

SCHOOL FOR MATE

LIVRET PÉDAGOGIQUE

# Expert en cybersécurité

**RNCP40897 · Certification RNCP · Niveau 7**

Ce parcours de 440 heures prépare aux quatre blocs de compétences de la certification RNCP40897 « Expert en cybersécurité » (niveau 7) : stratégie de sécurité, intégration et audit de solutions, maintien en condition de sécurité et gestion de crise cyber. Le parcours suit une entreprise industrielle fictive confrontée à des menaces réalistes. L'apprenant y construit, cours après cours, les livrables attendus par le jury de certification.

| VOLUME HORAIRE | COURS | BLOCS |
| --- | --- | --- |
| 440 h | 20 | 4 |

01 · PRÉSENTATION

# La formation en bref

| | |
|---|---|
| Intitulé | Expert en cybersécurité |
| Code | RNCP40897 |
| Type | Certification RNCP |
| Niveau | Niveau 7 |
| Certificateur | YNOV |
| 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 | 25/06/2028 |

### Le métier et les compétences visées

L'expert en cybersécurité garantit la résilience numérique d'une organisation. Il étudie l'écosystème de l'organisation, cartographie le système d'information et analyse les risques. Il définit ensuite la politique de sécurité du SI (PSSI) et le plan d'actions qui en découle. Il conçoit des architectures sécurisées, pilote l'intégration de solutions de sécurité (gestion des identités, cryptographie, supervision) et en évalue l'efficacité par des audits techniques. Au quotidien, il maintient le SI en condition de sécurité : il gère l'obsolescence, met en place un SOC et traite les vulnérabilités. En cas d'attaque, il qualifie l'incident, organise la cellule de crise, conduit l'endiguement et l'analyse forensique, puis pilote la remédiation et la capitalisation.

### Public visé

- Titulaires d'un titre ou diplôme de niveau 6 en informatique souhaitant se spécialiser en cybersécurité
- Administrateurs systèmes et réseaux ou ingénieurs infrastructure en évolution vers des fonctions de sécurité
- Analystes SOC, techniciens sécurité ou pentesters visant un poste d'expert ou de responsable sécurité
- Consultants IT souhaitant développer une offre de conseil et d'audit en sécurité des systèmes d'information
- Salariés en reconversion ou en promotion interne disposant d'un socle informatique solide

### Prérequis

- Parcours complet : 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
- Admission en 4e année : être titulaire d'un diplôme ou titre de niveau 6 dans le domaine de l'informatique
- Toute demande ne répondant pas à ces prérequis est étudiée par une commission placée sous l'autorité du certificateur

## Objectifs pédagogiques

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

- Auditer une organisation, cartographier son système d'information et en analyser les risques pour évaluer sa maturité en sécurité
- Rédiger une PSSI alignée sur les référentiels normatifs et la réglementation applicables, puis analyser les écarts avec l'existant
- Construire et chiffrer un plan d'actions de sécurité intégrant l'impact écologique, puis le défendre devant les décisionnaires
- Concevoir les plans de sauvegarde, de secours, de reprise et de continuité d'activité ainsi qu'un plan de sensibilisation accessible
- Spécifier, planifier et piloter un projet d'intégration de solutions de sécurité
- Concevoir une architecture sécurisée et déployer la gestion des identités, le contrôle d'accès et des solutions cryptographiques
- Organiser un audit technique, en rédiger le rapport et suivre les actions correctives
- Maintenir le SI en condition de sécurité : gestion de l'obsolescence, mise en place et évaluation d'un SOC, traitement des vulnérabilités
- Préparer l'organisation à la crise cyber : communication de crise, cellule stratégique et exercices d'entraînement
- Qualifier, endiguer et analyser un incident, puis piloter l'éradication, la restauration et l'analyse post mortem

02 · FIL ROUGE PÉDAGOGIQUE

# Altévia Industries

IM

**Inès Moreau**

Ingénieure cybersécurité, puis responsable de la sécurité des systèmes d'information

Industrie manufacturière (conception et fabrication d'équipements hydrauliques)

Altévia Industries est une entreprise de taille intermédiaire implantée sur quatre sites en France. Elle compte un siège administratif, deux usines et une plateforme logistique. Son SI s'est construit par couches successives : ERP vieillissant, réseau industriel connecté au réseau bureautique, nombreuses applications métiers et premiers services hébergés dans le cloud. Plusieurs clients du secteur de l'énergie exigent désormais des garanties de sécurité contractuelles. La direction anticipe aussi de nouvelles obligations réglementaires européennes. Après une tentative d'hameçonnage ciblant la comptabilité, le directeur général décide de structurer la cybersécurité et recrute Inès Moreau. Sa mission : bâtir une stratégie de sécurité, la déployer avec la DSI et les métiers, maintenir le SI en condition de sécurité et préparer l'entreprise à affronter une crise cyber majeure.

