

SCHOOL FOR MATE

LIVRET PÉDAGOGIQUE

Expert en cybersécurité et sécurité informatique

RNCP41976 · Certification RNCP · Niveau 7

Ce parcours de 440 heures prépare aux quatre blocs de compétences de la certification RNCP41976 « Expert en cybersécurité et sécurité informatique » (niveau 7) : analyse des risques et audit, architecture de sécurité, pilotage de projet agile et gouvernance en amélioration continue. Construit autour d'une entreprise fictive soumise à de fortes exigences réglementaires, il fait progresser l'apprenant d'un rôle d'ingénieur cybersécurité vers des responsabilités de pilotage stratégique de la sécurité du système d'information.

VOLUME HORAIRE	COURS	BLOCS
440 h	20	4

01 · PRÉSENTATION

La formation en bref

Intitulé	Expert en cybersécurité et sécurité informatique
Code	RNCP41976
Type	Certification RNCP
Niveau	Niveau 7
Certificateur	ASSOCIATION INTERNATIONALE POUR LA FORMATION, ASSOCIATION POUR LA FORMATION A L'INFORMATIQUE ET AU NUMERIQUE
Durée	440 h, 20 cours
Modalité	Formation à distance (e-learning), tutorat assuré par l'organisme de formation
Formats	SCORM 1.2 / 2004, xAPI, sources éditables
Mise à jour	Novembre 2026
Fin d'enregistrement de la certification	27/02/2028

Le métier et les compétences visées

L'expert en cybersécurité et sécurité informatique protège le système d'information d'une organisation face à des menaces en évolution constante. Il évalue les vulnérabilités et les risques, audite la conformité aux cadres applicables (RGPD, NIS2, DORA, ISO/IEC 27001, recommandations de l'ANSSI) et définit la politique de sécurité. Il conçoit des architectures de sécurité techniques et organisationnelles, structure un centre opérationnel de sécurité (SOC) et orchestre les outils de détection et de réponse, y compris des solutions de détection comportementale fondées sur l'intelligence artificielle. Il pilote les projets de déploiement de la stratégie cyber en mode agile, coordonne équipes et prestataires, puis supervise la gouvernance de la sécurité : indicateurs, revues, tests de PCA/PRA, communication avec les parties prenantes et sensibilisation au « security by design ».

Public visé

- Titulaires d'un diplôme ou titre de niveau 6 en informatique souhaitant se spécialiser en cybersécurité
- Administrateurs systèmes et réseaux, ingénieurs infrastructure ou cloud visant un poste d'ingénieur ou d'architecte sécurité
- Analystes SOC, auditeurs ou consultants juniors en sécurité souhaitant évoluer vers des fonctions d'expertise et de pilotage
- Chefs de projet informatique et professionnels de la gouvernance des SI s'orientant vers la GRC et la fonction RSSI
- Alternants inscrits dans un cursus de niveau 7 en informatique au sein d'un organisme de formation ou d'un CFA

Prérequis

- Parcours en 5 ans : être titulaire d'un baccalauréat ou d'une certification de niveau 4
- Admission en 3e année : être titulaire d'un diplôme ou titre de niveau 5 dans le domaine de l'informatique (parcours en 3 ans) ; admission en 4e année : être titulaire d'un diplôme ou titre de niveau 6 dans le domaine de l'informatique (parcours en 2 ans)
- À défaut, admission exceptionnelle possible sur dossier de candidature examiné par une commission de l'organisme de formation, dans le cadre d'une Validation des Acquis Professionnels et Personnels (VAPP)
- Pour tous les candidats : fournir la copie du dernier diplôme ou titre obtenu

Objectifs pédagogiques

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

- Évaluer les vulnérabilités et cartographier les risques d'un système d'information à l'aide de méthodes reconnues (EBIOS Risk Manager, ISO/IEC 27005, NIST SP 800-30)
- Auditer la conformité réglementaire et normative d'une organisation et formuler des recommandations correctives priorisées
- Définir une politique de sécurité du SI alignée sur la stratégie de l'organisation et la décliner en plan d'actions et en dispositifs PCA/PRA
- Concevoir et documenter une architecture de sécurité technique et organisationnelle intégrée en mobilisant TOGAF, COBIT et ISO/IEC 27001
- Structurer un SOC et configurer les outils de supervision, de détection comportementale et d'automatisation de la réponse (SIEM, EDR, UEBA, SOAR)
- Évaluer la robustesse d'une architecture par des tests d'intrusion et des exercices Red Team, Blue Team et Purple Team appuyés sur MITRE ATT&CK
- Planifier, conduire et piloter en mode agile un projet de déploiement de la stratégie de cybersécurité, prestataires et reporting compris
- Animer une équipe projet de manière inclusive et organiser un partage d'information sécurisé et accessible
- Superviser la gouvernance de la sécurité par des indicateurs, des revues périodiques, des tests de PCA/PRA et un pilotage des actions correctives
- Concevoir des programmes de sensibilisation accessibles et une communication stratégique adaptée à chaque partie prenante

02 · FIL ROUGE PÉDAGOGIQUE

Hélionys Réseaux

IM

Inès Marchetti

Ingénieure cybersécurité rattachée au RSSI, puis adjointe au RSSI en charge de la gouvernance et des opérations de sécurité

Énergie : production et distribution de chaleur urbaine et services énergétiques aux collectivités (entité concernée par NIS2)

Hélionys Réseaux exploite des réseaux de chaleur urbains dans plusieurs agglomérations et pilote ses chaufferies via des systèmes industriels (OT) interconnectés au SI de gestion. Son SI s'est construit par acquisitions successives : plusieurs annuaires, un cloud public partiellement maîtrisé, des prestataires d'infogérance et de maintenance industrielle aux accès distants peu contrôlés. Une tentative d'intrusion par hameçonnage ciblé sur la direction financière vient d'être détectée tardivement. La direction générale doit en parallèle préparer la mise en conformité NIS2 et répondre aux exigences de ses collectivités clientes. Elle confie au RSSI, Bertrand Lacombe, un programme de transformation de la sécurité sur trois ans. Inès Marchetti, recrutée pour l'appuyer, va analyser les risques, concevoir l'architecture cible, piloter le déploiement et installer une gouvernance durable de la cybersécurité.

