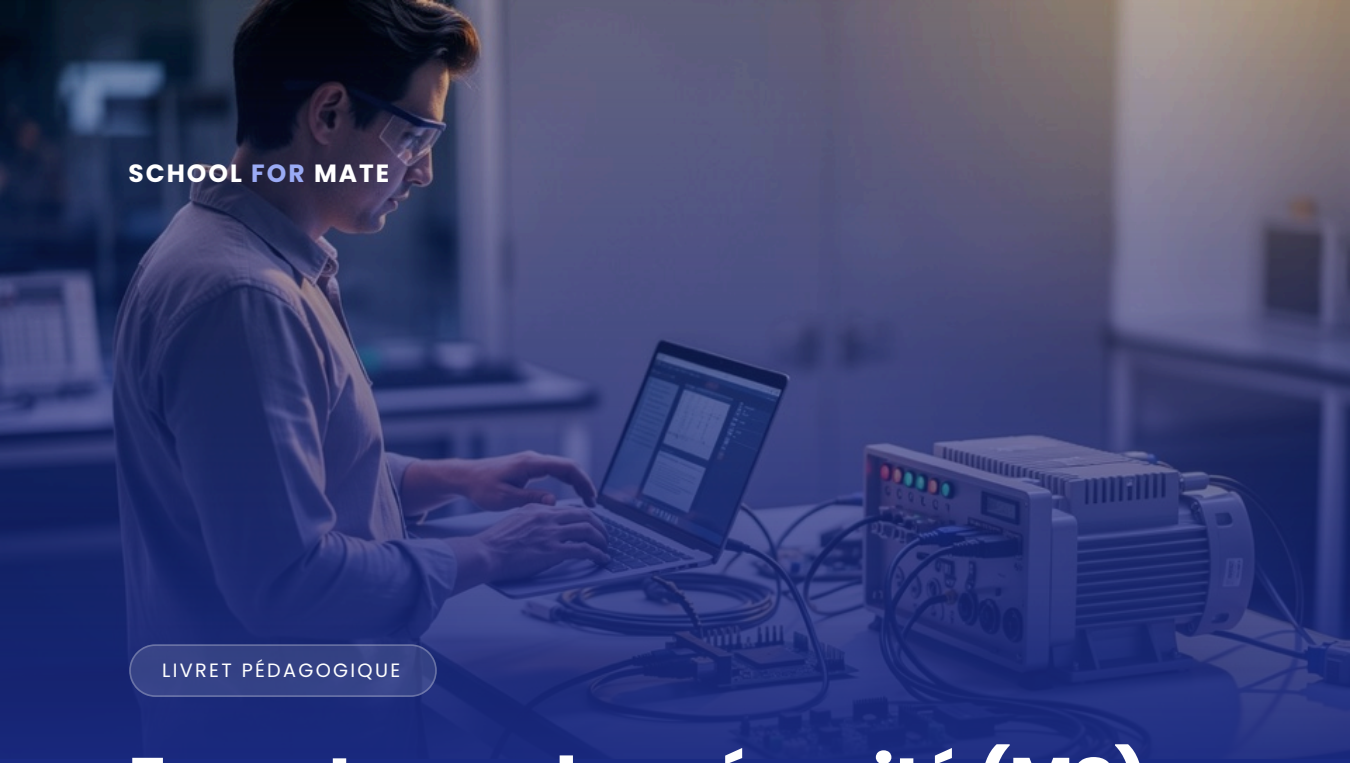


SCHOOL FOR MATE

LIVRET PÉDAGOGIQUE

Expert en cybersécurité (MS)

RNCP40640 · Certification RNCP · Niveau 7

Ce parcours de niveau 7 forme des experts capables de traiter les incidents de cybersécurité, d'analyser la menace, d'auditer la sécurité technique d'une organisation et de conduire des investigations technico-légales. Construit sur les quatre blocs de compétences du référentiel RNCP40640, il alterne apports experts, laboratoires guidés et mises en situation autour d'un groupe industriel fictif confronté à une crise cyber réaliste.

VOLUME HORAIRE	COURS	BLOCS
440 h	**20**	**4**

01 · PRÉSENTATION

La formation en bref

Intitulé	Expert en cybersécurité (MS)
Code	RNCP40640
Type	Certification RNCP
Niveau	Niveau 7
Certificateur	UNIVERSITE DE TECHNOLOGIE DE TROYES (UTT)
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	23/05/2030

Le métier et les compétences visées

L'expert en cybersécurité protège les systèmes d'information contre les actes malveillants. Il identifie, corrige et prévient les vulnérabilités exploitables par des cybercriminels. Il intervient lors des incidents : il collecte et analyse les traces, reconstitue le déroulement de l'attaque et pilote la remédiation dans le respect de la PSSI, qu'il contribue à enrichir. Il supervise les événements de sécurité au moyen d'un SIEM, analyse les codes malveillants et modélise les intrusions. Il conduit des audits et des tests d'intrusion cadrés juridiquement. Il réalise des analyses forensiques dont les conclusions peuvent appuyer une action interne ou une procédure judiciaire. Il exerce en grand groupe, banque, administration, PME, ESN ou chez un prestataire spécialisé.