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 audite Altévia, cartographie son SI, analyse les risques, rédige la PSSI et le plan d'actions, puis les présente au comité de direction avant de concevoir les plans de résilience et la sensibilisation.
2. Bloc 2 : Inès pilote l'intégration des solutions retenues (segmentation du réseau industriel, gestion des identités, chiffrement), puis fait auditer le résultat et suit les corrections.
3. Bloc 3 : Devenue RSSI, Inès met en place la gestion de l'obsolescence, intègre un SOC hybride, en teste l'efficacité et organise le traitement continu des vulnérabilités.
4. Bloc 4 : Inès structure la gestion de crise. Lorsqu'un rançongiciel frappe une usine, elle conduit la qualification, l'endiguement, l'analyse forensique, la restauration et le retour d'expérience.

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 |
|---|---|---|
| **RNCP40897BC01 · Elaborer la stratégie de cybersécurité d'une organisation** | | **132 h** |
| 1 | Auditer l'organisation : besoins métiers, acteurs et dépendances fonctionnelles | 22 h |
| 2 | Cartographier le SI et organiser la veille de sécurité | 22 h |
| 3 | Analyser les risques et mesurer la maturité de sécurité | 22 h |
| 4 | Définir la PSSI et analyser les écarts | 22 h |
| 5 | Bâtir le plan d'actions de sécurité et le corpus documentaire | 22 h |
| 6 | Concevoir la résilience du SI et la sensibilisation des utilisateurs | 22 h |
| **RNCP40897BC02 · Piloter le cycle de conception, d'intégration et d'évaluation de solutions de sécurité du système d'information** | | **110 h** |
| 7 | Spécifier les solutions de sécurité et organiser le projet d'intégration | 22 h |
| 8 | Piloter l'avancement du projet de sécurité | 22 h |
| 9 | Concevoir une architecture sécurisée du SI | 22 h |
| 10 | Gérer les identités, les accès et déployer la cryptographie | 22 h |
| 11 | Auditer les solutions de sécurité et suivre les actions correctives | 22 h |
| **RNCP40897BC03 · Maintenir en condition de sécurité le système d'information (SI) d'une organisation** | | **88 h** |
| 12 | Gérer l'obsolescence et les mises à jour du SI | 22 h |
| 13 | Définir la surveillance continue et intégrer un SOC | 22 h |
| 14 | Évaluer l'efficacité du SOC | 22 h |
| 15 | Détecter, documenter et corriger les vulnérabilités | 22 h |
| **RNCP40897BC04 · Gérer stratégiquement et opérationnellement une crise cyber** | | **110 h** |
| 16 | Concevoir la communication de crise et organiser la cellule de crise | 22 h |
| 17 | Entraîner l'organisation à la gestion de crise | 22 h |
| 18 | Qualifier l'incident et l'endiguer | 22 h |
| 19 | Réaliser l'analyse forensique de l'incident | 22 h |
| 20 | Remédier, restaurer et capitaliser sur la crise | 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

RNCP40897BC01 · 132 h

## Elaborer la stratégie de cybersécurité d'une organisation

### Cours 1 · Auditer l'organisation : besoins métiers, acteurs et dépendances fonctionnelles

22 h

OBJECTIFS

- Conduire un audit organisationnel en analysant les processus métiers et les interactions entre systèmes
- Recueillir et formaliser les attentes des parties prenantes
- Produire une vision exhaustive du fonctionnement opérationnel de l'organisation

ÉVALUATION FORMATIVE

QCM de validation et grille d'entretien à compléter à partir d'une étude de cas

CONTENUS

- Rôle de l'expert en cybersécurité et posture d'auditeur
- Méthodologie d'audit organisationnel : cadrage, périmètre, planning
- Analyse et modélisation des processus métiers
- Identification des acteurs, des actifs métiers et des dépendances fonctionnelles
- Conduite d'entretiens et d'ateliers avec les parties prenantes
- Évaluation des interactions entre systèmes et des dépendances aux tiers
- Formalisation du rapport d'étude de l'écosystème

**Fil rouge** · Pour sa première mission chez Altévia Industries, Inès mène des entretiens avec la direction de production, la logistique et la comptabilité afin d'identifier les processus critiques et leurs dépendances. Elle en tire une synthèse de l'écosystème.