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

La progression

1. Bloc 1 : Inès cartographie les actifs critiques, mène l'analyse de risques EBIOS RM et l'audit de conformité NIS2 et RGPD, puis rédige la PSSI, le plan d'actions et les premiers dispositifs PCA/PRA d'Hélionys Réseaux.
2. Bloc 2 : Inès conçoit l'architecture de sécurité cible IT et OT, construit le SOC avec ses outils SIEM, EDR, UEBA et SOAR, puis organise un exercice Purple Team et une preuve de concept de chiffrement post-quantique pour la télégestion des chaufferies.
3. Bloc 3 : Inès pilote en mode agile le projet de déploiement de la stratégie cyber, coordonne les prestataires d'infogérance et de maintenance, anime une équipe projet multisite et inclusive et rend compte au comité de direction.
4. Bloc 4 : Devenue adjointe au RSSI, Inès installe le tableau de bord de gouvernance, conduit les revues et les tests de PCA/PRA, pilote les actions correctives, représente Hélionys Réseaux auprès de son écosystème sectoriel et déploie le programme de sensibilisation « security by design ».

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
RNCP41976BC01 · Analyser les risques et auditer la sécurité d'un système d'information		**110 h**
1	Cartographier le SI et évaluer les vulnérabilités internes et externes	22 h
2	Identifier et hiérarchiser les risques avec EBIOS Risk Manager et ISO/IEC 27005	22 h
3	Prioriser dynamiquement les risques et modéliser les impacts des vulnérabilités	22 h
4	Auditer la conformité réglementaire et normative et formuler des recommandations	22 h
5	Définir la politique de sécurité, piloter la veille et concevoir les dispositifs PCA/PRA	22 h
RNCP41976BC02 · Concevoir et piloter une architecture de sécurité		**132 h**
6	Élaborer une architecture de sécurité intégrée, technique et organisationnelle	22 h
7	Modéliser une architecture dynamique et intégrer les solutions de sécurité	22 h
8	Concevoir et développer un centre opérationnel de sécurité (SOC)	22 h
9	Configurer la supervision et implémenter la détection comportementale	22 h
10	Automatiser les contre-mesures avec une plateforme SOAR	22 h
11	Évaluer la robustesse de l'architecture et explorer les solutions innovantes	22 h
RNCP41976BC03 · Piloter un projet de déploiement de la stratégie de sécurité informatique et cybersécurité en mobilisant une démarche agile et innovante		**88 h**
12	Cadrer et planifier le projet de déploiement de la stratégie cyber	22 h
13	Gérer le projet en mode agile et piloter le reporting	22 h
14	Piloter les prestataires et sécuriser le partage d'information du projet	22 h
15	Conduire une équipe projet inclusive, communicante et innovante	22 h
RNCP41976BC04 · Superviser la gouvernance de la sécurité du système d'information dans une logique d'amélioration continue		**110 h**
16	Mesurer l'efficacité de la sécurité et conduire les revues périodiques	22 h
17	Analyser les menaces émergentes et actualiser les dispositifs de sécurité	22 h
18	Tester les PCA/PRA et piloter les actions correctives	22 h
19	Piloter la communication stratégique et animer l'écosystème cyber	22 h
20	Déployer la culture cyber et le security by design	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

RNCP41976BC01 · 110 h

Analyser les risques et auditer la sécurité d'un système d'information

Cours 1 · Cartographier le SI et évaluer les vulnérabilités internes et externes

22 h

OBJECTIFS

- Inventorier et cartographier les actifs critiques et les infrastructures réseau d'une organisation
- Conduire une analyse de vulnérabilités interne et externe à partir d'audits techniques et mesurer l'exposition aux menaces

ÉVALUATION FORMATIVE

QCM de validation des notions et étude de cas : analyse de résultats de scan et priorisation commentée des vulnérabilités

CONTENUS

- Panorama des menaces : acteurs, motivations, vecteurs d'attaque et spécificités des environnements IT, OT et cloud
- Inventaire et cartographie des actifs selon le guide de cartographie du SI de l'ANSSI (vues métier, applicative, infrastructure)
- Méthodologies d'analyse de vulnérabilités : scans authentifiés et non authentifiés, revue de configuration, analyse de la surface d'attaque externe
- Référentiels de scoring des vulnérabilités (CVSS, EPSS) et catalogues de vulnérabilités exploitées
- Audit technique d'annuaires, de pare-feu et d'environnements cloud : points de contrôle et preuves
- Cadre légal des tests de sécurité : autorisations, loi Godfrain, référentiel PASSI
- Rédaction d'un rapport de vulnérabilités exploitable par les équipes techniques et la direction

Fil rouge · Inès dresse la cartographie des actifs d'Hélionys Réseaux, découvre des accès distants de maintenance non recensés vers les chaufferies et produit un premier rapport d'exposition destiné au RSSI.