Public visé

- Ingénieurs et diplômés de niveau Bac+5 en informatique, réseaux ou systèmes souhaitant se spécialiser en cybersécurité
- Administrateurs systèmes et réseaux expérimentés visant un poste d'expert ou d'auditeur sécurité
- Professionnels de la SSI (analystes SOC, techniciens sécurité) souhaitant accéder à un niveau d'expertise
- Consultants d'ESN ou de prestataires de services numériques intervenant sur des missions de sécurité
- Professionnels justifiant d'une expérience significative en lien avec la cybersécurité et candidats à une admission par VAPP

Prérequis

- Titre d'ingénieur diplômé conférant le grade de master, diplôme d'école de management conférant le grade de master, diplôme de 3e cycle ou diplôme professionnel de niveau Bac+5, titre RNCP de niveau 7 ou diplôme étranger équivalent
- Ou diplôme de niveau M1 assorti d'au moins trois années d'expérience professionnelle en lien avec la formation visée
- Par dérogation (dans la limite de 40 % de la promotion) : admission sur VAPP avec au moins 5 années d'expérience en lien avec les compétences visées, ou M1 avec moins de trois ans d'expérience, ou licence (L3) ou titre RNCP de niveau 6 avec au moins 3 ans d'expérience en lien avec la formation
- Maîtrise des bases des systèmes Linux et Windows, des réseaux TCP/IP et d'un langage de script (recommandé pour suivre les laboratoires)

Objectifs pédagogiques

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

- Coordonner la collecte, le tri et l'analyse des traces d'un incident de cybersécurité pour en évaluer l'ampleur et reconstituer le déroulement de l'attaque
- Élaborer un plan de remédiation conforme à la PSSI et contribuer à l'enrichissement de cette dernière à l'aide des méthodes EBIOS RM, Méhari et de la norme ISO 27001
- Superviser les événements de sécurité au moyen d'un SIEM et configurer les dispositifs de détection pour bloquer les tentatives d'intrusion en temps réel
- Analyser et catégoriser un code malveillant par des techniques statiques et dynamiques, puis développer un correctif en Python, Bash ou C++
- Modéliser et attribuer une intrusion à l'aide de la Cyber Kill Chain, du Diamond Model et de la matrice MITRE ATT&CK
- Mettre en place un dispositif de veille sur la menace (OSINT, SOCMINT, HUMINT, Deep et Dark web) et exploiter l'IA générative pour renforcer la prévention et la détection
- Cadrer, conduire et superviser des tests d'intrusion sur des systèmes, réseaux, applications web et mobiles dans le respect du Code pénal
- Rédiger un rapport d'audit assorti de contre-mesures et restituer les résultats aux décideurs et aux équipes techniques
- Préserver, acquérir et analyser des preuves numériques selon une méthodologie technico-légale garantissant leur recevabilité
- Rédiger un rapport forensique accessible et adapté aux publics techniques, judiciaires et institutionnels

02 · FIL ROUGE PÉDAGOGIQUE

Hydronéa Industries

IG

Inès Garnier

Experte en cybersécurité au sein de la cellule sécurité des systèmes d'information, rattachée au RSSI du groupe

Industrie : conception et fabrication d'équipements de traitement et de pompage de l'eau pour les collectivités et les industriels

Hydronéa Industries est un groupe industriel français de taille intermédiaire, implanté sur cinq sites de production et un siège à Lyon. Son système d'information combine une informatique de gestion classique, un ERP, un portail client web, une application mobile de télémaintenance et des systèmes industriels pilotant les lignes de fabrication. Plusieurs de ses clients sont des collectivités, ce qui place le groupe sous une forte exigence de continuité et de conformité. Inès Garnier vient d'intégrer la cellule SSI pour structurer la réponse à incident, la détection, l'audit et l'investigation. Dès ses premières semaines, un rançongiciel chiffre une partie des serveurs d'un site de production. Cet incident sert de point de départ à tout le parcours : Inès va devoir gérer la crise, comprendre la menace, faire auditer le SI puis conduire l'investigation qui permettra au groupe de déposer plainte.

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 pilote la réponse à l'incident rançongiciel, collecte et trie les traces, rédige le plan de remédiation, enrichit la PSSI avec le RSSI et organise la sensibilisation des équipes.
2. Bloc 2 : Inès structure la supervision du groupe autour d'un SIEM, analyse l'échantillon malveillant, développe un correctif, modélise l'intrusion avec MITRE ATT&CK et lance une veille sur les menaces visant le secteur de l'eau.
3. Bloc 3 : Inès cadre et supervise un audit de sécurité technique du SI d'Hydronéa, conduit les tests d'intrusion sur le réseau, le portail web et l'application mobile, puis restitue les résultats au comité de direction.
4. Bloc 4 : Inès mène l'investigation technico-légale des postes, serveurs et smartphones impliqués, et rédige le rapport forensique remis à la direction juridique, aux enquêteurs et au magistrat.