### Cours 2 · Cartographier le SI et organiser la veille de sécurité

22 h

OBJECTIFS

- Établir la cartographie du SI en inventoriant services, actifs, liaisons et flux de données
- Choisir un modèle et un outil de modélisation adaptés au contexte
- Mettre en place une veille technologique, technique, réglementaire et normative et en analyser les impacts

ÉVALUATION FORMATIVE

Exercice de cartographie sur un cas guidé et fiche de veille commentée

CONTENUS

- Inventaire des services et des actifs techniques
- Vues de cartographie : écosystème, métier, applicative, infrastructure
- Identification des liaisons et des flux de données
- Choix des modèles et des outils de modélisation
- Sources de veille : menaces, vulnérabilités, innovations technologiques
- Veille réglementaire et normative : cadres nationaux, européens et sectoriels
- Outillage et industrialisation de la veille
- Analyse d'impact et identification des obligations et opportunités

**Fil rouge** · Inès découvre que le réseau industriel d'une usine communique directement avec le réseau bureautique. Elle construit la cartographie du SI d'Altévia et produit une note de veille sur les obligations réglementaires susceptibles de s'appliquer à l'entreprise.

### Cours 3 · Analyser les risques et mesurer la maturité de sécurité

22 h

OBJECTIFS

- Identifier les événements redoutés, les sources de risque et les scénarios d'attaque
- Hiérarchiser les risques selon leur gravité et leur impact potentiel
- Évaluer la maturité de l'organisation en matière de sécurité

ÉVALUATION FORMATIVE

Étude de cas notée : matrice de risques et synthèse de maturité

CONTENUS

- Fondamentaux de la gestion des risques numériques
- Panorama des méthodes d'analyse de risques (EBIOS Risk Manager, ISO/IEC 27005)
- Valeurs métiers, biens supports et événements redoutés
- Sources de risque, scénarios stratégiques et opérationnels
- Échelles de gravité et de vraisemblance, cartographie des risques
- Modèles d'évaluation de la maturité en sécurité
- Restitution des résultats aux décideurs

**Fil rouge** · Inès anime des ateliers d'analyse de risques avec le directeur industriel et le DSI. Elle identifie un scénario de rançongiciel paralysant la production comme risque prioritaire et établit un premier score de maturité d'Altévia.

### Cours 4 · Définir la PSSI et analyser les écarts

22 h

OBJECTIFS

- Rédiger une PSSI intégrant référentiels, réglementation, modèles de sécurité et homologation visée
- Réaliser une analyse des écarts entre l'existant et les objectifs de la PSSI
- Classer les écarts par criticité pour prioriser les actions

ÉVALUATION FORMATIVE

Rédaction commentée d'un extrait de PSSI et tableau d'écarts à prioriser

CONTENUS

- Structure et principes d'une PSSI
- Référentiels normatifs : famille ISO/IEC 27000, guides de l'ANSSI
- Réglementation applicable : RGPD, directive NIS 2, exigences sectorielles
- Modèles de sécurité et principes de contrôle d'accès
- Démarche d'homologation de sécurité
- Méthodologie d'analyse des écarts
- Classement des écarts par criticité et priorisation

**Fil rouge** · À partir de l'analyse de risques, Inès rédige la PSSI d'Altévia en s'appuyant sur la norme ISO/IEC 27001. Elle mesure ensuite les écarts avec l'existant, notamment sur la gestion des comptes à privilèges.

### Cours 5 · Bâtir le plan d'actions de sécurité et le corpus documentaire

22 h

OBJECTIFS

- Définir un plan d'actions chiffré intégrant moyens techniques et humains et impact écologique
- Présenter et faire valider le plan auprès des décisionnaires
- Élaborer un corpus documentaire de sécurité accessible aux personnes en situation de handicap

ÉVALUATION FORMATIVE

Simulation de présentation orale au comité de direction avec grille d'évaluation

CONTENUS

- Du rapport d'écarts au plan d'actions : feuille de route pluriannuelle
- Estimation des ressources, des coûts et des délais
- Évaluation de l'impact écologique des actions de sécurité
- Argumentation et présentation au comité de direction
- Architecture du corpus documentaire : politiques, procédures, chartes, guides
- Rédaction de la charte d'utilisation du SI
- Accessibilité numérique des supports documentaires

**Fil rouge** · Inès présente au comité de direction d'Altévia un plan d'actions sur trois ans, chiffré et argumenté, qui intègre la sobriété des équipements. Elle produit ensuite une charte informatique au format accessible.