Cours 2 · Identifier et hiérarchiser les risques avec EBIOS Risk Manager et ISO/IEC 27005

22 h

OBJECTIFS

- Identifier les risques cyber à partir des processus métiers, des actifs critiques et des interdépendances technologiques
- Construire une cartographie des risques hiérarchisée et justifiée selon une méthode reconnue

ÉVALUATION FORMATIVE

Exercice pratique guidé : réalisation des ateliers 1 à 3 d'EBIOS RM sur le cas fil rouge, avec grille de correction

CONTENUS

- Fondamentaux de la gestion des risques : vocabulaire, critères d'acceptation, appétence au risque
- EBIOS Risk Manager : les cinq ateliers, du socle de sécurité aux scénarios opérationnels
- ISO/IEC 27005 et NIST SP 800-30 : comparaison des approches et choix méthodologique
- Analyse des processus métiers, valeurs métier et biens supports
- Cartographie de l'écosystème et des parties prenantes : prestataires, fournisseurs, clients
- Évaluation de la vraisemblance et de la gravité, matrices et cartographies de risques
- Plan de traitement des risques : réduction, transfert, acceptation, refus

Fil rouge · Inès anime les ateliers EBIOS RM avec la direction des opérations et la direction financière d'Hélionys Réseaux pour hiérarchiser les scénarios d'attaque visant la télégestion des réseaux de chaleur.

Cours 3 · Prioriser dynamiquement les risques et modéliser les impacts des vulnérabilités

22 h

OBJECTIFS

- Exploiter des modèles de scoring et d'analyse prédictive, y compris assistés par intelligence artificielle, pour prioriser dynamiquement les risques
- Modéliser les impacts techniques et métiers d'une compromission par la simulation et l'analyse de scénarios en cascade

ÉVALUATION FORMATIVE

Mise en situation : préparation et restitution d'un exercice tabletop, complétée d'un QCM sur les méthodes de scoring

CONTENUS

- Priorisation contextuelle des risques : menaces émergentes, exposition des actifs, criticité métier
- Algorithmes de scoring et moteurs d'analyse prédictive : principes, apports et limites
- Modèles d'évaluation des risques assistés par intelligence artificielle : données d'entrée, biais, explicabilité et gouvernance
- Cartographies dynamiques de dépendances inter-systèmes et identification des points de défaillance critiques
- Analyse de scénarios en cascade : propagation d'une compromission entre IT et OT
- Simulation d'incidents : exercices tabletop, war-gaming et cyber range
- Restitution des impacts aux décideurs : traduction en conséquences opérationnelles, financières et réglementaires

Fil rouge · Inès anime un exercice tabletop simulant un rançongiciel qui se propage du SI de gestion vers la supervision des chaufferies, puis met à jour la priorisation des risques avec un modèle de scoring contextuel.

Cours 4 · Auditer la conformité réglementaire et normative et formuler des recommandations

22 h

OBJECTIFS

- Identifier et classer par criticité les écarts de conformité aux référentiels applicables
- Élaborer des plans d'action correctifs ou compensatoires priorisés et alignés sur la stratégie de l'organisation

ÉVALUATION FORMATIVE

Étude de cas : rédaction d'un extrait de rapport d'audit avec tableau des écarts classés par criticité

CONTENUS

- Cartographie des exigences : RGPD, NIS2, DORA, règlement sur la cyberrésilience (CRA), LPM, recommandations de l'ANSSI
- Famille ISO/IEC 27000 : exigences de l'ISO/IEC 27001 et mesures de l'ISO/IEC 27002
- Conduite d'un audit selon l'ISO 19011 : programme, entretiens, échantillonnage, preuves
- Revue documentaire : politiques, procédures, preuves de mise en œuvre
- Outils de gouvernance, risque et conformité (GRC) : référentiels de contrôles, suivi des écarts
- Classement des non-conformités par criticité et formulation de mesures correctives ou compensatoires
- Rédaction du rapport d'audit et présentation des recommandations à la direction

Fil rouge · Inès réalise l'audit de conformité NIS2 et RGPD d'Hélionys Réseaux, relève l'absence de clauses de sécurité dans les contrats de maintenance et propose un plan de mise en conformité priorisé.

Cours 5 · Définir la politique de sécurité, piloter la veille et concevoir les dispositifs PCA/PRA

22 h

OBJECTIFS

- Définir les objectifs stratégiques de cybersécurité et élaborer une PSSI déclinée en plan d'actions priorisé
- Piloter une veille stratégique, technique et réglementaire et concevoir des dispositifs PCA/PRA respectant les RTO/RPO

ÉVALUATION FORMATIVE

Livrable formatif : plan d'actions priorisé et fiche BIA, évalués avec une grille critériée, suivi d'un QCM

CONTENUS

- Objectifs stratégiques de cybersécurité et référentiels de gouvernance : COBIT, ISO/IEC 27001
- Rédaction d'une PSSI : structure, périmètre, rôles et responsabilités, validation
- Évaluation de la maturité du SI et construction d'un plan d'actions sous contrainte budgétaire
- Organisation de la veille : sources spécialisées, outils d'automatisation, détection des signaux faibles
- Analyse d'impact métier (BIA) et définition des RTO/RPO
- Conception des PCA et PRA selon l'ISO 22301 : scénarios de sinistre, dépendances critiques, stratégies de reprise
- Alignement des dispositifs de continuité avec les exigences réglementaires (NIS2, DORA)

Fil rouge · Inès présente au comité de direction d'Hélionys Réseaux la PSSI et la feuille de route triennale, puis conduit l'analyse d'impact métier qui fixe les RTO de la télégestion des chaufferies.

