la direction financière, construit les tableaux de bord de suivi et contrôle la solidité des prestataires retenus.

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
RNCP40246BC01 · Mener une analyse stratégique des cyber-risques		**88 h**
1	Géopolitique des cybermenaces et cartographie des menaces sectorielles	22 h
2	Audit du système d'information et des réseaux	22 h
3	Analyse des dommages sur les données et conformité ISO/IEC 27032 et NIS2	22 h
4	Intelligence économique et surveillance de l'environnement concurrentiel	22 h
RNCP40246BC02 · Concevoir et organiser la sécurité des SI et des réseaux		**88 h**
5	Schéma général de cybersécurité et architecture de sécurité cible	22 h
6	Spécifications techniques, cahier des charges et appel d'offres sécurité	22 h
7	Sécurité du cloud : sauvegardes et formation des utilisateurs IaaS, PaaS, SaaS	22 h
8	Veille réglementaire et technologique en cybersécurité	22 h
RNCP40246BC03 · Déployer la sécurité des SI et des réseaux		**110 h**
9	Hacking éthique et catalogue des risques d'intrusion	22 h
10	Élaborer et diffuser la PSSI selon les recommandations de l'ANSSI	22 h
11	Intelligence artificielle et cybersécurité : usages offensifs et défensifs	22 h
12	Sécurité physique des locaux et continuité de l'alimentation énergétique	22 h
13	Protection des données et sûreté de fonctionnement	22 h
RNCP40246BC04 · Développer une culture de la cybersécurité dans l'entreprise		**88 h**
14	Diagnostic des compétences et plan de formation en cybersécurité	22 h
15	Gestion de projet et conduite du changement en cybersécurité	22 h
16	Anticiper et communiquer en situation de crise cyber	22 h
17	Accessibilité et multiculturalité dans le management de la cybersécurité	22 h
RNCP40246BC05 · Gérer les aspects budgétaires et financiers de la cyber sécurité		**66 h**
18	Budget prévisionnel et plan de financement du projet de cybersécurité	22 h
19	Contrôle de gestion, tableaux de bord et analyse des écarts	22 h
20	Suivi des contrats de sous-traitance et des garanties financières	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

RNCP40246BC01 · 88 h

Mener une analyse stratégique des cyber-risques

Cours 1 · Géopolitique des cybermenaces et cartographie des menaces sectorielles

22 h

OBJECTIFS

- Analyser une situation géopolitique propice aux cyberattaques contre le potentiel économique d'un pays ou d'une industrie
- Recenser et qualifier les cyberattaques passées pour cartographier les menaces potentielles sur un secteur

ÉVALUATION FORMATIVE

QCM de fin de cours et note de synthèse stratégique corrigée selon une grille critériée

CONTENUS

- Le cyberespace comme champ de conflictualité : acteurs étatiques, groupes cybercriminels, hacktivistes
- Typologie des menaces : espionnage, sabotage, rançongiciel, déstabilisation
- Méthode de recensement des cyberattaques passées à partir de sources ouvertes et de rapports institutionnels
- Lecture des rapports publics de l'ANSSI et de l'ENISA sur l'état de la menace
- Référentiels de modes opératoires des attaquants (tactiques, techniques et procédures)
- Construction d'une cartographie des menaces par pays et par industrie
- Restitution de l'analyse à une direction générale : note de synthèse stratégique

Fil rouge · Camille doit présenter au comité de direction d'Hydralys une cartographie des menaces pesant sur le secteur de l'eau en France et au Maroc, à partir des attaques documentées contre des opérateurs comparables.