### Cours 6 · Concevoir la résilience du SI et la sensibilisation des utilisateurs

22 h

OBJECTIFS

- Concevoir les plans de sauvegarde, de secours informatique, de reprise et de continuité d'activité
- Vérifier la capacité de mise en œuvre de ces plans par des tests et en indiquer l'impact écologique
- Élaborer un plan de sensibilisation et de formation adapté aux profils et accessible

ÉVALUATION FORMATIVE

Étude de cas : élaboration d'un plan de reprise et d'un plan de sensibilisation, QCM de fin de bloc

CONTENUS

- Bilan d'impact sur l'activité et objectifs de reprise (DMIA, PDMA)
- Politique et architecture de sauvegarde
- Plan de secours informatique et plan de reprise d'activité
- Plan de continuité d'activité et articulation avec les métiers
- Tests, simulations d'incidents et impact écologique des dispositifs de résilience
- Identification des besoins de sensibilisation par profil d'utilisateur
- Conception de contenus et de supports variés et accessibles

**Fil rouge** · Inès conçoit le PRA de l'ERP et le PCA de l'usine principale d'Altévia, puis organise un test de restauration. Elle prépare enfin un programme de sensibilisation distinct pour les opérateurs de production, les fonctions support et les dirigeants.

RNCP40897BC02 · 110 h

## Piloter le cycle de conception, d'intégration et d'évaluation de solutions de sécurité du système d'information

### Cours 7 · Spécifier les solutions de sécurité et organiser le projet d'intégration

22 h

OBJECTIFS

- Rédiger les spécifications techniques et fonctionnelles en lien avec la PSSI
- Choisir une méthodologie de gestion de projet et définir les critères de performance
- Établir le planning, les échéances et l'allocation des ressources

ÉVALUATION FORMATIVE

Exercice de rédaction d'un extrait de spécifications et d'un planning commenté

CONTENUS

- Analyse des besoins métiers, des contraintes réglementaires et des enjeux opérationnels
- Rédaction d'un cahier des charges de solution de sécurité
- Exigences fonctionnelles, techniques et de sécurité
- Méthodologies de gestion de projet : prédictive, agile, hybride
- Critères de performance et indicateurs de réussite du projet
- Planification, jalons et échéances d'intégration
- Allocation des ressources et budget

**Fil rouge** · Inès rédige le cahier des charges d'une solution de segmentation du réseau industriel d'Altévia. Elle construit le planning du projet en tenant compte des arrêts de production programmés.

### Cours 8 · Piloter l'avancement du projet de sécurité

22 h

OBJECTIFS

- Coordonner les parties prenantes internes et externes
- Superviser l'exécution des tâches et suivre délais, coûts et objectifs de sécurité
- Ajuster les actions en cas de dérive

ÉVALUATION FORMATIVE

Mise en situation : analyse d'un tableau de bord projet et proposition d'actions correctives

CONTENUS

- Gouvernance de projet et instances de pilotage
- Coordination des équipes internes, prestataires et éditeurs
- Tableaux de bord de suivi : délais, coûts, qualité, sécurité
- Gestion des risques projet et des aléas
- Gestion du changement auprès des utilisateurs
- Recette, mise en production et clôture du projet

**Fil rouge** · Le prestataire intégrateur d'Altévia accuse trois semaines de retard. Inès réunit le comité de pilotage, réajuste le planning et arbitre entre périmètre et délai sans dégrader les objectifs de sécurité.

### Cours 9 · Concevoir une architecture sécurisée du SI

22 h

OBJECTIFS

- Concevoir une architecture fondée sur la défense en profondeur, la segmentation et le contrôle d'accès
- Sélectionner des solutions technologiques adaptées aux besoins et aux risques
- Protéger données, applications et infrastructures contre les menaces internes et externes

ÉVALUATION FORMATIVE

Étude de cas : critique et amélioration d'un schéma d'architecture

CONTENUS

- Principes de défense en profondeur et de moindre privilège
- Segmentation et cloisonnement des réseaux, zones de confiance
- Sécurisation des systèmes industriels et de leur interconnexion
- Sécurité des environnements cloud et hybrides
- Approche Zero Trust
- Sélection des briques de sécurité : pare-feu, passerelles, protection des terminaux
- Documentation d'un dossier d'architecture sécurisée

**Fil rouge** · Inès conçoit la nouvelle architecture cible d'Altévia, avec une zone démilitarisée entre les réseaux industriel et bureautique et des accès distants sécurisés pour les mainteneurs.

