

SCHOOL FOR MATE

LIVRET PÉDAGOGIQUE

Architecte réseaux et cybersécurité (MS)

RNCP38140 · Certification RNCP · Niveau 7

Ce parcours prépare à la certification RNCP38140 « Architecte réseaux et cybersécurité (MS) » de niveau 7. Il couvre l'ensemble du référentiel : concevoir une architecture réseau sécurisée, piloter des projets de cybersécurité, gouverner la sécurité de l'information et défendre un système d'information face aux cyberattaques.

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

01 · PRÉSENTATION

La formation en bref

Intitulé	Architecte réseaux et cybersécurité (MS)
Code	RNCP38140
Type	Certification RNCP
Niveau	Niveau 7
Certificateur	INSTITUT MINES TELECOM - TELECOM PARIS
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	18/10/2028

Le métier et les compétences visées

L'architecte réseaux et cybersécurité est l'expert qui conçoit et fait évoluer des réseaux télécoms et des systèmes d'information sécurisés dès leur conception. Il analyse le besoin de l'organisation et intègre les contraintes réglementaires, techniques et de qualité de service. Il traduit ce besoin en architecture fonctionnelle puis en spécifications techniques. Il pilote les projets de sécurité, mène les analyses de risque, contribue à la politique de sécurité et organise la détection et le traitement des incidents, jusqu'au plan de continuité et de reprise d'activité. Il est le référent de son domaine. À ce titre, il assure la veille technologique et conseille, forme et alerte les directions sur les risques liés au SI, conformément aux exigences de l'ANSSI et aux réglementations applicables.

Public visé

- Ingénieurs réseaux, systèmes ou télécoms souhaitant se spécialiser en architecture et cybersécurité
- Administrateurs systèmes et réseaux expérimentés visant un poste d'architecte ou d'expert sécurité
- Chefs de projet informatique souhaitant piloter des projets de sécurisation du SI
- Consultants en systèmes d'information orientant leur activité vers le conseil en cybersécurité
- Professionnels en reconversion justifiant d'une expérience significative en informatique, éligibles par validation des acquis personnels et professionnels (VAPP)

Prérequis

- Être titulaire, ou dans l'année d'obtention, d'un diplôme d'ingénieur habilité CTI, d'un diplôme d'école de management conférant le grade de Master, d'un diplôme de niveau Bac+5 ou d'un titre RNCP de niveau 7
- À défaut, être titulaire d'un M1 ou équivalent avec au moins trois années d'expérience professionnelle
- Conditions dérogatoires possibles, dans les limites fixées par le référentiel : VAPP pour les candidats justifiant d'au moins 5 années d'expérience en lien avec les compétences visées, M1 validé sans expérience, ou L3 avec 3 ans d'expérience adaptée
- Disposer de bases solides en réseaux (modèle TCP/IP, routage, commutation) et en administration de systèmes

Objectifs pédagogiques

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

- Analyser le besoin d'une organisation et transposer un cahier des charges en exigences de réalisation d'un réseau ou d'un SI sécurisé
- Concevoir une architecture fonctionnelle puis technique intégrant la sécurité dès la conception, en tenant compte de l'existant et des contraintes réglementaires
- Spécifier l'ingénierie sécurisée des éléments du réseau : protocoles, dimensionnement et règles de mise en œuvre
- Piloter un projet de cybersécurité en choisissant une méthode adaptée et en maîtrisant le triptyque coût, délai, qualité
- Constituer et mobiliser une équipe projet, et communiquer de façon accessible auprès de toutes les parties prenantes
- Conduire une analyse de risque selon une méthode de référence et proposer un plan de traitement des risques
- Contribuer à l'élaboration ou à l'évolution d'une politique de sécurité des systèmes d'information (PSSI)
- Sélectionner et comparer les solutions techniques de protection selon des critères de coût, de technique et de souveraineté
- Détecter, classifier et gérer les incidents de sécurité en s'appuyant sur un SOC ou un CERT
- Établir un plan de continuité et de reprise d'activité (PCA/PRA) opérationnel