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
RNCP40640BC01 · Traiter les incidents de cybersécurité		**132 h**
1	Fondamentaux de la réponse à incident et de la gestion de crise cyber	22 h
2	Coordonner la collecte des informations relatives à un incident	22 h
3	Trier, catégoriser et analyser les preuves numériques d'un incident	22 h
4	Contextualiser l'incident et élaborer le plan de remédiation	22 h
5	Enrichir la PSSI : analyse de risques, ISO 27001 et SMSI	22 h
6	Sensibiliser les collaborateurs et piloter l'amélioration continue	22 h
RNCP40640BC02 · Analyser la menace cyber pesant sur une organisation		**132 h**
7	Supervision de la sécurité et exploitation d'un SIEM	22 h
8	Détection en temps réel et architecture réseau de sécurité	22 h
9	Analyse et catégorisation des codes malveillants	22 h
10	Développer des correctifs et outils de sécurité en Python, Bash et C++	22 h
11	Modéliser et attribuer les intrusions : Kill Chain, Diamond Model, MITRE ATT&CK	22 h
12	Renseignement sur la menace et IA générative appliquée à la cybersécurité	22 h
RNCP40640BC03 · Auditer la sécurité technique d'une organisation		**88 h**
13	Cadrer un audit de sécurité et animer la réunion de lancement	22 h
14	Tests d'intrusion sur les systèmes et les réseaux	22 h
15	Tests d'intrusion sur les applications web et mobiles	22 h
16	Rédiger le rapport d'audit et restituer les résultats	22 h
RNCP40640BC04 · Réaliser une analyse technico-légale (forensique)		**88 h**
17	Cadrer l'investigation et définir la stratégie de préservation des données	22 h
18	Collecte technico-légale des données	22 h
19	Analyse forensique avancée des artefacts numériques	22 h
20	Rédiger et communiquer le rapport d'analyse forensique	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

RNCP40640BC01 · 132 h

Traiter les incidents de cybersécurité

Cours 1 · Fondamentaux de la réponse à incident et de la gestion de crise cyber

22 h

OBJECTIFS

- Situer les phases de la réponse à incident et le rôle de chaque acteur de la cellule de crise
- Qualifier un incident de sécurité et estimer une première ampleur de la crise

ÉVALUATION FORMATIVE

QCM de fin de sous-chapitre et étude de cas : fiche de qualification d'incident à compléter à partir d'un scénario

CONTENUS

- Typologie des incidents de cybersécurité et indicateurs de compromission
- Cycle de la réponse à incident : préparation, détection, confinement, éradication, rétablissement, retour d'expérience
- Organisation d'une cellule de crise cyber : rôles, circuits de décision, main courante
- Qualification et priorisation d'un incident selon son impact métier
- Obligations de notification : CNIL, autorités compétentes, clients et partenaires
- Distribution Kali Linux : présentation de l'environnement et des outils de réponse à incident

Fil rouge · Un lundi matin, les opérateurs d'un site de production d'Hydronéa découvrent des fichiers chiffrés et une note de rançon. Inès doit qualifier l'incident, activer la cellule de crise et proposer au RSSI une première estimation de l'ampleur.

Cours 2 · Coordonner la collecte des informations relatives à un incident

22 h

OBJECTIFS

- Planifier et coordonner la collecte des journaux, topologies et images systèmes liés à un incident
- Mettre en œuvre les outils open source de collecte et de première exploitation (Autopsy, foremost, scalpel, Volatility, plaso, log2timeline)

ÉVALUATION FORMATIVE

Laboratoire guidé sur Kali Linux : production d'une super-chronologie à partir d'un jeu de traces fourni, suivi d'un QCM

CONTENUS

- Cartographie des sources de traces : journaux systèmes, réseau, applicatifs, équipements de sécurité
- Exploitation des diagrammes de topologie réseau pour délimiter le périmètre touché
- Capture et exploitation de la mémoire vive avec Volatility
- Récupération de fichiers et carving avec foremost et scalpel
- Construction de chronologies avec plaso et log2timeline
- Premier examen des images systèmes avec Autopsy
- Coordination des équipes IT et des prestataires pendant la collecte

Fil rouge · Inès coordonne la collecte des journaux des contrôleurs de domaine, des pare-feu et des serveurs chiffrés du site touché, et réalise une capture mémoire d'un serveur encore actif pour mesurer l'étendue de la compromission.

Cours 3 · Trier, catégoriser et analyser les preuves numériques d'un incident

22 h

OBJECTIFS

- Définir des catégories de tri et classer les éléments collectés pour constituer des preuves analysables
- Analyser les preuves selon la méthodologie forensique pour identifier la nature de l'incident et reconstituer l'attaque

ÉVALUATION FORMATIVE

Étude de cas : tri d'un jeu de journaux d'événements et rédaction d'une synthèse du déroulement de l'attaque

CONTENUS

- Grilles de tri des éléments d'incident : catégories, criticité, pertinence
- Filtrage et réduction du bruit dans les journaux d'événements
- Principes de la méthodologie forensique appliquée à la réponse à incident
- Exploitation de données brutes ou altérées : limites et précautions
- Identification du vecteur initial, des mouvements latéraux et de l'exfiltration
- Reconstitution chronologique du déroulement de l'attaque
- Choix entre action interne et procédure judiciaire : critères et conséquences

Fil rouge · À partir de plusieurs millions de lignes de journaux, Inès isole les traces pertinentes, identifie un accès VPN compromis comme vecteur initial et reconstitue les étapes ayant mené au chiffrement.