### Cours 10 · Gérer les identités, les accès et déployer la cryptographie

22 h

OBJECTIFS

- Mettre en œuvre des processus d'authentification, d'autorisation et de gestion des droits, en tenant compte des personnes en situation de handicap
- Déployer et configurer des solutions cryptographiques intégrées à l'existant
- Garantir la confidentialité, l'intégrité et l'authenticité des données

ÉVALUATION FORMATIVE

QCM technique et exercice de conception d'une matrice des droits

CONTENUS

- Cycle de vie des identités : arrivées, mobilités, départs
- Mécanismes d'authentification forte et accessibilité
- Modèles d'autorisation et revue des droits
- Gestion des comptes à privilèges
- Fondamentaux de la cryptographie symétrique et asymétrique
- Infrastructures de gestion de clés et certificats
- Chiffrement des données au repos et en transit, protocoles sécurisés

**Fil rouge** · Inès déploie l'authentification multifacteur chez Altévia en prévoyant une alternative adaptée pour un collaborateur malvoyant. Elle met également en place le chiffrement des postes nomades des commerciaux.

### Cours 11 · Auditer les solutions de sécurité et suivre les actions correctives

22 h

OBJECTIFS

- Organiser un audit technique avec périmètre et référentiels définis
- Rédiger un rapport d'audit structuré avec recommandations réalisables
- Suivre la mise en œuvre et l'efficacité des actions correctives

ÉVALUATION FORMATIVE

Rédaction guidée d'un extrait de rapport d'audit, QCM de fin de bloc

CONTENUS

- Typologie des audits techniques : configuration, architecture, code, tests d'intrusion
- Plan d'audit : périmètre, référentiels, règles d'engagement
- Outils et techniques d'investigation
- Qualification des vulnérabilités et non-conformités
- Structure et rédaction du rapport d'audit
- Formulation de recommandations conformes aux normes et standards
- Suivi et vérification de l'efficacité des actions correctives

**Fil rouge** · Inès fait réaliser un audit de la nouvelle architecture d'Altévia, rédige le rapport à destination de la DSI et organise des points de suivi jusqu'à la clôture des corrections critiques.

RNCP40897BC03 · 88 h

## Maintenir en condition de sécurité le système d'information (SI) d'une organisation

### Cours 12 · Gérer l'obsolescence et les mises à jour du SI

22 h

OBJECTIFS

- Définir une politique de gestion de l'obsolescence et des mises à jour selon le cycle de vie des composants
- Réaliser mises à jour et décommissionnements selon une procédure établie
- Développer des indicateurs de suivi automatisés

ÉVALUATION FORMATIVE

Étude de cas : rédaction d'une procédure de mise à jour et choix d'indicateurs

CONTENUS

- Typologie et cycle de vie des composants matériels et logiciels
- Politique de gestion des correctifs et de l'obsolescence
- Procédures de mise à jour : tests, déploiement, retour arrière
- Décommissionnement sécurisé et fin de vie des actifs
- Cas particuliers des systèmes industriels non maintenus
- Indicateurs, données historiques et collecte en temps réel
- Automatisation des tableaux de bord et des rapports

**Fil rouge** · Nommée RSSI, Inès découvre des automates et des serveurs hors support dans les usines d'Altévia. Elle définit une politique d'obsolescence, pilote un décommissionnement et construit un tableau de bord de suivi des correctifs.

### Cours 13 · Définir la surveillance continue et intégrer un SOC

22 h

OBJECTIFS

- Élaborer une politique de surveillance alignée sur les menaces, la PSSI, la réglementation et les besoins métiers
- Définir les dispositifs, les équipes et les indicateurs d'un SOC
- Déployer les outils de détection et d'analyse avancée

ÉVALUATION FORMATIVE

QCM et exercice de définition d'une politique de supervision

CONTENUS

- Politique de contrôle et de surveillance continue
- Modèles de SOC : interne, externalisé, hybride
- Organisation des équipes et niveaux d'analyse
- Outils de détection : SIEM, EDR, NDR, sondes
- Collecte et corrélation des journaux
- Règles de détection et référentiel MITRE ATT&CK
- Indicateurs clés de performance du SOC

**Fil rouge** · Inès compare les options d'internalisation et d'externalisation du SOC d'Altévia. Elle retient un modèle hybride et définit les sources de journaux prioritaires, dont les passerelles du réseau industriel.