02 · FIL ROUGE PÉDAGOGIQUE

Aurévia Santé

IK

Inès Kerbrat

Architecte réseaux et cybersécurité, rattachée à la direction des systèmes d'information

Groupe privé de santé : six cliniques régionales, un centre d'imagerie et une plateforme de téléconsultation

Aurévia Santé a grandi par rachats successifs. Son système d'information est hétérogène : réseaux de sites interconnectés sans cloisonnement, équipements biomédicaux connectés anciens, comptes à privilèges partagés et plateforme de téléconsultation hébergée chez un prestataire. Après une tentative d'intrusion par hameçonnage sur l'une des cliniques, la direction générale lance le programme « Bouclier Aurévia ». Ce programme doit refondre l'architecture réseau, structurer la gouvernance de la sécurité et doter le groupe d'une capacité de détection et de réponse aux incidents. Inès Kerbrat est recrutée pour porter ce programme. Elle travaille avec Marc Delaunay, DSI du groupe, avec le futur RSSI et avec les directeurs de site. Elle doit respecter les exigences propres aux données de santé et un budget contraint.

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 l'existant et recueille les besoins des cliniques. Elle conçoit ensuite l'architecture cible segmentée et sécurisée du groupe, puis la spécifie techniquement.
2. Bloc 2 : Inès structure le programme « Bouclier Aurévia » en projet. Elle planifie les lots, recrute son équipe et présente l'avancement au comité de direction et aux équipes soignantes.
3. Bloc 3 : Inès délimite le périmètre de sécurité et conduit l'analyse de risque du groupe. Elle propose les mesures prioritaires de la nouvelle PSSI et organise la remontée des incidents avec un SOC.
4. Bloc 4 : Inès choisit et déploie les solutions de protection, puis gère une cyberattaque simulée sur la clinique de Vannes. Elle formalise enfin le PCA/PRA qui garantit la continuité des soins.

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
RNCP38140BC01 · Réaliser l'architecture cybersécurisée d'un réseau télécom ou d'un système d'information		**154 h**
1	Analyser le besoin et cadrer un projet de réseau ou de SI sécurisé	22 h
2	Intégrer les facteurs externes : risques, réglementation, capacités et qualité de service	22 h
3	Concevoir l'architecture fonctionnelle d'un réseau télécom ou d'un SI	22 h
4	Transposer l'architecture en spécifications techniques et choisir les composants	22 h
5	Ingénierie sécurisée des éléments du réseau télécom	22 h
6	Intégrer la sécurité dans l'architecture : sécurité dès la conception	22 h
7	Veille technologique et évolutivité de l'architecture	22 h
RNCP38140BC02 · Piloter et réaliser un projet de développement de la cybersécurité dans le domaine des réseaux ou des systèmes d'information		**88 h**
8	Piloter un projet de cybersécurité : méthodes et suivi	22 h
9	Construire le plan de gestion du projet : planification, risques, coût, délai, qualité	22 h
10	Constituer l'équipe projet : plan de recrutement et management	22 h
11	Communiquer auprès des parties prenantes, y compris en situation de handicap	22 h
RNCP38140BC03 · Gérer la gouvernance de la sécurité des réseaux et des systèmes d'information		**88 h**
12	Définir le périmètre de sécurité à partir des normes et méthodes de référence	22 h
13	Réaliser une analyse de risque en sécurité	22 h
14	Contribuer à la politique de sécurité de l'information (PSSI)	22 h
15	Recueillir les incidents de sécurité : SOC, CERT et organisation de la réponse	22 h
RNCP38140BC04 · Sécuriser, protéger et défendre un réseau ou un système d'information		**110 h**
16	Sécuriser les communications, segmenter et filtrer le réseau	22 h
17	Détection d'intrusion, contrôle d'accès, traçabilité et sécurité physique	22 h
18	Comparer et choisir les solutions de sécurité du marché	22 h
19	Détecter, classifier et gérer les incidents de sécurité	22 h
20	Établir un plan de continuité et de reprise d'activité (PCA/PRA)	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