Cours 4 · Contextualiser l'incident et élaborer le plan de remédiation

22 h

OBJECTIFS

- Corréler signes d'incident et traces collectées à l'aide d'outils de modélisation et de visualisation pour bâtir des scénarios d'incident
- Élaborer un plan de remédiation conforme à la PSSI, assorti de recommandations aux collaborateurs

ÉVALUATION FORMATIVE

Livrable formatif : plan de remédiation rédigé à partir d'un cas, avec proposition argumentée de solutions de sécurité

CONTENUS

- Corrélation entre signes d'incident et traces techniques
- Outils de visualisation : graphes de relations, chronologies, tableaux de bord
- Construction et hiérarchisation de scénarios potentiels d'incident
- Stratégies de confinement et d'éradication
- Rédaction du plan de remédiation : actions, responsables, échéances, critères de clôture
- Analyse comparative des solutions de sécurité disponibles sur le marché
- Recommandations aux collaborateurs et communication de crise

Fil rouge · Inès présente au comité de crise deux scénarios d'attaque plausibles, puis rédige le plan de remédiation d'Hydronéa : réinitialisation des comptes privilégiés, durcissement du VPN, restauration ordonnée des serveurs et consignes aux utilisateurs.

Cours 5 · Enrichir la PSSI : analyse de risques, ISO 27001 et SMSI

22 h

OBJECTIFS

- Conduire une analyse de risques avec les méthodes EBIOS Risk Manager et Méhari
- Spécifier les exigences d'un SMSI selon la norme ISO 27001 et enrichir la PSSI en coordination avec le RSSI et la DSI

ÉVALUATION FORMATIVE

Étude de cas : réalisation d'un atelier EBIOS RM simplifié et proposition de modifications de la PSSI

CONTENUS

- Structure et rôle de la PSSI et des documents associés (chartes, procédures, politiques thématiques)
- Méthode EBIOS Risk Manager : ateliers, sources de risque, scénarios stratégiques et opérationnels
- Méthode Méhari : principes, bases de connaissances et usages
- Norme ISO 27001 : exigences du SMSI, déclaration d'applicabilité, mesures de l'annexe
- Intégration du retour d'expérience d'incident dans la PSSI
- Coordination avec le RSSI, la DSI et la direction juridique
- Résilience du SI : continuité d'activité et plan de reprise

Fil rouge · Après la crise, le RSSI confie à Inès la mise à jour de la PSSI d'Hydronéa. Elle anime un atelier EBIOS RM avec les responsables métiers et propose de nouvelles mesures alignées sur ISO 27001.

Cours 6 · Sensibiliser les collaborateurs et piloter l'amélioration continue

22 h

OBJECTIFS

- Organiser des actions de sensibilisation accessibles à tous les publics, y compris aux personnes en situation de handicap
- Définir des actions d'amélioration continue en coopérant avec la communauté (CERT, plateformes de partage, VirusTotal)

ÉVALUATION FORMATIVE

Mise en situation : conception d'un module de sensibilisation accessible et d'une fiche de partage d'indicateurs de compromission

CONTENUS

- Conception d'un programme de sensibilisation : vulnérabilités, correctifs, bonnes pratiques
- Exercices et cas pratiques sur les plans de réponse aux incidents
- Accessibilité des supports et des sessions : formats adaptés, sous-titrage, lisibilité, compatibilité avec les aides techniques
- Écosystème des CERT et CSIRT : rôles et modalités de coopération
- Partage d'indicateurs de compromission sur les plateformes communautaires
- Utilisation de VirusTotal et précautions de confidentialité
- Retour d'expérience et plan d'amélioration continue

Fil rouge · Inès organise un exercice de crise sur table pour les managers des cinq sites, avec des supports accessibles à un collaborateur malvoyant, puis partage les indicateurs de compromission de l'attaque avec le CERT sectoriel.

RNCP40640BC02 · 132 h

Analyser la menace cyber pesant sur une organisation

Cours 7 · Supervision de la sécurité et exploitation d'un SIEM

22 h

OBJECTIFS

- Exploiter un SIEM pour superviser les infrastructures et les événements de sécurité
- Retracer la chronologie d'une cyberattaque et mettre en évidence les signaux faibles

ÉVALUATION FORMATIVE

Laboratoire : création de règles de détection et reconstitution d'une chronologie d'attaque à partir de journaux fournis

CONTENUS

- Architecture d'un SIEM : collecte, normalisation, corrélation, stockage
- Choix des sources de journaux et politique de journalisation
- Écriture de règles de corrélation et de cas d'usage de détection
- Recherche de signaux faibles et chasse aux menaces
- Reconstitution de la chronologie d'une attaque dans le SIEM
- Apports de l'apprentissage automatique à la détection d'anomalies
- Organisation d'un SOC : niveaux, processus, indicateurs de pilotage

Fil rouge · Inès déploie des règles de corrélation dans le SIEM d'Hydronéa et découvre, a posteriori, des connexions nocturnes anormales qui avaient précédé l'attaque de plusieurs semaines.

Cours 8 · Détection en temps réel et architecture réseau de sécurité

22 h

OBJECTIFS

- Détecter en temps réel les incidents et menaces et en identifier les sources
- Configurer l'architecture réseau et les dispositifs de sécurité pour bloquer les tentatives d'intrusion

ÉVALUATION FORMATIVE

Cas pratique : détection et blocage de menaces à partir de journaux d'événements, avec QCM de validation

CONTENUS

- Segmentation et cloisonnement du réseau, y compris des systèmes industriels
- Pare-feu, proxys et filtrage applicatif
- Systèmes de détection et de prévention d'intrusion : signatures et comportements
- Détection sur les terminaux et sur le réseau
- Contrôle des accès et gestion des comptes à privilèges
- Identification des sources d'une attaque et blocage
- Durcissement des systèmes selon les guides de bonnes pratiques

Fil rouge · Inès propose une nouvelle segmentation isolant les automates des lignes de production et configure une sonde de détection qui bloque une tentative de connexion depuis une adresse déjà associée à l'attaquant.