RNCP41976BC02 · 132 h

Concevoir et piloter une architecture de sécurité

Cours 6 · Élaborer une architecture de sécurité intégrée, technique et organisationnelle

22 h

OBJECTIFS

- Élaborer une architecture de sécurité intégrée à partir des processus critiques, des contraintes réglementaires et des menaces ciblées
- Structurer l'architecture technique et organisationnelle en mobilisant TOGAF, COBIT, ISO/IEC 27001 et des outils de modélisation formelle

ÉVALUATION FORMATIVE

Exercice de modélisation : production d'une vue d'architecture cible commentée, évaluée par grille critériée

CONTENUS

- Principes d'architecture de sécurité : défense en profondeur, moindre privilège, Zero Trust, cloisonnement
- Cadres d'architecture et de gouvernance : TOGAF, COBIT, ISO/IEC 27001
- Analyse croisée des processus métiers critiques, contraintes sectorielles et scénarios de menaces
- Architecture technique : segmentation réseau, IAM, sécurisation des environnements hybrides et des systèmes industriels
- Architecture organisationnelle : flux d'information transverses, rôles, instances de gouvernance
- Modélisation formelle d'architecture : notation ArchiMate et vues de sécurité
- Documentation technique et fonctionnelle de l'architecture cible

Fil rouge · Inès conçoit l'architecture cible d'Hélionys Réseaux qui sépare le SI de gestion et les réseaux industriels, et formalise les instances de gouvernance entre DSI, exploitation et RSSI.

Cours 7 · Modéliser une architecture dynamique et intégrer les solutions de sécurité

22 h

OBJECTIFS

- Modéliser une architecture de sécurité dynamique avec ses flux sécurisés, mécanismes de défense et indicateurs de performance
- Sélectionner sur une base multicritère, déployer et configurer des dispositifs techniques de sécurité adaptés

ÉVALUATION FORMATIVE

Étude de cas : grille de sélection multicritère justifiée et plan de déploiement, suivis d'un QCM

CONTENUS

- Architecture dynamique : détection proactive, évaluation continue et capacité d'adaptation
- Orchestration des flux de données sécurisés et documentation des interdépendances techniques
- Indicateurs de performance de l'architecture (KPI et KRI)
- Sélection multicritère des solutions : efficacité, interopérabilité, coût, scalabilité
- Panorama des dispositifs : pare-feu nouvelle génération, passerelles de messagerie, IAM et PAM, chiffrement, protection du cloud
- Pilotage du déploiement et configuration fine dans les environnements cibles
- Recommandations de l'ANSSI et guides de durcissement

Fil rouge · Inès compare trois solutions de gestion des accès à privilèges pour encadrer les accès distants des mainteneurs d'Hélionys Réseaux et pilote le déploiement de la solution retenue.

Cours 8 · Concevoir et développer un centre opérationnel de sécurité (SOC)

22 h

OBJECTIFS

- Définir le périmètre fonctionnel, technique et organisationnel d'un SOC
- Structurer les processus de détection, d'analyse, d'investigation numérique et de réponse aux incidents, et constituer l'équipe dédiée

ÉVALUATION FORMATIVE

Livrable formatif : dossier de conception de SOC (périmètre, processus, organisation) évalué par grille critériée

CONTENUS

- Modèles de SOC : interne, externalisé, hybride, et critères de choix
- Périmètre de supervision et sources de journaux prioritaires
- Intégration des outils : SIEM, EDR, SOAR et plateformes de Threat Intelligence
- Processus de détection, de qualification et d'escalade des alertes
- Investigation numérique post-incident (forensic) : collecte, préservation des preuves, analyse
- Réponse aux incidents selon l'ISO/IEC 27035 et articulation avec la gestion de crise
- Organisation et compétences de l'équipe SOC : niveaux d'analystes, astreintes, montée en compétences

Fil rouge · Inès rédige le dossier de conception du SOC hybride d'Hélionys Réseaux, répartit les missions entre l'équipe interne et un prestataire de supervision et définit le processus d'escalade.

Cours 9 · Configurer la supervision et implémenter la détection comportementale

22 h

OBJECTIFS

- Paramétrer les outils SIEM et EDR, définir des règles de corrélation multi-sources, des seuils d'alerte et des tableaux de bord
- Implémenter des modèles de détection comportementale (UEBA, intelligence artificielle) et réduire les faux positifs

ÉVALUATION FORMATIVE

Exercice pratique : rédaction de règles de corrélation à partir de journaux fournis et analyse des faux positifs

CONTENUS

- Collecte et normalisation des journaux : sources, formats, rétention
- Règles de corrélation multi-sources et ingénierie de la détection
- Seuils d'alerte contextuelle et tableaux de bord de supervision
- Configuration des politiques EDR et réponse sur les terminaux
- Principes de l'UEBA : profils de référence, détection d'anomalies, scoring d'entités
- Entraînement de modèles d'intelligence artificielle sur des jeux de données représentatifs
- Optimisation des algorithmes et réduction des faux positifs

Fil rouge · Inès crée les règles de corrélation qui auraient détecté plus tôt l'hameçonnage de la direction financière d'Hélionys Réseaux et calibre un modèle UEBA sur les comptes à privilèges.

Cours 10 · Automatiser les contre-mesures avec une plateforme SOAR

22 h

OBJECTIFS

- Déployer une plateforme d'orchestration, d'automatisation et de réponse aux incidents intégrée aux outils existants
- Développer des playbooks automatisant détection, analyse et remédiation afin de réduire le temps de réponse

ÉVALUATION FORMATIVE

Mise en situation : modélisation d'un playbook complet, évaluée par grille, et QCM de validation

CONTENUS

- Rôle du SOAR dans la chaîne de détection et de réponse
- Intégration avec le SIEM, l'EDR, l'IAM, la messagerie et la Threat Intelligence
- Conception de playbooks : déclencheurs, enrichissement, décisions, actions
- Niveaux d'automatisation et validation humaine des actions sensibles
- Playbooks types : hameçonnage, compte compromis, poste infecté
- Tests, maintien en conditions opérationnelles et versionnement des playbooks
- Mesure du temps de détection et du temps de réponse

Fil rouge · Inès conçoit le playbook de traitement des signalements d'hameçonnage d'Hélionys Réseaux, qui isole automatiquement le message et désactive le compte compromis après validation d'un analyste.