Contenu des cours

RNCP38140BC01 · 154 h

Réaliser l'architecture cybersécurisée d'un réseau télécom ou d'un système d'information

Cours 1 · Analyser le besoin et cadrer un projet de réseau ou de SI sécurisé — 22 h

OBJECTIFS

- Recueillir et formaliser le besoin des parties prenantes en tenant compte de l'existant
- Transposer un cahier des charges en exigences de réalisation fonctionnelles, techniques et de sécurité

ÉVALUATION FORMATIVE

QCM de fin de cours et étude de cas : rédaction d'une note d'exigences à partir d'un cahier des charges

CONTENUS

- Le rôle de l'architecte réseaux et cybersécurité dans l'organisation
- Techniques de recueil du besoin : entretiens, ateliers, questionnaires
- Audit et cartographie de l'existant : réseau, applications, flux, équipements
- Lecture critique d'un cahier des charges et identification des non-dits
- Formalisation des exigences fonctionnelles, non fonctionnelles et de sécurité
- Définition et validation d'une solution cible

Fil rouge · Inès mène des entretiens avec les directeurs de trois cliniques et le responsable biomédical, puis cartographie le réseau existant d'Aurévia Santé. Elle en déduit une note d'exigences qu'elle soumet au DSI.

Cours 2 · Intégrer les facteurs externes : risques, réglementation, capacités et qualité de service — 22 h

OBJECTIFS

- Identifier les facteurs externes influençant la conception ou l'évolution du système
- Intégrer les exigences réglementaires et de qualité de service dans la définition de la solution cible

ÉVALUATION FORMATIVE

QCM réglementaire et étude de cas : matrice des facteurs externes appliquée à un projet

CONTENUS

- Panorama réglementaire : textes rassemblés par l'ANSSI, Cybersecurity Act, protection des données personnelles
- Instructions ministérielles ACSSI et n°300 sur la protection contre les signaux compromettants
- Contraintes sectorielles : données de santé, opérateurs et fournisseurs stratégiques
- Enjeux de capacité, de disponibilité et de qualité de service
- Prise en compte des profils utilisateurs et des usages, y compris en mobilité
- Premiers éléments d'analyse de risque appliqués à la conception
- Synthèse des facteurs externes et impacts sur la solution cible

Fil rouge · Inès recense les obligations liées à l'hébergement des données de santé et les exigences de disponibilité de la téléconsultation. Elle complète ensuite la solution cible avec une matrice des contraintes externes.

Cours 3 · Concevoir l'architecture fonctionnelle d'un réseau télécom ou d'un SI

22 h

OBJECTIFS

- Traduire le besoin en architecture fonctionnelle adaptée à l'organisation
- Identifier et caractériser les éléments et fonctions du système en corrigeant les défaillances de l'existant

ÉVALUATION FORMATIVE

Exercice de modélisation corrigé et QCM sur les principes d'architecture

CONTENUS

- Principes et niveaux de l'architecture : métier, fonctionnelle, applicative, technique
- Modélisation fonctionnelle : blocs, fonctions, flux et interfaces
- Analyse des défaillances de l'existant et des points uniques de défaillance
- Architectures de réseaux d'entreprise : cœur, distribution, accès, interconnexion de sites
- Architectures de services : centres de données, cloud privé, public et hybride
- Documentation d'architecture : dossier d'architecture et schémas de référence

Fil rouge · Inès modélise l'architecture fonctionnelle cible reliant les six cliniques, le centre d'imagerie et la plateforme de téléconsultation. Elle corrige au passage les points uniques de défaillance relevés lors de l'audit.