Cours 9 · Analyse et catégorisation des codes malveillants

22 h

OBJECTIFS

- Analyser un code malveillant par des techniques statiques et dynamiques
- Identifier signatures et vecteurs d'attaque pour qualifier et catégoriser la menace

ÉVALUATION FORMATIVE

Cas pratique : analyse statique et dynamique d'un échantillon pédagogique et rédaction d'une fiche de qualification

CONTENUS

- Familles de codes malveillants : rançongiciels, chevaux de Troie, chargeurs, vers
- Mise en place d'un environnement d'analyse isolé
- Analyse statique : métadonnées, chaînes, imports, désassemblage
- Analyse dynamique : exécution contrôlée, observation des comportements système et réseau
- Techniques d'obfuscation et de contournement de l'analyse
- Rédaction de signatures de détection
- Qualification et fiche d'identité d'une menace

Fil rouge · Inès extrait l'échantillon du rançongiciel retrouvé sur un serveur d'Hydronéa, l'analyse dans un environnement isolé, identifie sa famille et rédige une signature de détection pour le SIEM.

Cours 10 · Développer des correctifs et outils de sécurité en Python, Bash et C++

22 h

OBJECTIFS

- Développer un correctif ou un outil de réponse à incident sous Kali Linux
- Programmer en Python, Bash et C++ des outils utilisables par les équipes

ÉVALUATION FORMATIVE

Cas pratique : développement d'un correctif à partir d'une vulnérabilité identifiée, avec revue de code

CONTENUS

- Environnement de développement sécurisé sous Kali Linux
- Scripts Bash d'automatisation : collecte, vérification, durcissement
- Python pour la sécurité : parsing de journaux, appels d'API, automatisation de la détection
- Écriture d'exécutables en C++ : compilation, gestion mémoire, bonnes pratiques
- Conception d'un correctif de sécurité : besoin, développement, tests, déploiement
- Documentation et transmission des outils aux équipes

Fil rouge · Inès développe un script Python qui repère sur les postes du groupe les traces laissées par le rançongiciel et un utilitaire en C++ qui neutralise son mécanisme de persistance.

Cours 11 · Modéliser et attribuer les intrusions : Kill Chain, Diamond Model, MITRE ATT&CK

22 h

OBJECTIFS

- Établir une grille d'analyse d'intrusion à l'aide de la Cyber Kill Chain, du Diamond Model et de la matrice MITRE ATT&CK
- Rédiger un rapport d'investigation modélisant une intrusion ciblée

ÉVALUATION FORMATIVE

Cas pratique : modélisation d'un article de blog en Kill Chain, Diamond Model et ATT&CK, présentation orale entre pairs

CONTENUS

- Principes et limites de l'attribution d'une cyberattaque
- Cyber Kill Chain : phases et points de rupture
- Diamond Model : adversaire, capacité, infrastructure, victime
- Matrice MITRE ATT&CK : tactiques, techniques, procédures
- Construction d'une grille d'analyse d'intrusion
- Modélisation d'une attaque à partir d'un rapport public
- Rédaction et soutenance orale d'un rapport d'investigation

Fil rouge · Inès cartographie l'attaque subie par Hydronéa dans la matrice MITRE ATT&CK et la compare à un rapport public décrivant un groupe ciblant les industriels de l'eau.

Cours 12 · Renseignement sur la menace et IA générative appliquée à la cybersécurité

22 h

OBJECTIFS

- Mettre en place un système de veille couvrant OSINT, SOCMINT, HUMINT et sources du Deep et Dark web
- Exploiter l'IA générative pour simuler des attaques et analyser les patterns de menaces émergentes

ÉVALUATION FORMATIVE

Cas pratique : programmation d'un outil de veille sur des menaces identifiées et note d'analyse sur l'exposition de l'entreprise

CONTENUS

- Cycle du renseignement sur la menace et besoins des parties prenantes
- OSINT, SOCMINT et flux commerciaux et communautaires
- HUMINT : sources humaines, capacités d'analyse et de corrélation
- Surveillance du Deep et du Dark web : méthodes et cadre légal
- Réduction de l'exposition de l'entreprise sur les réseaux sociaux et les moteurs de recherche
- Développement d'un outil de veille automatisé (scrapper)
- IA générative en cybersécurité : algorithmes, simulation d'attaques, détection de patterns
- Risques, limites et gouvernance des usages de l'IA en défense

Fil rouge · Inès découvre sur un forum du Dark web des identifiants de collaborateurs d'Hydronéa. Elle déploie un scrapper de veille et teste un modèle génératif pour simuler des courriels d'hameçonnage ciblant le groupe et entraîner la détection.