Cours 11 · Évaluer la robustesse de l'architecture et explorer les solutions innovantes

22 h

OBJECTIFS

- Piloter des campagnes de tests d'intrusion et d'exercices Red Team, Blue Team et Purple Team appuyées sur des cadres de référence
- Évaluer des technologies émergentes de sécurisation des communications sensibles au moyen de preuves de concept

ÉVALUATION FORMATIVE

Étude de cas : analyse d'un rapport de test d'intrusion avec cartographie MITRE ATT&CK des techniques observées

CONTENUS

- Tests d'intrusion contrôlés : cadrage, conventions, périmètre, restitution
- Exercices Red Team, Blue Team et Purple Teaming
- Cadres de référence : MITRE ATT&CK, NIST SP 800-53, TIBER-EU, ISO/IEC 27035
- Exercices de gestion de crise et de réponse à incident
- Analyse des vulnérabilités résiduelles et plan de remédiation
- Technologies émergentes : cryptographie post-quantique, chiffrement de bout en bout, blockchain, sécurisation de l'IoT et de l'edge computing
- Conduite d'une preuve de concept et de tests de performance

Fil rouge · Inès pilote un exercice Purple Team sur le scénario d'attaque prioritaire d'Hélionys Réseaux, puis réalise une preuve de concept de chiffrement post-quantique pour les flux de télégestion.

RNCP41976BC03 · 88 h

Piloter un projet de déploiement de la stratégie de sécurité informatique et cybersécurité en mobilisant une démarche agile et innovante

Cours 12 · Cadrer et planifier le projet de déploiement de la stratégie cyber

22 h

OBJECTIFS

- Recueillir et formaliser les exigences utilisateurs d'un projet de sécurité
- Planifier le projet en tâches et livrables en répartissant les ressources humaines, techniques et financières

ÉVALUATION FORMATIVE

Livrable formatif : note de cadrage et planning du projet évalués par grille critériée

CONTENUS

- Spécificités des projets de cybersécurité : contraintes, parties prenantes, risques projet
- Recueil et formalisation des exigences utilisateurs
- Rédaction et lecture critique d'un cahier des charges
- Découpage du projet : structure de découpage, lots, livrables, jalons
- Estimation des charges et répartition des ressources humaines, techniques et financières
- Construction du planning et du budget, gestion des dépendances
- Organisation du cycle de vie du projet

Fil rouge · Inès cadre le projet de déploiement de la stratégie cyber d'Hélionys Réseaux, recueille les exigences des sites d'exploitation et construit le planning et le budget soumis au comité de pilotage.

Cours 13 · Gérer le projet en mode agile et piloter le reporting

22 h

OBJECTIFS

- Gérer un projet de sécurité avec des méthodes et outils agiles adaptés
- Élaborer des tableaux de bord de suivi pour le commanditaire et corriger les écarts en temps réel

ÉVALUATION FORMATIVE

Exercice pratique : construction d'un tableau de bord de suivi à partir de données projet fournies

CONTENUS

- Méthodes agiles : Scrum, Kanban, cadres d'agilité à l'échelle
- Choix et justification d'une méthodologie pour un projet de cybersécurité
- Gestion du backlog sécurité, priorisation et rituels
- Outils de gestion de projet et de suivi agile
- Indicateurs de suivi : avancement, consommation des ressources, vélocité, budget
- Tableaux de bord pour le commanditaire et comité de pilotage
- Détection et correction des écarts, gestion des risques projet

Fil rouge · Inès organise le déploiement de l'EDR sur les sites d'Hélionys Réseaux en sprints et présente chaque mois au directeur général un tableau de bord d'avancement et de consommation budgétaire.

Cours 14 · Piloter les prestataires et sécuriser le partage d'information du projet

22 h

OBJECTIFS

- Piloter les prestataires gérant les ressources du SI existant, vérifier la pertinence des contrats et définir les KPI de suivi
- Établir un processus de partage d'information sécurisé et accessible aux parties prenantes

ÉVALUATION FORMATIVE

Étude de cas : analyse d'un contrat d'infogérance et construction d'un tableau de bord prestataire

CONTENUS

- Identification des prestataires à partir de la cartographie du SI
- Présentation du projet, des rôles et des objectifs aux parties prenantes externes
- Analyse des contrats existants : clauses de sécurité, niveaux de service, réversibilité
- KPI et tableaux de bord de suivi des prestataires
- Identification des besoins d'information des parties prenantes
- Choix des outils collaboratifs et de partage, protocoles et procédures
- Sécurisation et accessibilité de l'information projet : classification, droits d'accès

Fil rouge · Inès réunit l'infogérant et le mainteneur industriel d'Hélionys Réseaux, renégocie les engagements de sécurité et met en place un espace projet partagé aux droits d'accès maîtrisés.