Cours 2 · Audit du système d'information et des réseaux

22 h

OBJECTIFS

- Conduire un audit du SI et des réseaux de l'entreprise selon une démarche structurée
- Identifier les points de vulnérabilité au regard des menaces d'intrusion du cyberespace

ÉVALUATION FORMATIVE

Étude de cas : analyse d'un extrait de rapport d'audit et priorisation des vulnérabilités, QCM de validation

CONTENUS

- Cadre d'un audit de sécurité : périmètre, lettre de mission, parties prenantes
- Typologies d'audit : organisationnel, d'architecture, de configuration, de code
- Inventaire et cartographie du SI : actifs, flux, interconnexions, systèmes industriels
- Outils de découverte et d'analyse de vulnérabilités, interprétation des résultats
- Analyse des écarts au regard du guide d'hygiène informatique de l'ANSSI
- Priorisation des vulnérabilités selon criticité et exploitabilité
- Rédaction du rapport d'audit et du plan d'actions

Fil rouge · Camille conduit l'audit des trois sites d'Hydralys et découvre que la supervision des stations est accessible depuis le réseau bureautique : elle doit qualifier cette vulnérabilité et la hiérarchiser parmi les autres constats.

Cours 3 · Analyse des dommages sur les données et conformité ISO/IEC 27032 et NIS2

22 h

OBJECTIFS

- Caractériser les atteintes possibles aux données numériques (altération, captation, destruction) et en estimer les dommages
- Établir un cahier des charges de cybersécurité conforme à l'ISO/IEC 27032 et à la directive NIS2 dans le cadre du budget disponible

ÉVALUATION FORMATIVE

Exercice de rédaction d'un cahier des charges partiel et QCM sur les exigences ISO/IEC 27032 et NIS2

CONTENUS

- Classification des données et des traitements : sensibilité, criticité, obligations associées
- Scénarios d'atteinte aux données : altération, captation, destruction
- Évaluation des impacts métier, financiers, juridiques et d'image
- Introduction à la méthode EBIOS Risk Manager pour l'analyse de risques
- Norme ISO/IEC 27032 : lignes directrices de cybersécurité et articulation avec la famille ISO 27000
- Directive NIS2 : entités concernées, mesures de gestion des risques, obligations de notification, responsabilité des dirigeants
- Arbitrage entre exigences de conformité et budget disponible
- Structure et rédaction du cahier des charges de cybersécurité

Fil rouge · À partir des scénarios d'attaque sur les données de télé-exploitation, Camille doit rédiger le cahier des charges de cybersécurité d'Hydralys en montrant comment il répond aux obligations NIS2 sans dépasser l'enveloppe annoncée par la direction.

Cours 4 · Intelligence économique et surveillance de l'environnement concurrentiel

22 h

OBJECTIFS

- Organiser un dispositif de surveillance de l'environnement concurrentiel national et international
- Collecter, analyser et diffuser les informations économiques et stratégiques utiles pour anticiper les intentions des concurrents

ÉVALUATION FORMATIVE

Mise en situation : conception d'un plan de veille et rédaction d'un bulletin de synthèse, QCM de fin de cours

CONTENUS

- Fondamentaux de l'intelligence économique : veille, protection, influence
- Cycle du renseignement : orientation, collecte, analyse, diffusion
- Sources ouvertes et méthodes de recherche (OSINT) dans un cadre légal et éthique
- Outils de veille : agrégation, alertes, tableaux de bord de veille
- Analyse concurrentielle : signaux faibles, stratégies, mouvements de marché
- Protection du patrimoine informationnel face à l'espionnage économique
- Livrables de veille adaptés aux décideurs

Fil rouge · La direction commerciale d'Hydralys soupçonne un concurrent étranger de cibler ses appels d'offres publics : Camille met en place une cellule de veille et produit un premier bulletin d'intelligence économique.

RNCP40246BC02 · 88 h

Concevoir et organiser la sécurité des SI et des réseaux

Cours 5 · Schéma général de cybersécurité et architecture de sécurité cible

22 h

OBJECTIFS

- Établir le schéma général de la cybersécurité de l'entreprise à partir de l'audit de vulnérabilité
- Déterminer les caractéristiques d'une nouvelle architecture de sécurité adaptée au niveau de risque

ÉVALUATION FORMATIVE

Étude de cas : production d'un schéma d'architecture commenté et QCM

CONTENUS

- Du rapport d'audit au schéma directeur de cybersécurité
- Principes d'architecture : défense en profondeur, moindre privilège, cloisonnement
- Segmentation des réseaux et séparation des environnements bureautiques et industriels
- Approche « zéro confiance » et gestion des identités et des accès
- Briques de sécurité : filtrage, détection, journalisation, supervision
- Recommandations de l'ANSSI pour les architectures et l'administration sécurisée
- Formalisation et validation de l'architecture cible

Fil rouge · Camille dessine l'architecture cible d'Hydralys en isolant la supervision industrielle et en créant un poste d'administration dédié, puis la défend devant le directeur des systèmes d'information.