### Cours 14 · Évaluer l'efficacité du SOC

22 h

OBJECTIFS

- Concevoir des scénarios de test réalistes pour évaluer la détection
- Mesurer la performance des processus et des équipes du SOC
- Proposer des axes d'amélioration

ÉVALUATION FORMATIVE

Étude de cas : analyse des résultats d'un exercice et recommandations

CONTENUS

- Objectifs et cadre d'une évaluation de SOC
- Tests d'intrusion et simulations d'attaques
- Exercices en équipes rouge, bleue et violette
- Mesure des délais de détection et de réponse
- Analyse de la couverture de détection
- Restitution et plan d'amélioration continue

**Fil rouge** · Six mois après la mise en service du SOC, Inès organise un exercice d'attaque simulée sur un poste de l'usine d'Altévia. Elle mesure ensuite le temps de détection et identifie les angles morts.

### Cours 15 · Détecter, documenter et corriger les vulnérabilités

22 h

OBJECTIFS

- Analyser les alertes de supervision pour documenter les vulnérabilités
- Évaluer la criticité des vulnérabilités
- Élaborer et suivre un plan d'actions correctives

ÉVALUATION FORMATIVE

Exercice de qualification de vulnérabilités, QCM de fin de bloc

CONTENUS

- Processus de gestion des vulnérabilités
- Analyse et tri des alertes de monitoring
- Scores et évaluation de la criticité en contexte
- Documentation et fiche de vulnérabilité
- Plan d'actions correctives et mesures compensatoires
- Vérification de la correction et clôture

**Fil rouge** · Le SOC d'Altévia remonte une vulnérabilité critique sur le portail fournisseurs. Inès la documente, en évalue l'exposition et pilote un plan de correction avec mesure compensatoire temporaire.

RNCP40897BC04 · 110 h

## Gérer stratégiquement et opérationnellement une crise cyber

### Cours 16 · Concevoir la communication de crise et organiser la cellule de crise

22 h

OBJECTIFS

- Concevoir une stratégie de communication de crise avec parties prenantes, canaux de secours et messages types
- Organiser une cellule stratégique de crise : membres, rôles, missions
- Définir les critères et procédures d'activation

ÉVALUATION FORMATIVE

Exercice de rédaction de messages de crise et d'une fiche réflexe d'activation

CONTENUS

- Caractéristiques d'une crise cyber
- Cartographie des parties prenantes internes et externes
- Obligations de notification aux autorités
- Canaux de communication de secours
- Rédaction de messages types clés en main
- Composition et rôles de la cellule stratégique et de la cellule opérationnelle
- Critères, seuils et procédures d'activation

**Fil rouge** · Inès rédige pour Altévia un dispositif de crise comprenant l'annuaire des contacts critiques, des messages types destinés aux clients et aux salariés, et la procédure d'activation de la cellule.

### Cours 17 · Entraîner l'organisation à la gestion de crise

22 h

OBJECTIFS

- Déployer une stratégie d'entraînement progressive et adaptée
- Concevoir des exercices variés fondés sur des scénarios d'attaque réalistes
- Évaluer les exercices et renforcer les compétences de l'équipe

ÉVALUATION FORMATIVE

Conception d'un scénario d'exercice évaluée par grille

CONTENUS

- Typologie d'exercices : sur table, fonctionnels, grandeur nature
- Conception d'un scénario et d'un chronogramme d'exercice
- Rôles d'animation, d'observation et de joueurs
- Scénarios adaptés au secteur et aux menaces de l'organisation
- Débriefing à chaud et retour d'expérience
- Programme pluriannuel d'entraînement

**Fil rouge** · Inès anime un exercice sur table avec le comité de direction d'Altévia autour d'une fuite de données de conception. Elle en tire des ajustements du dispositif de crise.

### Cours 18 · Qualifier l'incident et l'endiguer

22 h

OBJECTIFS

- Vérifier qu'une alerte n'est pas un faux positif et qualifier l'incident
- Définir nature, portée et criticité pour décider de l'activation de la cellule
- Mettre en place des mesures d'endiguement protégeant les actifs essentiels

ÉVALUATION FORMATIVE

Mise en situation chronométrée de qualification d'incident

CONTENUS

- Processus de réponse à incident
- Tri des alertes et élimination des faux positifs
- Qualification : nature, périmètre, criticité
- Décision d'activation de la cellule de crise
- Stratégies d'endiguement : isolement, cloisonnement, coupures maîtrisées
- Protection des actifs essentiels et préservation des preuves
- Main courante et traçabilité des décisions

**Fil rouge** · Un vendredi soir, le SOC signale des chiffrements massifs sur les serveurs d'une usine d'Altévia. Inès confirme l'attaque par rançongiciel, active la cellule de crise et fait isoler le site.