Cours 4 · Transposer l'architecture en spécifications techniques et choisir les composants

22 h

OBJECTIFS

- Rédiger les spécifications de réalisation technique à partir de l'architecture fonctionnelle
- Déterminer les équipements matériels, logiciels et outils supports adaptés

ÉVALUATION FORMATIVE

Étude de cas : rédaction d'un extrait de dossier de spécifications techniques

CONTENUS

- Du fonctionnel au technique : méthode de déclinaison des spécifications
- Choix des équipements réseau : commutateurs, routeurs, pare-feu, contrôleurs sans fil
- Choix des composants systèmes et logiciels, virtualisation et conteneurs
- Outils supports : supervision, gestion de configuration, inventaire
- Critères de sélection : performance, sécurité, maintenabilité, coût total de possession
- Rédaction du dossier de spécifications techniques

Fil rouge · Inès décline l'architecture du groupe en spécifications techniques pour l'appel d'offres. Elle y précise les équipements de cœur de réseau et les outils de supervision.

Cours 5 · Ingénierie sécurisée des éléments du réseau télécom

22 h

OBJECTIFS

- Spécifier pour chaque élément du réseau ses fonctionnalités, ses protocoles et ses règles de dimensionnement
- Définir les règles de mise en œuvre sécurisée permettant le déploiement de la solution

ÉVALUATION FORMATIVE

Exercice de dimensionnement et QCM sur les protocoles et leur sécurisation

CONTENUS

- Protocoles de commutation et de routage et leur sécurisation (VLAN, OSPF, BGP)
- Réseaux étendus et interconnexions de sites : MPLS, SD-WAN, VPN
- Réseaux sans fil sécurisés et réseaux d'objets connectés
- Dimensionnement : débits, latence, redondance, haute disponibilité
- Durcissement des équipements réseau et gestion des configurations
- Qualité de service et priorisation des flux critiques
- Plan de déploiement et règles de mise en œuvre

Fil rouge · Inès dimensionne l'interconnexion des sites et spécifie le réseau sans fil des services de soins. Elle s'assure que les flux d'imagerie médicale restent prioritaires.

Cours 6 · Intégrer la sécurité dans l'architecture : sécurité dès la conception

22 h

OBJECTIFS

- Définir une architecture intégrant la sécurité à chaque niveau du SI ou du réseau
- Proposer et justifier des choix technologiques de sécurisation

ÉVALUATION FORMATIVE

Étude de cas individuelle : production d'un schéma d'architecture sécurisée argumenté

CONTENUS

- Principes de sécurité dès la conception et de défense en profondeur
- Modèles d'architecture : zones de confiance, DMZ, zéro confiance
- Cloisonnement des systèmes sensibles et des équipements biomédicaux
- Sécurisation des architectures cloud et hybrides
- Administration sécurisée : postes et réseaux d'administration dédiés, bastions
- Recommandations de l'ANSSI en matière d'architecture
- Argumentaire des choix technologiques de sécurité

Fil rouge · Inès propose au DSI une architecture en zones de confiance qui isole les équipements biomédicaux et l'administration du SI. Elle défend ses choix technologiques devant le comité technique.

Cours 7 · Veille technologique et évolutivité de l'architecture

22 h

OBJECTIFS

- Anticiper la croissance et les évolutions du système à partir d'une veille continue
- Garantir l'alignement durable de l'architecture avec la stratégie de l'entreprise

ÉVALUATION FORMATIVE

Livrable : note de veille et feuille de route d'évolution, préparatoire au projet collectif soutenu devant un jury

CONTENUS

- Organiser une veille technologique et réglementaire : sources, outils, diffusion
- Technologies émergentes : 5G privée, virtualisation des fonctions réseau, SASE
- Évolutions des facteurs externes et impacts sur l'architecture
- Gestion de la croissance : capacité, scalabilité, obsolescence
- Alignement stratégique du SI et schéma directeur
- Feuille de route d'évolution de l'architecture

Fil rouge · Aurévia Santé annonce le rachat de deux nouvelles cliniques. Inès met à jour la feuille de route d'architecture et présente une note de veille sur les technologies d'accès sécurisé.