Cours 6 · Spécifications techniques, cahier des charges et appel d'offres sécurité

22 h

OBJECTIFS

- Traduire les attentes d'architecture et de solutions de sécurité en spécifications techniques
- Coordonner la rédaction du cahier des charges et de l'appel d'offres en vue de la sélection des prestataires et sous-traitants

ÉVALUATION FORMATIVE

Rédaction d'un extrait de cahier des charges et d'une grille de sélection, QCM de validation

CONTENUS

- Expression du besoin : exigences fonctionnelles, techniques, de sécurité et de service
- Rédaction de spécifications techniques mesurables et vérifiables
- Structure d'un dossier de consultation : règlement, cahier des charges, annexes
- Coordination des contributeurs : DSI, achats, juridique, métiers
- Visas de sécurité de l'ANSSI : produits et prestataires qualifiés
- Grille d'analyse des offres et critères de sélection pondérés
- Clauses de sécurité et de réversibilité dans les contrats

Fil rouge · Hydralys décide d'externaliser la détection des incidents : Camille coordonne avec le service achats le cahier des charges et la grille d'évaluation des candidats.

Cours 7 · Sécurité du cloud : sauvegardes et formation des utilisateurs IaaS, PaaS, SaaS

22 h

OBJECTIFS

- Concevoir et organiser les systèmes de sauvegarde en cohérence avec la stratégie cloud et les catégories d'utilisateurs
- Définir les contenus de formation des utilisateurs aux bonnes pratiques de sécurité cloud selon le modèle IaaS, PaaS ou SaaS

ÉVALUATION FORMATIVE

Étude de cas sur une politique de sauvegarde et conception d'un plan de formation cloud, QCM

CONTENUS

- Modèles de services cloud et partage des responsabilités de sécurité
- Qualification SecNumCloud et critères de choix d'un hébergeur
- Stratégie de sauvegarde : règle 3-2-1, sauvegardes hors ligne et immuables, tests de restauration
- Adaptation des politiques de sauvegarde aux catégories d'utilisateurs et de données
- Risques spécifiques du cloud : mauvaise configuration, gestion des identités, fuite de données
- Bonnes pratiques par modèle de service et par profil d'utilisateur
- Conception d'un programme de formation cloud orienté efficacité et rentabilité

Fil rouge · Camille constate que les sauvegardes de la filiale marocaine ne sont jamais testées : elle refond la politique de sauvegarde et conçoit un module de sensibilisation adapté aux utilisateurs des outils collaboratifs en SaaS.

Cours 8 · Veille réglementaire et technologique en cybersécurité

22 h

OBJECTIFS

- Concevoir un système de veille sur les contraintes légales et réglementaires de la cybersécurité
- Utiliser les sites des organismes spécialisés et les bases de données juridiques pour assurer la conformité des dispositifs

ÉVALUATION FORMATIVE

Mise en situation : construction d'un plan de veille et d'un registre de conformité, QCM

CONTENUS

- Panorama du cadre juridique : RGPD, NIS2, DORA, Cyber Resilience Act, droit pénal du numérique
- Sources institutionnelles : ANSSI, CNIL, ENISA, CERT-FR, Journal officiel de l'Union européenne
- Bases de données juridiques et recherche documentaire
- Outils numériques de veille : flux, alertes, agrégateurs, organisation des sources
- Veille technologique : bulletins de vulnérabilités, évolutions des solutions
- Qualification de l'information et analyse d'impact sur l'entreprise
- Registre de conformité et diffusion des alertes aux parties prenantes

Fil rouge · Camille met en place le dispositif de veille réglementaire d'Hydralys et doit, dès la première alerte, évaluer l'impact d'un nouveau texte sur ses obligations de notification d'incident.