### Cours 19 · Réaliser l'analyse forensique de l'incident

22 h

OBJECTIFS

- Collecter les preuves numériques dans le respect de leur intégrité
- Corréler les traces pour reconstituer le scénario d'attaque
- Préparer une réponse et une remédiation adaptées

ÉVALUATION FORMATIVE

Étude de cas : reconstitution d'une chronologie d'attaque à partir de journaux

CONTENUS

- Principes de l'investigation numérique et chaîne de conservation
- Collecte de données volatiles et non volatiles
- Analyse des systèmes, de la mémoire et des journaux
- Analyse des flux réseau
- Indicateurs de compromission et chronologie de l'attaque
- Rapport d'investigation et préconisations de remédiation

**Fil rouge** · Avec un prestataire spécialisé, Inès reconstitue l'intrusion chez Altévia : un accès distant de maintenance compromis, puis une latéralisation vers les serveurs de production.

### Cours 20 · Remédier, restaurer et capitaliser sur la crise

22 h

OBJECTIFS

- Déployer les actions d'éviction et d'éradication et en vérifier l'efficacité
- Mettre en œuvre le plan de restauration du SI
- Conduire l'analyse post mortem et capitaliser

ÉVALUATION FORMATIVE

Rédaction d'un rapport post mortem évalué par grille, QCM de fin de bloc

CONTENUS

- Planification de l'éviction et de l'éradication
- Mobilisation des experts et des outils de sécurité
- Vérification de l'élimination de la menace
- Restauration progressive et sécurisée du SI
- Retour à la normale et levée de la cellule de crise
- Analyse post mortem et enseignements
- Mise à jour de la PSSI, des plans et du dispositif de crise

**Fil rouge** · Inès pilote l'éradication et la restauration de l'usine à partir des sauvegardes testées au cours 6. Elle présente ensuite au comité de direction d'Altévia l'analyse post mortem et les évolutions du dispositif.

05 · CONFORMITÉ AU RÉFÉRENTIEL

# Couverture des compétences

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

| Compétence | Bloc | Cours |
|---|---|---|
| Auditer l'organisation (besoins métiers, acteurs, dépendances fonctionnelles) | RNCP40897BC01 | 1 |
| Établir la cartographie du SI | RNCP40897BC01 | 2 |
| Assurer une veille technologique, technique, réglementaire et normative | RNCP40897BC01 | 2 |
| Réaliser une analyse des risques et mesurer la maturité | RNCP40897BC01 | 3 |
| Définir la PSSI | RNCP40897BC01 | 4 |
| Réaliser une analyse des écarts PSSI / SI | RNCP40897BC01 | 4 |
| Définir et faire valider un plan d'actions de sécurité | RNCP40897BC01 | 5 |
| Élaborer le corpus documentaire de sécurité accessible | RNCP40897BC01 | 5 |
| Concevoir les plans de sauvegarde, secours, reprise et continuité d'activité | RNCP40897BC01 | 6 |
| Élaborer un plan de sensibilisation et de formation des utilisateurs | RNCP40897BC01 | 6 |
| Rédiger les spécifications techniques et fonctionnelles des solutions de sécurité | RNCP40897BC02 | 7 |
| Organiser le projet d'intégration des solutions de sécurité | RNCP40897BC02 | 7, 8 |
| Piloter l'avancement du projet | RNCP40897BC02 | 8 |
| Concevoir une architecture sécurisée du SI | RNCP40897BC02 | 9 |
| Gérer les identités et contrôler les accès | RNCP40897BC02 | 10 |
| Déployer des solutions cryptographiques | RNCP40897BC02 | 10 |
| Organiser un audit technique des solutions de sécurité | RNCP40897BC02 | 11 |
| Rédiger un rapport d'audit technique | RNCP40897BC02 | 11 |
| Assurer le suivi des actions correctives d'audit | RNCP40897BC02 | 11 |
| Définir une politique de gestion de l'obsolescence et des mises à jour | RNCP40897BC03 | 12 |
| Réaliser les mises à jour ou décommissionnements des actifs | RNCP40897BC03 | 12 |
| Développer des indicateurs de suivi des mises à jour et de l'obsolescence | RNCP40897BC03 | 12 |
| Élaborer une politique de contrôle et de surveillance continue | RNCP40897BC03 | 13 |
| Intégrer un SOC au sein de l'organisation | RNCP40897BC03 | 13 |
| Évaluer l'efficacité du SOC | RNCP40897BC03 | 14 |
| Documenter les vulnérabilités détectées | RNCP40897BC03 | 15 |