RNCP40640BC03 · 88 h

Auditer la sécurité technique d'une organisation

Cours 13 · Cadrer un audit de sécurité et animer la réunion de lancement

22 h

OBJECTIFS

- Analyser le périmètre des tests d'intrusion et définir les modalités et outils (nmap, Metasploit, Armitage)
- Animer une réunion de cadrage réunissant les fonctions SI, technique et conformité, en intégrant les besoins d'adaptation liés au handicap

ÉVALUATION FORMATIVE

Cas d'étude : étude de vulnérabilité et note de cadrage définissant le périmètre des tests d'intrusion

CONTENUS

- Typologies d'audit : boîte noire, grise, blanche, interne, externe
- Étude de vulnérabilité préalable et définition du périmètre
- Convention d'audit, autorisations et règles d'engagement
- Cadre légal : atteintes aux systèmes de traitement automatisé de données dans le Code pénal
- Choix des outils et modalités d'intervention
- Préparation et animation de la réunion de cadrage : objectifs, méthodes, planning, responsabilités
- Identification des besoins d'adaptation du dispositif pour les personnes en situation de handicap

Fil rouge · Le comité de direction d'Hydronéa commande un audit complet. Inès définit le périmètre et anime la réunion de cadrage avec la DSI, le responsable conformité et un responsable de site qui utilise un logiciel de lecture d'écran.

Cours 14 · Tests d'intrusion sur les systèmes et les réseaux

22 h

OBJECTIFS

- Réaliser des tests d'intrusion sur systèmes et réseaux selon une méthodologie reconnue
- Superviser l'application des protocoles de test dans un environnement de simulation sécurisé

ÉVALUATION FORMATIVE

Laboratoire : identification de l'ensemble des vulnérabilités d'un serveur cible, avec journal de test

CONTENUS

- Méthodologie des tests d'intrusion : reconnaissance, énumération, exploitation, post-exploitation
- Découverte et cartographie avec nmap
- Exploitation de vulnérabilités avec Metasploit et Armitage
- Attaques sur l'annuaire et escalade de privilèges
- Configuration d'un environnement de simulation sécurisé
- Pilotage des scénarios de test et communication au sein de l'équipe technique
- Veille technique sur les outils d'audit et les pratiques d'attaque

Fil rouge · Dans une réplique isolée du réseau d'un site d'Hydronéa, Inès supervise deux auditeurs, valide les scénarios de test et découvre un serveur de fichiers obsolète exploitable.

Cours 15 · Tests d'intrusion sur les applications web et mobiles

22 h

OBJECTIFS

- Réaliser des tests d'intrusion sur des applications web et mobiles avec les outils adéquats
- Valider l'application des scénarios de test selon les spécifications définies

ÉVALUATION FORMATIVE

Cas pratique : test d'une application web pédagogique vulnérable et documentation des failles trouvées

CONTENUS

- Référentiels de vulnérabilités applicatives web et mobiles
- Proxy d'interception et analyse des échanges
- Injections, contournement d'authentification, gestion de session
- Tests des API et des services exposés
- Analyse d'applications mobiles : stockage local, communications, permissions
- Traçabilité des tests et preuves de vulnérabilité
- Respect du périmètre autorisé et gestion des incidents en cours de test

Fil rouge · Inès teste le portail client web et l'application mobile de télémaintenance d'Hydronéa, et met en évidence une faille d'authentification permettant d'accéder aux données d'autres clients.

Cours 16 · Rédiger le rapport d'audit et restituer les résultats

22 h

OBJECTIFS

- Élaborer un rapport détaillé comprenant captures d'écran et contre-mesure pour chaque vulnérabilité
- Présenter les résultats aux décideurs et aux équipes techniques à l'aide d'outils de visualisation de données

ÉVALUATION FORMATIVE

Livrable formatif : rapport de résultats avec correctifs proposés et restitution orale simulée

CONTENUS

- Structure d'un rapport d'audit : synthèse managériale, détails techniques, annexes
- Cotation des vulnérabilités et évaluation des impacts
- Rédaction des contre-mesures et du plan de remédiation
- Captures d'écran et preuves : sélection et anonymisation
- Visualisation des vulnérabilités et des impacts pour les décideurs
- Préparation et animation de la session de restitution
- Planification des suivis et contre-audit

Fil rouge · Inès rédige le rapport d'audit d'Hydronéa et le présente au comité de direction avec un tableau de bord des risques, puis anime une seconde séance technique avec les équipes d'exploitation.

RNCP40640BC04 · 88 h

Réaliser une analyse technico-légale (forensique)

Cours 17 · Cadrer l'investigation et définir la stratégie de préservation des données

22 h

OBJECTIFS

- Identifier le périmètre et l'environnement technique pour évaluer la volumétrie des données à acquérir, conformément à la PSSI
- Définir la stratégie de préservation et rédiger le document de traçabilité en lien avec les équipes juridiques

ÉVALUATION FORMATIVE

Étude de cas : note de cadrage d'investigation et document de traçabilité à compléter

CONTENUS

- Principes de l'investigation technico-légale : intégrité, reproductibilité, traçabilité
- Identification du périmètre : systèmes, supports, sauvegardes, services en ligne
- Évaluation de la volumétrie et des contraintes de temps et de matériel
- Définition des exigences avec les responsables IT et projet
- Cadre légal et éthique : vie privée, données personnelles, droit du travail, recevabilité de la preuve
- Chaîne de conservation et document de traçabilité des actions
- Choix de la stratégie de préservation selon le contexte

Fil rouge · Hydronéa décide de déposer plainte. Inès recense les serveurs, postes et smartphones à examiner, estime la volumétrie et valide avec la direction juridique la stratégie de préservation.