Déployer la sécurité des SI et des réseaux

Cours 9 · Hacking éthique et catalogue des risques d'intrusion

22 h

OBJECTIFS

- Établir le catalogue des risques d'intrusion et failles de sécurité d'un SI sur la base d'un audit et selon les principes du hacking éthique
- Planifier le déploiement des solutions de cybersécurité à partir de ce catalogue

ÉVALUATION FORMATIVE

Étude de cas : analyse d'un rapport de test d'intrusion et élaboration d'un catalogue des risques, QCM

CONTENUS

- Cadre légal et éthique du test d'intrusion : autorisation, convention, périmètre
- Méthodologie d'un test d'intrusion : reconnaissance, exploitation, élévation de privilèges, rapport
- Tests en boîte noire, grise et blanche
- Failles courantes : applications web, Active Directory, accès distants, ingénierie sociale
- Construction du catalogue des risques d'intrusion
- Prestataires d'audit de sécurité qualifiés (PASSI)
- Feuille de route de remédiation et planification du déploiement

Fil rouge · Camille commande un test d'intrusion qui révèle des mots de passe faibles sur des comptes à privilèges : elle intègre ces résultats au catalogue des risques et planifie les correctifs.

Cours 10 · Élaborer et diffuser la PSSI selon les recommandations de l'ANSSI

22 h

OBJECTIFS

- Définir une politique de sécurité des systèmes d'information en s'appuyant sur les recommandations de l'ANSSI
- Organiser sa diffusion auprès des parties prenantes internes et externes

ÉVALUATION FORMATIVE

Rédaction de chapitres de PSSI et d'un plan de diffusion, QCM

CONTENUS

- Rôle et place de la PSSI dans la gouvernance de la sécurité
- Démarche d'élaboration recommandée par l'ANSSI
- Structure d'une PSSI : principes, organisation, règles par domaine
- Déclinaisons opérationnelles : chartes, procédures, politiques thématiques
- Validation par la direction et implication des dirigeants
- Diffusion aux salariés, prestataires et partenaires
- Mise à jour et contrôle d'application de la PSSI

Fil rouge · Camille rédige la première PSSI d'Hydralys, la fait valider par le comité de direction et organise sa diffusion auprès des salariés et des sous-traitants de maintenance.

Cours 11 · Intelligence artificielle et cybersécurité : usages offensifs et défensifs

22 h

OBJECTIFS

- Évaluer les potentialités de l'intelligence artificielle en matière de cybersécurité offensive et défensive
- Formuler des recommandations d'usage maîtrisé de l'IA dans le dispositif de sécurité

ÉVALUATION FORMATIVE

Étude de cas comparative et note de recommandation, QCM

CONTENUS

- Notions clés : apprentissage automatique, modèles génératifs, détection d'anomalies
- Usages offensifs : hameçonnage personnalisé, hypertrucages, automatisation de la reconnaissance
- Usages défensifs : détection comportementale, tri des alertes, analyse de journaux
- Risques propres aux systèmes d'IA : empoisonnement, fuite de données, manipulation des requêtes
- Cadre réglementaire européen de l'IA et recommandations de l'ANSSI
- Critères d'évaluation d'une solution de sécurité intégrant de l'IA
- Charte d'usage de l'IA générative en entreprise

Fil rouge · Un salarié d'Hydralys reçoit un message vocal imitant la voix du directeur financier : Camille évalue la menace et compare deux solutions de détection fondées sur l'IA.

Cours 12 · Sécurité physique des locaux et continuité de l'alimentation énergétique

22 h

OBJECTIFS

- Identifier les risques d'atteinte aux infrastructures physiques et placer les alertes et protections adaptées
- Optimiser la fourniture d'énergie et les dispositifs de secours pour assurer l'alimentation permanente des SI

ÉVALUATION FORMATIVE

Mise en situation : diagnostic de sécurité physique d'un site sur plan, QCM

CONTENUS

- Analyse des risques physiques : intrusion, vol, malveillance interne, risques naturels
- Zonage des locaux et contrôle d'accès physique
- Détection d'intrusion, vidéoprotection et alarmes
- Sécurisation des salles serveurs et des locaux techniques
- Alimentation électrique : onduleurs, groupes électrogènes, redondance des arrivées
- Maintenance et tests des dispositifs de secours
- Coordination avec les services généraux et les prestataires

Fil rouge · Lors d'une visite du site principal, Camille découvre que la salle serveurs partage son accès avec un local d'archives et que l'onduleur n'a jamais été testé : elle bâtit un plan de sécurisation physique et énergétique.