RNCP38140BC02 · 88 h

Piloter et réaliser un projet de développement de la cybersécurité dans le domaine des réseaux ou des systèmes d'information

Cours 8 · Piloter un projet de cybersécurité : méthodes et suivi

22 h

OBJECTIFS

- Sélectionner la méthode de gestion de projet adaptée à un projet de cybersécurité
- Assurer la conformité au cahier des charges et rédiger des comptes rendus de suivi et d'avancement

ÉVALUATION FORMATIVE

QCM et exercice de rédaction d'un compte rendu d'avancement

CONTENUS

- Spécificités des projets de cybersécurité réseaux et SI
- Méthodes prédictives, agiles et hybrides : critères de choix
- Gouvernance du projet : comités, rôles, circuits de décision
- Contrôle de conformité au cahier des charges et recette
- Indicateurs de pilotage et tableaux de bord
- Rédaction de comptes rendus de suivi et d'avancement

Fil rouge · Inès choisit une approche hybride pour le programme « Bouclier Aurévia » et met en place sa gouvernance. Elle rédige ensuite le premier compte rendu d'avancement pour le comité de pilotage.

Cours 9 · Construire le plan de gestion du projet : planification, risques, coût, délai, qualité

22 h

OBJECTIFS

- Ordonnancer les tâches et établir un planning réaliste
- Dresser la cartographie des risques projet et des palliatifs, et déterminer les éléments de coût, de délai et de qualité

ÉVALUATION FORMATIVE

Étude de cas : élaboration d'un plan de gestion de projet avec cartographie des risques

CONTENUS

- Découpage du projet : organigramme des tâches et lots
- Ordonnancement, chemin critique et diagramme de Gantt
- Cartographie des risques projet et plans de mitigation
- Estimation des charges et construction du budget
- Plan qualité et critères d'acceptation des livrables
- Plan de gestion du projet : structure et diffusion

Fil rouge · Inès planifie les lots de refonte réseau site par site, sans interrompre les soins. Elle identifie le risque de retard de livraison des équipements et prévoit des palliatifs.

Cours 10 · Constituer l'équipe projet : plan de recrutement et management

22 h

OBJECTIFS

- Élaborer un plan de recrutement fondé sur les compétences nécessaires et les contraintes du projet
- Argumenter ce plan pour obtenir l'accord de la hiérarchie

ÉVALUATION FORMATIVE

Mise en situation : présentation argumentée d'un plan de recrutement

CONTENUS

- Identification des compétences requises à partir des livrables du projet
- Arbitrage entre ressources internes, recrutement et prestataires
- Fiches de poste et profils en cybersécurité
- Construction du plan de recrutement sous contraintes de coût, de délai et de qualité
- Prise en compte de la diversité et de l'inclusion dans le recrutement
- Présentation et défense du plan auprès de la hiérarchie
- Animation et management de l'équipe projet

Fil rouge · Inès évalue les compétences manquantes en sécurité réseau et en détection d'incidents. Elle présente au DSI un plan de recrutement mêlant embauches et renfort externe.

Cours 11 · Communiquer auprès des parties prenantes, y compris en situation de handicap

22 h

OBJECTIFS

- Adapter le support et le message aux différentes parties prenantes du projet
- Concevoir une communication accessible et argumenter sur les enjeux pour mobiliser les acteurs

ÉVALUATION FORMATIVE

Soutenance orale simulée du projet devant un jury, préparatoire à l'épreuve collective

CONTENUS

- Cartographie et analyse des parties prenantes
- Plan de communication projet
- Argumenter les enjeux de cybersécurité auprès de publics non techniques
- Accessibilité des supports : principes du RGAA, documents et présentations accessibles
- Communication orale : réunions, comités, soutenance
- Gestion des résistances au changement

Fil rouge · Inès prépare une présentation du programme pour le comité de direction et un support accessible destiné aux équipes soignantes, dont un cadre de santé malvoyant.