Cours 15 · Conduire une équipe projet inclusive, communicante et innovante

22 h

OBJECTIFS

- Conduire l'équipe projet en favorisant l'inclusion et en adaptant les conditions de travail aux contraintes
- Définir un processus de communication inclusif et animer des démarches d'innovation collective

ÉVALUATION FORMATIVE

Mise en situation : préparation d'un ordre du jour de réunion et d'un plan de communication d'équipe, évalués par grille

CONTENUS

- Constitution et présentation de l'équipe projet : rôles, complémentarités
- Inclusion des personnes en situation de handicap et adaptation des conditions de travail
- Gestion de la pression, des incertitudes et de l'équilibre entre vie professionnelle et personnelle
- Communication inclusive : contexte, cultures, langues, équipes multisites
- Rituels de synchronisation et ordres du jour de réunion
- Animation de séances de brainstorming et techniques de créativité
- Recueil de retours réguliers et développement de l'autonomie et de l'initiative

Fil rouge · Inès adapte l'organisation de son équipe projet, qui compte une analyste malentendante et un prestataire anglophone, et anime un atelier de créativité sur l'adhésion des exploitants aux nouvelles règles d'accès.

RNCP41976BC04 · 110 h

Superviser la gouvernance de la sécurité du système d'information dans une logique d'amélioration continue

Cours 16 · Mesurer l'efficacité de la sécurité et conduire les revues périodiques

22 h

OBJECTIFS

- Définir des indicateurs de performance et d'efficacité des mesures de sécurité, y compris d'accessibilité et d'inclusivité
- Réaliser des revues périodiques des politiques et procédures et recommander les ajustements

ÉVALUATION FORMATIVE

Livrable formatif : tableau de bord d'indicateurs commenté, suivi d'un QCM

CONTENUS

- Mesure de la sécurité selon l'ISO/IEC 27004 : indicateurs, mesures, critères de décision
- Indicateurs opérationnels, réglementaires et d'inclusion
- Indicateurs d'accessibilité des dispositifs de sécurité numérique
- Configuration des outils de collecte et d'analyse des données
- Conception d'un tableau de bord de gouvernance
- Organisation des revues périodiques des politiques et procédures
- Outils de reporting et formulation des recommandations d'ajustement

Fil rouge · Promue adjointe au RSSI, Inès construit le tableau de bord de gouvernance d'Hélionys Réseaux et conduit la première revue annuelle de la PSSI.

Cours 17 · Analyser les menaces émergentes et actualiser les dispositifs de sécurité

22 h

OBJECTIFS

- Analyser les tendances et les menaces émergentes à partir de plateformes de veille et de référentiels
- Piloter l'actualisation des dispositifs techniques, organisationnels et documentaires

ÉVALUATION FORMATIVE

Étude de cas : rapport de tendances de veille et plan de mise à jour des dispositifs

CONTENUS

- Plateformes de Threat Intelligence, avis des CERT et publications de l'ANSSI
- Analyse des groupes de menace (APT) et de l'évolution des vecteurs d'attaque avec MITRE ATT&CK
- Menaces liées aux IA génératives : hameçonnage automatisé, code malveillant, manipulation de l'information
- Rédaction d'un rapport de tendances et alignement de la stratégie
- Suivi des évolutions réglementaires et normatives
- Mise à jour des outils, procédures, politiques et référentiels documentaires
- Intégration des exigences d'accessibilité numérique et d'inclusivité

Fil rouge · Inès analyse une campagne d'un groupe APT ciblant le secteur de l'énergie et pilote la mise à jour des règles de détection et des procédures d'Hélionys Réseaux.

Cours 18 · Tester les PCA/PRA et piloter les actions correctives

22 h

OBJECTIFS

- Définir et organiser des exercices de test des PCA/PRA représentatifs des risques critiques et analyser les écarts
- Consolider les résultats des revues, audits et tests et piloter les actions correctives priorisées

ÉVALUATION FORMATIVE

Mise en situation : synthèse d'exercice PCA/PRA (objectifs, écarts, préconisations) et planning des actions correctives

CONTENUS

- Objectifs et typologie des tests : revue documentaire, exercice sur table, exercice technique, exercice grandeur nature
- Construction de scénarios représentatifs des risques critiques
- Organisation coordonnée avec les parties prenantes métiers et IT
- Analyse des écarts et dysfonctionnements, synthèse de l'exercice
- Consolidation des résultats de revues, audits et tests
- Priorisation et planification des actions correctives, y compris d'accessibilité et d'inclusivité
- Suivi des actions avec des outils de gestion de projet et des référentiels de gouvernance

Fil rouge · Inès organise un exercice de reprise après la perte du centre de supervision des chaufferies d'Hélionys Réseaux, constate un dépassement du RTO et pilote le plan correctif associé.

Cours 19 · Piloter la communication stratégique et animer l'écosystème cyber

22 h

OBJECTIFS

- Élaborer des supports de reporting adaptés à chaque partie prenante et coordonner les échanges via des canaux sécurisés
- Animer l'écosystème cyber de l'organisation et capitaliser sur les incidents par l'analyse de cause racine

ÉVALUATION FORMATIVE

Exercice pratique : élaboration d'un support de reporting pour la direction et d'une fiche RCA

CONTENUS

- Consolidation des résultats des indicateurs, audits et veille
- Supports de reporting : comité de direction, métiers, équipes techniques
- Échanges avec partenaires, prestataires et autorités : notification d'incidents, canaux sécurisés
- Communication de crise cyber
- Réseaux professionnels et initiatives sectorielles : CERT, CSIRT régionaux, clubs de RSSI
- Participation aux exercices collaboratifs de gestion de crise
- Retours d'expérience et analyse de cause racine (RCA)

Fil rouge · Inès présente le bilan cyber annuel au conseil d'administration d'Hélionys Réseaux, représente l'entreprise lors d'un exercice de crise sectoriel et anime le retour d'expérience de l'incident d'hameçonnage.