Cours 13 · Protection des données et sûreté de fonctionnement

22 h

OBJECTIFS

- Protéger l'accès aux espaces de stockage et aux données par des codes d'accès et un chiffrement adaptés aux menaces
- Établir le schéma général de la sûreté de fonctionnement pour garantir la continuité de l'activité

ÉVALUATION FORMATIVE

Étude de cas : conception d'un plan de continuité et QCM sur les mécanismes de protection

CONTENUS

- Gestion des identités et des accès : authentification multifacteur, gestion des comptes à privilèges
- Politique de mots de passe et de codes d'accès
- Principes de cryptographie : chiffrement symétrique et asymétrique, gestion des clés
- Chiffrement des postes, des supports et des espaces de stockage
- Protection du patrimoine immatériel : savoir-faire, propriété intellectuelle, données clients
- Bilan d'impact sur l'activité, plan de continuité et plan de reprise d'activité
- Schéma général de sûreté de fonctionnement et exercices de continuité

Fil rouge · Camille déploie l'authentification multifacteur et le chiffrement des postes nomades, puis rédige le plan de continuité d'Hydralys en simulant une attaque par rançongiciel sur l'ERP.

RNCP40246BC04 · 88 h

Développer une culture de la cybersécurité dans l'entreprise

Cours 14 · Diagnostic des compétences et plan de formation en cybersécurité

22 h

OBJECTIFS

- Analyser les compétences du personnel en cybersécurité au moyen de questionnaires et d'entretiens
- Concevoir et mettre en place un plan de formation des personnels et de conseil aux services supports

ÉVALUATION FORMATIVE

Conception d'un questionnaire de positionnement et d'un plan de formation, QCM

CONTENUS

- Cartographie des profils et des besoins : utilisateurs, managers, équipes informatiques, services supports
- Conception de questionnaires de positionnement
- Conduite d'entretiens et analyse des résultats
- Construction d'un plan de formation et de sensibilisation
- Modalités : campagnes d'hameçonnage simulé, ateliers, modules en ligne
- Conseil aux services supports : RH, juridique, achats, services généraux
- Mesure de l'efficacité des actions de formation

Fil rouge · Camille diffuse un questionnaire à l'ensemble des salariés d'Hydralys et mène des entretiens avec les services supports pour construire le plan de formation de l'année.

Cours 15 · Gestion de projet et conduite du changement en cybersécurité

22 h

OBJECTIFS

- Utiliser une méthode de gestion de projet pour mettre en place une nouvelle organisation de la cybersécurité
- Accompagner le changement au plus près des postes de travail

ÉVALUATION FORMATIVE

Étude de cas : note de cadrage de projet et plan d'accompagnement du changement, QCM

CONTENUS

- Cadrage d'un projet d'organisation de la cybersécurité : objectifs, périmètre, gouvernance
- Méthodes prédictives, agiles et hybrides : choix et adaptation
- Planification, gestion des risques projet et comitologie
- Organisation cible : rôles, responsabilités, relais sécurité
- Analyse des résistances et leviers d'adhésion
- Accompagnement terrain des dispositions locales et internationales
- Suivi de l'appropriation et ajustements

Fil rouge · Camille pilote le projet de réorganisation de la sécurité d'Hydralys et nomme des relais sécurité sur chaque site, face à des équipes de maintenance qui jugent les nouvelles règles contraignantes.