RNCP38140BC03 · 88 h

Gérer la gouvernance de la sécurité des réseaux et des systèmes d'information

Cours 12 · Définir le périmètre de sécurité à partir des normes et méthodes de référence

22 h

OBJECTIFS

- S'appuyer sur les normes et méthodes de référence pour définir le périmètre de sécurité
- Recenser les biens supports, réseaux, informations et personnes à retenir

ÉVALUATION FORMATIVE

QCM sur les normes et étude de cas : formalisation d'un périmètre de sécurité

CONTENUS

- Gouvernance de la sécurité : rôles du RSSI, de la direction et des métiers
- Normes de la famille ISO/IEC 27000 et système de management de la sécurité de l'information
- Guides et référentiels de l'ANSSI
- Identification des valeurs métier et des biens supports
- Inventaire et classification des informations
- Formalisation du périmètre de sécurité

Fil rouge · Inès anime un atelier avec les métiers pour recenser les valeurs métier d'Aurévia Santé, comme le dossier patient ou la prise de rendez-vous, et les biens supports associés.

Cours 13 · Réaliser une analyse de risque en sécurité

22 h

OBJECTIFS

- Conduire une analyse de risque selon une méthode appropriée
- Identifier les principaux risques et failles, et proposer un plan de traitement

ÉVALUATION FORMATIVE

Étude de cas : livrable d'analyse de risque avec plan de traitement

CONTENUS

- Concepts : menace, vulnérabilité, impact, vraisemblance
- Panorama des méthodes : EBIOS Risk Manager, ISO/IEC 27005
- Ateliers EBIOS RM : socle, sources de risque, scénarios stratégiques et opérationnels
- Évaluation et cartographie des risques
- Options de traitement : réduire, transférer, éviter, accepter
- Plan de traitement des risques et risques résiduels

Fil rouge · Inès conduit une analyse EBIOS RM sur la plateforme de téléconsultation. Elle met en évidence un scénario de compromission passant par le prestataire d'hébergement.

Cours 14 · Contribuer à la politique de sécurité de l'information (PSSI)

22 h

OBJECTIFS

- Identifier les éléments prioritaires à protéger à partir de l'analyse de risque et des documents d'architecture
- Proposer des mesures organisationnelles et techniques pour faire évoluer la PSSI

ÉVALUATION FORMATIVE

Étude de cas : livrable de propositions de mesures pour une PSSI

CONTENUS

- Structure et contenu d'une PSSI
- Exploitation de l'analyse de risque et des documents d'architecture
- Priorisation des mesures organisationnelles et techniques
- Chartes, procédures et sensibilisation des utilisateurs
- Gestion des tiers et sécurité de la chaîne d'approvisionnement
- Indicateurs de sécurité et amélioration continue

Fil rouge · Inès propose au futur RSSI les mesures prioritaires de la PSSI du groupe. Elle y intègre la gestion des comptes à privilèges et les exigences contractuelles imposées aux prestataires.

Cours 15 · Recueillir les incidents de sécurité : SOC, CERT et organisation de la réponse

22 h

OBJECTIFS

- Organiser la remontée des incidents de sécurité en s'appuyant sur l'analyse de risque, un SOC ou un CERT
- Structurer techniquement les mesures de sécurité face à une cyberattaque

ÉVALUATION FORMATIVE

Étude de cas : livrable de processus de recueil et de gestion des incidents

CONTENUS

- Rôles et fonctionnement d'un SOC et d'un CERT ou CSIRT
- Liens entre analyse de risque et cas d'usage de détection
- Circuits de signalement internes et externes, obligations de notification
- Processus de gestion des incidents et matrice de responsabilités
- Externalisation d'un SOC : critères et contractualisation
- Organisation technique des mesures de réponse

Fil rouge · Inès définit avec un SOC externe les scénarios de détection prioritaires, issus de l'analyse de risque. Elle formalise aussi le circuit de signalement des incidents des cliniques.