Cours 20 · Déployer la culture cyber et le security by design

22 h

OBJECTIFS

- Concevoir des programmes de sensibilisation et de formation adaptés aux profils et accessibles aux personnes en situation de handicap
- Intégrer les standards du security by design et évaluer la montée en compétences des parties prenantes

ÉVALUATION FORMATIVE

Livrable formatif : plan de programme de sensibilisation avec quiz de validation, puis QCM de synthèse du parcours

CONTENUS

- Diagnostic de la culture cyber et identification des publics : utilisateurs, développeurs, chefs de projet, décideurs
- Ingénierie d'un programme de sensibilisation : objectifs, formats, calendrier
- Accessibilité des contenus : principes du RGAA et adaptation aux situations de handicap
- Standards du security by design : intégration de la sécurité dans les projets, développement sécurisé, recommandations de l'ANSSI
- Modules pratiques : campagnes d'hameçonnage simulé, ateliers de modélisation des menaces
- Évaluation de la montée en compétences : mises en situation et quiz
- Synthèse du parcours et méthodologie de préparation des dossiers et soutenances de certification

Fil rouge · Inès lance le programme de sensibilisation d'Hélionys Réseaux, avec un parcours security by design pour les chefs de projet et des contenus accessibles aux collaborateurs malvoyants.

Couverture des compétences

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

Compétence	Bloc	Cours
Évaluer les vulnérabilités internes et externes du SI et des infrastructures réseau	RNCP41976BC01	1, 11
Identifier, cartographier et hiérarchiser les risques de cybersécurité du SI	RNCP41976BC01	2
Exploiter des modèles d'évaluation des risques assistés par IA et des algorithmes de scoring	RNCP41976BC01	3
Modéliser les impacts techniques et métiers des vulnérabilités (tabletop, war-gaming, cyber range)	RNCP41976BC01	3
Identifier et classer les écarts de conformité des dispositifs de sécurité	RNCP41976BC01	4
Élaborer des recommandations priorisées de conformité réglementaire, légale et normative	RNCP41976BC01	4
Définir les objectifs stratégiques de cybersécurité et la politique de sécurité	RNCP41976BC01	5
Piloter une veille stratégique, technique, technologique et réglementaire	RNCP41976BC01	5, 17
Décliner la politique de sécurité en plan d'actions opérationnel priorisé	RNCP41976BC01	5
Concevoir des dispositifs intégrés de continuité et de reprise d'activité (PCA/PRA)	RNCP41976BC01	5
Élaborer une architecture de sécurité intégrée	RNCP41976BC02	6
Modéliser une architecture de sécurité dynamique du SI	RNCP41976BC02	7
Intégrer des solutions de cybersécurité sélectionnées sur une base multicritère	RNCP41976BC02	7
Élaborer l'architecture organisationnelle de sécurité intégrée	RNCP41976BC02	6
Structurer l'architecture technique de sécurité (TOGAF, COBIT, ISO/IEC 27001)	RNCP41976BC02	6
Développer un centre opérationnel de sécurité (SOC)	RNCP41976BC02	8
Déployer des dispositifs techniques de sécurité	RNCP41976BC02	7
Configurer et orchestrer les outils de supervision (SIEM, EDR, corrélation, tableaux de bord)	RNCP41976BC02	8, 9
Implémenter des modèles avancés de détection comportementale (UEBA, IA)	RNCP41976BC02	9
Automatiser les contre-mesures de sécurité avec une plateforme SOAR et des playbooks	RNCP41976BC02	10
Évaluer la robustesse opérationnelle de l'architecture (pentest, Red, Blue et Purple Team)	RNCP41976BC02	11
Explorer des solutions innovantes de sécurisation des communications sensibles	RNCP41976BC02	11
Planifier le projet à partir des exigences utilisateurs et des ressources	RNCP41976BC03	12
Gérer un projet avec des méthodes agiles et des outils adaptés	RNCP41976BC03	13
Réaliser le reporting du projet auprès du commanditaire	RNCP41976BC03	13
Piloter les prestataires extérieurs gérant les ressources du SI existant	RNCP41976BC03	14
Conduire l'équipe projet de manière inclusive	RNCP41976BC03	15
Définir un processus de communication inclusif au sein de l'équipe	RNCP41976BC03	15
Identifier des solutions innovantes par l'animation collective	RNCP41976BC03	15
Établir un processus sécurisé de partage d'information	RNCP41976BC03	14
Définir des indicateurs de performance et d'efficacité des mesures de sécurité, y compris d'inclusivité	RNCP41976BC04	16

Réaliser des revues périodiques des politiques et procédures de sécurité	RNCP41976BC04	16
Analyser les tendances et les menaces émergentes (APT, vecteurs d'attaque)	RNCP41976BC04	17
Piloter l'actualisation des dispositifs de sécurité technique, organisationnelle et documentaire	RNCP41976BC04	17
Définir les objectifs et scénarios de test des PCA/PRA et analyser les écarts	RNCP41976BC04	18
Piloter la mise en œuvre des actions correctives en cybersécurité	RNCP41976BC04	18
Piloter la communication stratégique en cybersécurité	RNCP41976BC04	19
Animer l'écosystème cyber de l'organisation (réseaux, exercices de crise, RCA)	RNCP41976BC04	19
Organiser des programmes de formation et de sensibilisation au security by design	RNCP41976BC04	20

Évaluations formatives

Chaque cours intègre des évaluations formatives qui permettent à l'apprenant et au formateur de l'organisme de mesurer la progression : QCM de validation des notions à la fin des sous-chapitres, études de cas, exercices pratiques et livrables intermédiaires construits dans le fil rouge Hélionys Réseaux (cartographie des risques, extrait de rapport d'audit, vue d'architecture, playbook SOAR, tableau de bord projet, synthèse d'exercice PCA/PRA). Les livrables sont évalués à l'aide de grilles critériées alignées sur les attendus des épreuves de certification. Les résultats des QCM sont disponibles dans la plateforme, ce qui permet à l'organisme de formation d'identifier les besoins de remédiation et d'adapter son accompagnement.