Cours 16 · Anticiper et communiquer en situation de crise cyber

22 h

OBJECTIFS

- Concevoir une communication destinée à anticiper la gestion des crises liées aux intrusions
- Déployer le dispositif de communication de crise dans l'entreprise

ÉVALUATION FORMATIVE

Mise en situation : rédaction d'un plan de communication de crise et de messages types, QCM

CONTENUS

- Anatomie d'une crise cyber : phases, acteurs, enjeux
- Organisation d'une cellule de crise et répartition des rôles
- Guides de l'ANSSI sur la gestion et la communication de crise cyber
- Plan de communication de crise : cibles internes et externes, messages, canaux de secours
- Obligations de notification aux autorités et aux personnes concernées
- Exercices de crise : conception, animation, retour d'expérience
- Préparation des porte-parole et des messages types

Fil rouge · Camille organise le premier exercice de crise d'Hydralys simulant l'arrêt de la télé-exploitation de plusieurs stations, avec communication aux collectivités clientes et aux autorités.

Cours 17 · Accessibilité et multiculturalité dans le management de la cybersécurité

22 h

OBJECTIFS

- Adapter le management interne de la cybersécurité aux personnes handicapées en prenant en compte le RGAA et les WCAG 2.1 au niveau AAA
- Prendre en compte la multiculturalité des personnels pour adapter la diffusion et l'appropriation des directives

ÉVALUATION FORMATIVE

Étude de cas : audit d'accessibilité d'un support de sensibilisation et plan d'adaptation interculturelle, QCM

CONTENUS

- Handicap et cybersécurité : enjeux d'inclusion et obligations de l'employeur
- RGAA et WCAG 2.1 : principes, critères et niveau AAA
- Accessibilité des supports de sensibilisation, des procédures et des outils d'authentification
- Adaptation des postes et des parcours de formation
- Dimensions culturelles et rapport à la règle, à la hiérarchie et au risque
- Adaptation des messages et des directives à des équipes internationales
- Évaluation de l'inclusion du dispositif de sécurité

Fil rouge · Camille découvre qu'un collaborateur malvoyant ne peut pas utiliser la nouvelle solution d'authentification et que les consignes sont mal comprises sur le site marocain : elle adapte outils et communication.

RNCP40246BC05 · 66 h

Gérer les aspects budgétaires et financiers de la cyber sécurité

Cours 18 · Budget prévisionnel et plan de financement du projet de cybersécurité

22 h

OBJECTIFS

- Estimer les investissements (coûts et calendrier) et déterminer les besoins de financement du projet
- Négocier les conditions de financement en tenant compte des évolutions technologiques pour construire un budget fiable à moyen terme

ÉVALUATION FORMATIVE

Étude de cas : construction d'un budget prévisionnel et d'un argumentaire de financement, QCM

CONTENUS

- Typologie des coûts : investissement, fonctionnement, licences, prestations, ressources humaines
- Méthodes d'estimation des coûts et construction du calendrier de dépenses
- Coût du risque et argumentaire de retour sur investissement sécurité
- Modes de financement : budget interne, location, abonnement, aides publiques
- Anticipation de l'obsolescence et des évolutions technologiques
- Négociation avec la direction financière et les fournisseurs
- Formalisation du budget prévisionnel pluriannuel

Fil rouge · Camille chiffre le programme de sécurisation d'Hydralys sur trois ans et doit convaincre le directeur administratif et financier de financer une partie en abonnement plutôt qu'en investissement.

Cours 19 · Contrôle de gestion, tableaux de bord et analyse des écarts

22 h

OBJECTIFS

- Choisir des indicateurs de suivi budgétaire adaptés à la cybersécurité et constituer les tableaux de bord
- Analyser en continu les écarts budgétaires et décider des mesures correctives

ÉVALUATION FORMATIVE

Exercice pratique : construction d'un tableau de bord et analyse d'écarts sur un jeu de données fictif, QCM

CONTENUS

- Principes du contrôle de gestion appliqués à la fonction sécurité
- Indicateurs budgétaires, de performance et de pilotage des risques
- Conception de tableaux de bord conformes aux standards de l'entreprise
- Suivi de l'engagement et de la consommation budgétaire
- Analyse des écarts : volume, prix, calendrier
- Mesures correctives et arbitrages
- Reporting au comité de direction

Fil rouge · Six mois après le lancement du programme, le tableau de bord de Camille révèle un dépassement sur les prestations d'audit : elle analyse l'écart et propose un arbitrage au comité de direction.