Cours 18 · Collecte technico-légale des données

22 h

OBJECTIFS

- Réaliser des copies technico-légales avec des outils open source (dd, dcfldd) et commerciaux (FTK Imager)
- Extraire les données de supports amovibles en respectant les politiques internes et les cadres légaux

ÉVALUATION FORMATIVE

Laboratoire : acquisition d'une image disque avec vérification d'intégrité et fiche de traçabilité

CONTENUS

- Bloqueurs d'écriture et matériel d'acquisition
- Création de copies avec dd et dcfldd
- Acquisition avec FTK Imager
- Calcul et vérification des empreintes
- Acquisition de la mémoire vive et des données volatiles
- Extraction des données de clés USB et supports amovibles
- Collecte sur smartphones : modes d'extraction et limites

Fil rouge · Inès réalise les copies technico-légales des disques de deux serveurs et du poste de l'administrateur dont le compte a été compromis, en consignant chaque action et chaque empreinte.

Cours 19 · Analyse forensique avancée des artefacts numériques

22 h

OBJECTIFS

- Analyser disques, mémoires, traces réseau, journaux, emails, navigateurs et smartphones avec des logiciels forensiques avancés
- Tracer et documenter les preuves numériques pour les besoins de l'enquête

ÉVALUATION FORMATIVE

Cas d'étude : analyse technico-légale de copies de disque dur et de smartphone fournies sous forme de scénario

CONTENUS

- Analyse des systèmes de fichiers et récupération de données supprimées
- Artefacts Windows et Linux : registre, journaux, traces d'exécution
- Analyse mémoire approfondie
- Analyse des traces réseau et des captures de trafic
- Messageries et emails : en-têtes, pièces jointes, hameçonnage
- Artefacts de navigateurs
- Analyse de copies de smartphones
- Corrélation des artefacts et frise chronologique de l'enquête

Fil rouge · En analysant l'image du poste de l'administrateur et la copie de son smartphone, Inès retrouve le courriel d'hameçonnage initial et démontre comment ses identifiants VPN ont été dérobés.

Cours 20 · Rédiger et communiquer le rapport d'analyse forensique

22 h

OBJECTIFS

- Rédiger un rapport forensique mettant en avant implications légales, conclusions techniques et recommandations de sécurité
- Adapter le discours aux publics techniques et institutionnels et garantir l'accessibilité du rapport

ÉVALUATION FORMATIVE

Livrable formatif : restitution écrite d'un scénario forensique avec présentation synthétique des résultats

CONTENUS

- Structure d'un rapport d'analyse forensique
- Formulation des constatations : faits, hypothèses, limites
- Implications légales et articulation avec la procédure judiciaire
- Recommandations de sécurité issues de l'investigation
- Adaptation du discours aux forces de l'ordre, au magistrat et à l'équipe de réponse à incidents
- Accessibilité du rapport : structure, contrastes, alternatives textuelles, formats compatibles
- Présentation synthétique et soutenance des résultats

Fil rouge · Inès remet le rapport forensique à la direction juridique d'Hydronéa, en prépare une version synthétique pour l'enquêteur et le magistrat, et présente ses conclusions à l'équipe de réponse à incidents.

05 · CONFORMITÉ AU RÉFÉRENTIEL

Couverture des compétences

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

Compétence	Bloc	Cours
Coordonner la collecte des informations relatives aux incidents avec des outils open source	RNCP40640BC01	1, 2
Trier et catégoriser les éléments liés à l'incident	RNCP40640BC01	3
Analyser les preuves numériques selon la méthodologie forensique et reconstituer l'attaque	RNCP40640BC01	3
Contextualiser l'incident par corrélation et visualisation pour établir des scénarios	RNCP40640BC01	1, 4
Élaborer un plan de remédiation conforme à la PSSI	RNCP40640BC01	4
Organiser une sensibilisation accessible aux bonnes pratiques de cybersécurité	RNCP40640BC01	6
Enrichir la PSSI avec EBIOS, Méhari, ISO 27001 et les exigences du SMSI	RNCP40640BC01	5
Définir des actions d'amélioration continue avec les CERT et plateformes de partage	RNCP40640BC01	6
Superviser les infrastructures et les événements de sécurité avec un SIEM	RNCP40640BC02	7
Détecter en temps réel les menaces et configurer l'architecture de sécurité	RNCP40640BC02	8
Analyser le code malveillant par analyse statique et dynamique	RNCP40640BC02	9
Exploiter l'intelligence artificielle générative pour la prévention et la détection	RNCP40640BC02	7, 12
Développer un correctif de sécurité en Python, Bash et C++ sous Kali Linux	RNCP40640BC02	10
Attribuer l'incident avec la Kill Chain, le Diamond Model et MITRE ATT&CK	RNCP40640BC02	11
Anticiper les menaces par un système de veille OSINT, SOCMINT, HUMINT, Deep et Dark web	RNCP40640BC02	12
Analyser le périmètre des tests d'intrusion et définir modalités et outils	RNCP40640BC03	13
Animer la réunion de cadrage de l'audit de sécurité	RNCP40640BC03	13
Réaliser des tests d'intrusion dans le respect du Code pénal	RNCP40640BC03	13, 14, 15
Superviser l'application des protocoles de test en environnement sécurisé	RNCP40640BC03	14, 15
Élaborer le rapport détaillé des tests avec contre-mesures	RNCP40640BC03	16
Présenter les résultats de l'audit aux décideurs et aux équipes techniques	RNCP40640BC03	16
Identifier le périmètre et l'environnement technique de l'investigation	RNCP40640BC04	17
Définir la stratégie de préservation des données et le document de traçabilité	RNCP40640BC04	17
Réaliser la collecte de données de manière technico-légale	RNCP40640BC04	18
Analyser les artefacts numériques avec des techniques forensiques avancées	RNCP40640BC04	19
Rédiger un rapport d'analyse forensique adapté et accessible	RNCP40640BC04	20