RNCP38140BC04 · 110 h

Sécuriser, protéger et défendre un réseau ou un système d'information

Cours 16 · Sécuriser les communications, segmenter et filtrer le réseau

22 h

OBJECTIFS

- Mettre en place des solutions de sécurisation des communications : protocoles, chiffrement, certificats
- Concevoir la segmentation, le cloisonnement et le filtrage du réseau

ÉVALUATION FORMATIVE

Travaux pratiques guidés et QCM sur la cryptographie et le filtrage

CONTENUS

- Fondamentaux de la cryptographie : symétrique, asymétrique, hachage
- Protocoles sécurisés : TLS, IPsec, SSH
- Infrastructures de gestion de clés et cycle de vie des certificats
- Segmentation et cloisonnement : VLAN, microsegmentation, zones
- Dispositifs de filtrage : pare-feu, proxy, filtrage applicatif
- Politique de filtrage et revue des règles

Fil rouge · Inès déploie une infrastructure de gestion de clés interne pour les échanges entre cliniques. Elle rédige ensuite la politique de filtrage entre les zones du nouveau réseau.

Cours 17 · Détection d'intrusion, contrôle d'accès, traçabilité et sécurité physique

22 h

OBJECTIFS

- Mettre en œuvre des solutions de détection et de protection contre les intrusions sur le réseau et les terminaux
- Déployer l'authentification forte, le contrôle d'accès, la traçabilité et les mesures de sécurité physique

ÉVALUATION FORMATIVE

Étude de cas : plan de déploiement des mesures techniques de protection

CONTENUS

- IDS et IPS réseau, protection et détection sur les terminaux (EDR)
- Gestion des identités et des accès, authentification multifacteur
- Gestion des comptes à privilèges et principe du moindre privilège
- Journalisation et traçabilité en temps réel et en temps différé, SIEM
- Sécurité physique des locaux et des équipements, protection contre les signaux compromettants
- Outils de contrôle et d'audit de la sécurité

Fil rouge · Inès généralise l'authentification multifacteur pour les accès distants des médecins. Elle centralise aussi la journalisation des équipements critiques du groupe.

Cours 18 · Comparer et choisir les solutions de sécurité du marché

22 h

OBJECTIFS

- Analyser les solutions du marché adaptées à la protection du SI ou du réseau
- Comparer les solutions selon des critères de coût, de technique et de souveraineté pour aider à la décision

ÉVALUATION FORMATIVE

Étude de cas : livrable de benchmark et note d'aide à la décision

CONTENUS

- Typologie des solutions de sécurité et des modèles de commercialisation
- Construction d'une grille d'analyse multicritère
- Enjeux de souveraineté : localisation des données, droit applicable, qualifications et visas de sécurité de l'ANSSI
- Certification de cybersécurité européenne issue du Cybersecurity Act
- Preuves de concept et tests comparatifs
- Note d'aide à la décision

Fil rouge · Inès compare trois solutions de détection sur les terminaux à l'aide d'une grille de critères. Elle recommande à la direction une solution conforme aux exigences de souveraineté du groupe.

Cours 19 · Détecter, classifier et gérer les incidents de sécurité

22 h

OBJECTIFS

- Mobiliser les outils de surveillance pour détecter et anticiper une cyberattaque
- Classifier les incidents et piloter leur traitement jusqu'à la clôture

ÉVALUATION FORMATIVE

Exercice de gestion d'incident simulé et livrable de rapport d'incident

CONTENUS

- Supervision de sécurité : sources, corrélation, cas d'usage
- Renseignement sur la menace et indicateurs de compromission
- Qualification et classification des incidents selon leur gravité
- Réponse à incident : confinement, éradication, remédiation
- Préservation des preuves et premiers éléments d'investigation numérique
- Gestion de crise cyber et communication
- Retour d'expérience et amélioration des mesures

Fil rouge · Une attaque par rançongiciel est simulée sur la clinique de Vannes. Inès qualifie l'incident, coordonne le confinement avec le SOC et anime le retour d'expérience.