Cours 20 · Suivi des contrats de sous-traitance et des garanties financières

22 h

OBJECTIFS

- Assurer le suivi des contrats de sous-traitance des systèmes de sécurité
- Vérifier régulièrement la solidité des garanties financières des prestataires pour éviter les ruptures de service

ÉVALUATION FORMATIVE

Étude de cas sur la défaillance d'un sous-traitant et QCM final de bloc

CONTENUS

- Cadre contractuel : engagements de niveau de service, pénalités, réversibilité
- Exigences de sécurité de la chaîne d'approvisionnement dans NIS2
- Évaluation de la santé financière d'un prestataire : sources et indicateurs
- Garanties financières, assurances et clauses de continuité
- Revue périodique des fournisseurs et plan de contrôle
- Gestion de la défaillance d'un prestataire et plan de sortie
- Synthèse de fin de parcours : présentation du programme de cybersécurité d'Hydralys

Fil rouge · Le prestataire de maintenance des pare-feu d'Hydralys montre des signes de fragilité financière : Camille vérifie ses garanties, active les clauses prévues et prépare un plan de sortie.

05 · CONFORMITÉ AU RÉFÉRENTIEL

Couverture des compétences

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

Compétence	Bloc	Cours
Analyser une situation géopolitique propice aux cyberattaques et cartographier les menaces	RNCP40246BC01	1
Conduire un audit du SI et des réseaux pour identifier les vulnérabilités	RNCP40246BC01	2, 9
Dresser un état des dommages potentiels sur les données en vue d'un cahier des charges	RNCP40246BC01	3
Se conformer à l'ISO 27032 et à la directive NIS2 dans le cadre du budget	RNCP40246BC01	3, 8
Organiser la surveillance de l'environnement concurrentiel	RNCP40246BC01	4
Établir le schéma général de la cybersécurité et l'architecture cible	RNCP40246BC02	5
Traduire les attentes en spécifications techniques pour un appel d'offres	RNCP40246BC02	6
Coordonner la rédaction du cahier des charges et de l'appel d'offres	RNCP40246BC02	6
Concevoir et organiser les systèmes de sauvegarde selon la stratégie cloud	RNCP40246BC02	7
Définir les contenus de formation des utilisateurs à la sécurité cloud (IaaS, PaaS, SaaS)	RNCP40246BC02	7
Concevoir et utiliser un système de veille légale et réglementaire	RNCP40246BC02	8
Établir le catalogue des risques d'intrusion selon les principes du hacking éthique	RNCP40246BC03	9
Définir une PSSI selon les recommandations de l'ANSSI	RNCP40246BC03	10
Évaluer les potentialités de l'IA en cybersécurité offensive et défensive	RNCP40246BC03	11
Identifier les risques d'atteinte aux infrastructures physiques	RNCP40246BC03	12
Optimiser la fourniture d'énergie et les dispositifs de secours	RNCP40246BC03	12
Protéger l'accès aux stockages et aux données par codes d'accès et chiffrement	RNCP40246BC03	13
Établir le schéma général de la sûreté de fonctionnement	RNCP40246BC03	13
Analyser les compétences du personnel et concevoir un plan de formation	RNCP40246BC04	14
Utiliser une méthode de gestion de projet pour une nouvelle organisation de la cybersécurité	RNCP40246BC04	15
Accompagner le changement au plus près des postes de travail	RNCP40246BC04	15
Concevoir et déployer une communication d'anticipation des crises cyber	RNCP40246BC04	16
Prendre en compte le RGAA et les WCAG 2.1 niveau AAA	RNCP40246BC04	17
Prendre en compte la multiculturalité des personnels	RNCP40246BC04	17
Estimer les investissements (coûts et calendrier)	RNCP40246BC05	18
Négocier les conditions de financement pour un budget fiable à moyen terme	RNCP40246BC05	18
Choisir des indicateurs de suivi budgétaire et constituer les tableaux de bord	RNCP40246BC05	19
Analyser en continu les écarts budgétaires et décider des mesures correctives	RNCP40246BC05	19
Assurer le suivi des contrats de sous-traitance et des garanties financières	RNCP40246BC05	6, 20