Évaluations formatives

Chaque sous-chapitre se conclut par un QCM d'auto-positionnement permettant à l'apprenant de vérifier l'acquisition des notions clés. Chaque cours comporte en outre une évaluation formative appliquée : laboratoire guidé, étude de cas, livrable professionnel ou mise en situation orale, systématiquement ancrés dans le fil rouge Hydronéa Industries. Les livrables reproduisent les productions attendues dans le métier (plan de remédiation, règles de détection, fiche de qualification de malware, rapport d'audit, rapport forensique). Des grilles critériées sont fournies pour permettre aux formateurs de l'organisme de formation d'apprécier la progression, de délivrer un retour individualisé et de documenter le suivi pédagogique attendu dans le cadre de Qualiopi.

Modalités de certification

Bloc	Modalité d'évaluation
RNCP40640BC01	Cas d'études : à partir de journaux d'événements fournis, le candidat réunit les traces informatiques liées à l'incident et les trie pour identifier celles qui sont pertinentes. Il rédige un plan de remédiation et propose des solutions de sécurité en analysant les solutions existantes sur le marché.
RNCP40640BC02	Cas pratique : à partir de journaux d'événements, le candidat détecte les incidents et menaces afin de les bloquer, analyse et qualifie les codes malveillants et propose des correctifs. Test écrit : évaluation de l'assimilation des termes et définitions. Cas pratique : modélisation d'un article de blog selon la matrice MITRE ATT&CK, la Cyber Kill Chain et le Diamond Model, rédaction d'un rapport d'investigation et évaluation orale par les pairs. Cas pratique : programmation d'un outil de veille (scrapper) sur les menaces identifiées.
RNCP40640BC03	Cas d'étude : à partir d'un cas fourni par le formateur, le candidat réalise une étude de vulnérabilité visant à définir le périmètre des tests d'intrusion. Cas pratique : le candidat identifie l'ensemble des vulnérabilités d'un serveur et remet un rapport des résultats accompagné d'une proposition de correctifs.
RNCP40640BC04	Cas d'études : à partir de scénarios comportant des copies de disques durs et de smartphones, le candidat réalise une analyse technico-légale des supports à l'aide d'outils dédiés, puis produit une restitution écrite relatant le scénario, son analyse et une présentation synthétique des résultats.

Le parcours reproduit, cours après cours, le format des épreuves officielles : tri de journaux et plan de remédiation (cours 3 et 4), détection et qualification de codes malveillants avec proposition de correctifs (cours 8, 9 et 10), modélisation ATT&CK, Kill Chain et Diamond Model avec présentation orale entre pairs (cours 11), programmation d'un scrapper de veille (cours 12), étude de vulnérabilité et audit de serveur (cours 13 et 14), analyse de copies de disques et de smartphones avec restitution écrite (cours 19 et 20). Les QCM préparent au test écrit sur la terminologie. L'organisme de formation reste seul responsable de l'organisation de la certification auprès du certificateur, l'Université de Technologie de Troyes ; SFM fournit le contenu pédagogique aligné sur le référentiel.

Moyens pédagogiques et débouchés

Moyens pédagogiques et techniques

- Plateforme e-learning en marque blanche, au format SCORM, avec suivi de progression et traçabilité des connexions et des résultats
- Une vidéo de 3 à 5 minutes par sous-chapitre (30 % du volume horaire), complétée par des cours texte enrichis, infographies, études de cas, mises en situation et QCM
- Laboratoires guidés pas à pas sur la distribution Kali Linux, à déployer dans un environnement virtualisé isolé mis à disposition par l'organisme de formation
- Jeux de données pédagogiques fictifs : journaux d'événements, captures réseau, images disques, copies de smartphones et échantillons malveillants neutralisés
- Modèles de livrables professionnels : fiche de qualification d'incident, plan de remédiation, convention d'audit, rapport de tests d'intrusion, document de traçabilité, rapport forensique
- Grilles d'évaluation critériées et corrigés destinés aux formateurs de l'organisme de formation
- Supports conçus pour l'accessibilité : vidéos sous-titrées, transcriptions, documents structurés compatibles avec les aides techniques

Débouchés et évolutions

- Expert en cybersécurité ou expert en sécurité des systèmes d'information
- Ingénieur sécurité informatique ou ingénieur sécurité web
- Auditeur en sécurité des SI et expert en tests d'intrusion
- Architecte de sécurité des systèmes d'information
- Responsable sécurité des SI ou responsable sécurité informatique
- Expert sécurité, méthode et qualité informatique

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 RNCP40640 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.