| | | |
|---|---|---|
| Corriger les vulnérabilités identifiées | RNCP40897BC03 | 15 |
| Concevoir une stratégie de communication de crise | RNCP40897BC04 | 16 |
| Organiser une cellule stratégique de crise | RNCP40897BC04 | 16 |
| Déployer une stratégie d'entraînement de gestion de crise | RNCP40897BC04 | 17 |
| Réaliser l'analyse initiale de l'incident détecté | RNCP40897BC04 | 18 |
| Mettre en place des mesures d'endiguement | RNCP40897BC04 | 18 |
| Réaliser une analyse forensique de l'incident | RNCP40897BC04 | 19 |
| Déployer des actions d'éviction et d'éradication | RNCP40897BC04 | 20 |
| Mettre en œuvre le plan de restauration du SI | RNCP40897BC04 | 20 |
| Capitaliser sur les enseignements de la crise (analyse post mortem) | RNCP40897BC04 | 20 |

## Évaluations formatives

Chaque sous-chapitre se conclut par un QCM de validation des acquis. Chaque cours comporte en outre une évaluation formative appliquée au fil rouge Altévia Industries : étude de cas, exercice de rédaction de livrable, analyse de journaux ou simulation de présentation. Ces évaluations s'appuient sur des grilles critériées alignées sur les compétences du référentiel. Elles permettent à l'apprenant de se situer et au formateur de l'organisme de formation d'adapter l'accompagnement. Un QCM récapitulatif clôt chaque bloc. Les résultats sont tracés dans la plateforme et alimentent le suivi pédagogique attendu au titre de Qualiopi.

## Modalités de certification

| Bloc | Modalité d'évaluation |
|---|---|
| RNCP40897BC01 | Mise en situation professionnelle, réelle ou fictive, donnant lieu à une soutenance orale avec remise au jury du support de présentation. |
| RNCP40897BC02 | Mise en situation professionnelle, réelle ou fictive, donnant lieu à un dossier écrit. |
| RNCP40897BC03 | Mise en situation professionnelle, réelle ou fictive, donnant lieu à un dossier écrit. |
| RNCP40897BC04 | Mise en situation professionnelle, réelle ou fictive, donnant lieu à une soutenance orale avec remise au jury du support de présentation. |

Le fil rouge Altévia Industries reproduit les mises en situation professionnelles attendues par le certificateur. À chaque cours, l'apprenant produit une pièce réutilisable : cartographie, analyse de risques, PSSI, plan d'actions, spécifications, rapport d'audit, politique de supervision, dispositif de crise, rapport post mortem. Pour les blocs 1 et 4, évalués par soutenance orale, des simulations de présentation devant un comité de direction entraînent à l'argumentation et à la construction d'un support. Pour les blocs 2 et 3, évalués par dossier écrit, des trames commentées et des grilles d'autoévaluation guident la rédaction. SFM fournit le contenu pédagogique. L'organisme de formation reste responsable de l'inscription des candidats et de l'organisation de la certification auprès du 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
- Cours textes enrichis, infographies et fiches de synthèse téléchargeables
- Études de cas et mises en situation fondées sur le fil rouge Altévia Industries
- Modèles de livrables professionnels : trame de PSSI, matrice de risques, plan de reprise, rapport d'audit, fiche réflexe de crise
- QCM de validation par sous-chapitre et évaluations de fin de bloc avec grilles critériées
- Supports conçus selon les principes d'accessibilité numérique (sous-titrage des vidéos, structuration des contenus)

### Débouchés et évolutions

- Expert cybersécurité / Expert sécurité des systèmes d'information
- Consultant cybersécurité / Consultant en sécurité des systèmes d'information
- Ingénieur cybersécurité / Ingénieur sécurité des systèmes d'information
- Responsable sécurité informatique
- Auditeur sécurité des systèmes d'information
- Analyste SOC (Security Operations Center) ou pentester

### 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 RNCP40897 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.