Évaluations formatives

Chaque cours intègre des évaluations formatives régulières : QCM de validation à la fin de chaque sous-chapitre et de chaque cours, études de cas issues du fil rouge Hydralys, exercices de rédaction (notes de synthèse, extraits de cahier des charges, chapitres de PSSI, plans de communication) et mises en situation professionnelles. Les QCM offrent une correction immédiate et commentée ; les productions écrites sont accompagnées de grilles critériées permettant l'autoévaluation et, selon l'organisation retenue par l'organisme de formation, une correction par un formateur ou un tuteur. Les résultats sont tracés sur la plateforme, ce qui permet à l'organisme de formation de suivre la progression de chaque apprenant et de documenter l'atteinte des objectifs dans le cadre de sa démarche Qualiopi.

Modalités de certification

Bloc	Modalité d'évaluation
RNCP40246BC01	Travaux écrits (notes de synthèse relatives aux études de cas, rapports d'activité), étude de cas dont les supports sont proposés par les entreprises partenaires du certificateur, mise en situation professionnelle durant les périodes en entreprise et présentation orale individuelle devant le jury.
RNCP40246BC02	Questionnaire, travaux écrits (notes de synthèse relatives aux études de cas, rapports d'activité), mise en situation professionnelle durant les périodes en entreprise et présentation orale individuelle devant le jury.
RNCP40246BC03	Travaux écrits (notes de synthèse relatives aux études de cas, rapports d'activité), mise en situation professionnelle durant les périodes en entreprise et présentation orale individuelle devant le jury.

RNCP40246BC04	Travaux écrits (notes de synthèse relatives aux études de cas, rapports d'activité), mise en situation professionnelle durant les périodes en entreprise et présentation orale individuelle devant le jury.
RNCP40246BC05	Travaux écrits (notes de synthèse relatives aux études de cas, rapports d'activité), mise en situation professionnelle durant les périodes en entreprise et présentation orale individuelle devant le jury.

Le parcours reproduit la logique des épreuves du référentiel. Les études de cas du fil rouge Hydralys entraînent l'apprenant à rédiger des notes de synthèse argumentées et des rapports d'activité structurés, formats attendus pour les travaux écrits de chaque bloc. Les QCM réguliers préparent au questionnaire du bloc 2. Les mises en situation sont conçues pour être transposées dans l'entreprise d'accueil de l'apprenant, afin de nourrir les mises en situation professionnelles évaluées durant les périodes en entreprise. Enfin, les livrables produits au fil des cours (cartographie des menaces, architecture cible, PSSI, plan de continuité, plan de communication de crise, budget) constituent la matière de la présentation orale individuelle devant le jury. SFM fournit le contenu pédagogique ; l'organisme de formation reste responsable de l'inscription des candidats, de l'organisation des épreuves et de la relation avec le certificateur.

Moyens pédagogiques et débouchés

Moyens pédagogiques et techniques

- Plateforme e-learning en marque blanche accessible 24 h/24, avec suivi de progression et traçabilité des résultats
- Une vidéo de 3 à 5 minutes par sous-chapitre, représentant 30 % du volume horaire du parcours
- Cours textes enrichis, infographies et fiches de synthèse téléchargeables pour chaque sous-chapitre
- Études de cas et mises en situation scénarisées autour du fil rouge Hydralys
- QCM de validation à correction immédiate et grilles critériées pour les productions écrites
- Modèles de livrables professionnels : rapport d'audit, cahier des charges, PSSI, plan de continuité, plan de communication de crise, budget et tableau de bord
- Sélection commentée de ressources institutionnelles de référence (ANSSI, CNIL, ENISA, CERT-FR) pour prolonger les apprentissages

Débouchés et évolutions

- Manager de la cyber sécurité
- Responsable de la sécurité des systèmes d'information (RSSI)
- Expert en sécurité des SI
- Expert cyber défense
- Ingénieur cyber sécurité
- Consultant en sécurité des SI

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 RNCP40246 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.