Modalités de certification

Bloc	Modalité d'évaluation
RNCP41976BC01	Mise en situation professionnelle reconstituée en deux phases. Phase 1 : dossier écrit en groupe de projet à partir d'un scénario d'organisation confrontée à des problématiques de cybersécurité, comprenant l'inventaire et la cartographie des actifs critiques, l'analyse des vulnérabilités internes et externes, la modélisation des scénarios de risques selon une méthode reconnue (EBIOS RM, ISO/IEC 27005, NIST SP 800-30), une cartographie des risques hiérarchisée et justifiée, un rapport d'audit incluant les écarts de conformité (RGPD, NIS2, ISO 27001), un plan de traitement des risques priorisé et des recommandations d'amélioration continue et de mise en conformité. Phase 2 : présentation orale du dossier en groupe, avec questionnement individuel par le jury.
RNCP41976BC02	Mise en situation professionnelle reconstituée en deux phases. Phase 1 : dossier écrit en groupe de projet à partir d'un contexte fourni (organisation, flux critiques, menaces sectorielles), présentant l'architecture technique et organisationnelle cible, la modélisation des flux et composants de sécurité (SIEM, EDR, pare-feu, IAM), le choix justifié des outils de détection et d'automatisation (SOAR, UEBA), les indicateurs de performance de la sécurité (KPI/KRI), la proposition d'un SOC adapté, l'intégration de solutions innovantes pour sécuriser les échanges sensibles et la documentation technique et fonctionnelle de l'architecture. Phase 2 : présentation orale du dossier en groupe, avec questionnement individuel par le jury.
RNCP41976BC03	Mise en situation professionnelle reconstituée en deux phases. Phase 1 : dossier écrit en groupe de projet à partir d'un cahier des charges, comprenant la planification du projet, la présentation argumentée de la méthodologie choisie et de sa mise en œuvre, les outils de suivi des indicateurs, les tableaux de bord de suivi des prestataires externes, la présentation de l'équipe projet, des outils de communication et des outils collaboratifs, des propositions de solutions innovantes pour les rencontres et échanges, des ordres du jour de réunions d'animation et une stratégie d'organisation du partage d'informations par des outils numériques. Phase 2 : présentation orale du dossier en groupe, avec questionnement individuel par le jury.
RNCP41976BC04	Mise en situation professionnelle reconstituée en deux phases. Phase 1 : dossier écrit en groupe de projet à partir d'un contexte d'organisation avec des exigences de conformité et des incidents passés, présentant un tableau de bord des indicateurs de sécurité opérationnels, réglementaires et d'inclusion, une analyse critique des revues de sécurité et des écarts, un rapport d'analyse des tendances issues de la veille cyber (plateformes CTI, CERT, MITRE ATT&CK), un plan de mise à jour des dispositifs techniques, documentaires et organisationnels, la synthèse d'un exercice de test PCA/PRA, la planification des actions correctives et une stratégie de communication et de pilotage à destination des parties prenantes. Phase 2 : soutenance orale de la stratégie de gouvernance en groupe, avec questionnement individuel par le jury.

Le parcours reproduit la logique des épreuves : chaque bloc s'appuie sur un même contexte d'organisation (Hélionys Réseaux) et chaque cours produit un livrable intermédiaire qui correspond à une rubrique attendue dans le dossier de certification du bloc. L'apprenant constitue ainsi progressivement un portfolio réutilisable comme modèle pour travailler le scénario remis par le certificateur. Les grilles critériées des évaluations formatives reprennent les attendus listés dans les modalités officielles. Le cours 20 propose une méthodologie de rédaction des dossiers en groupe de projet et de préparation des soutenances orales, en particulier du questionnement individuel par le jury. L'organisation des épreuves, la constitution des groupes et la délivrance de la certification relèvent de l'organisme de formation habilité, en lien avec les certificateurs.

Moyens pédagogiques et débouchés

Moyens pédagogiques et techniques

- Plateforme e-learning en marque blanche accessible 24 h/24, avec suivi de la progression et des résultats aux évaluations pour l'organisme de formation
- Une vidéo de 3 à 5 minutes par sous-chapitre, représentant 30 % du volume horaire de chaque cours
- Cours texte enrichis, infographies et fiches de synthèse téléchargeables (méthodes EBIOS RM, ISO/IEC 27001, MITRE ATT&CK, cycle de vie SOC)
- Études de cas et mises en situation scénarisées dans le fil rouge Hélionys Réseaux, avec jeux de données fictifs (journaux, rapports de scan, contrats, tableaux de bord)
- Modèles de livrables professionnels : cartographie des risques, rapport d'audit, PSSI, dossier d'architecture, playbook, plan de PCA/PRA, tableau de bord de gouvernance
- QCM de validation et grilles critériées alignées sur les modalités de certification de chaque bloc
- Contenus conçus en tenant compte des exigences d'accessibilité numérique (sous-titrage des vidéos, transcriptions, contrastes et navigation adaptés)

Débouchés et évolutions

- Analyste SOC (Security Operation Center) ou Ingénieur cybersécurité
- Conseiller en SSI, Responsable audits ou Consultant GRC (Gouvernance, Risques, Conformité)
- Responsable résilience opérationnelle ou Responsable des assurances cyber
- Architecte sécurité, Expert cloud sécurisé ou Incident responder
- RSSI (Responsable Sécurité Systèmes d'Information), avec 3 à 10 ans d'expérience
- Directeur cybersécurité, manager CERT/SOC ou Security service delivery manager

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 RNCP41976 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.