Cours 20 · Établir un plan de continuité et de reprise d'activité (PCA/PRA)

22 h

OBJECTIFS

- Définir les processus de continuité et de reprise d'activité
- Identifier les ressources techniques et humaines et les compétences mobilisables pour rétablir le fonctionnement du système

ÉVALUATION FORMATIVE

Étude de cas : livrable de PCA/PRA, préparatoire à l'épreuve certificative

CONTENUS

- Bilan d'impact sur l'activité et identification des activités essentielles
- Objectifs de reprise : durée maximale d'interruption et perte de données admissible
- Stratégies techniques : sauvegardes, réplication, sites de secours
- Ressources humaines, compétences mobilisables et cellule de crise
- Rédaction des procédures de continuité et de reprise
- Tests, exercices et maintien en condition opérationnelle du plan

Fil rouge · Inès s'appuie sur le retour d'expérience de l'attaque simulée pour formaliser le PCA/PRA du groupe. Elle organise un premier exercice de bascule de la téléconsultation vers le site de secours.

05 · CONFORMITÉ AU RÉFÉRENTIEL

Couverture des compétences

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

Compétence	Bloc	Cours
Analyser le besoin et transposer le cahier des charges en exigences de réalisation	RNCP38140BC01	1, 3
Agréger les facteurs externes (risques, réglementation, technologies, capacités, qualité de service, utilisateurs, sécurité)	RNCP38140BC01	2, 7
Traduire le besoin en architecture fonctionnelle du réseau ou du SI	RNCP38140BC01	3
Transposer l'architecture fonctionnelle en spécifications techniques et composants	RNCP38140BC01	4, 5
Anticiper les évolutions du système par la veille et l'alignement stratégique	RNCP38140BC01	7
Concevoir l'ingénierie sécurisée des éléments du réseau télécom	RNCP38140BC01	5
Intégrer la sécurité dans l'architecture et les éléments du SI ou du réseau	RNCP38140BC01	6, 4
Piloter un projet de cybersécurité avec une méthode adaptée et des comptes rendus de suivi	RNCP38140BC02	8
Réaliser le plan de gestion du projet (tâches, risques, coût, délai, qualité)	RNCP38140BC02	9
Élaborer un plan de recrutement de l'équipe projet	RNCP38140BC02	10
Communiquer auprès des parties prenantes, y compris en situation de handicap	RNCP38140BC02	11
Définir le périmètre de sécurité à partir de normes et méthodes de référence	RNCP38140BC03	12
Réaliser une analyse de risque et proposer un traitement des risques	RNCP38140BC03	13
Proposer les éléments prioritaires à protéger pour la politique de sécurité de l'information	RNCP38140BC03	14
Recueillir les incidents de sécurité via l'analyse de risque, un SOC ou un CERT	RNCP38140BC03	15
Identifier les éléments techniques de sécurité (communications, segmentation, filtrage, IDS/IPS, authentification, traçabilité, sécurité physique)	RNCP38140BC04	16, 17
Analyser et comparer les outils du marché (coût, technique, souveraineté)	RNCP38140BC04	18
Détecter, classifier et gérer les incidents de sécurité	RNCP38140BC04	19, 15
Établir un plan de continuité et de reprise d'activités	RNCP38140BC04	20

Évaluations formatives

Chaque sous-chapitre se termine par un QCM d'auto-positionnement avec correction commentée. Chaque cours comporte en outre une évaluation formative alignée sur les modalités de certification du bloc : étude de cas, livrable professionnel (note d'exigences, analyse de risque, benchmark, PCA/PRA), exercice pratique ou soutenance simulée. Les mises en situation suivent le fil rouge Aurévia Santé. L'apprenant y produit des livrables proches de ceux qu'attend un employeur, et ces productions alimentent progressivement un portfolio réutilisable pour les épreuves. L'organisme de formation peut compléter ces évaluations par des corrections individualisées assurées par ses formateurs.

Modalités de certification

Bloc	Modalité d'évaluation
RNCP38140BC01	Étude de cas donnant lieu à une production individuelle ; mise en situation professionnelle dans le domaine des systèmes d'information sous forme de projet collectif soutenu devant un jury ; mise en situation professionnelle donnant lieu à un livrable et à une soutenance orale.
RNCP38140BC02	Mise en situation professionnelle sous forme de projet collectif, suivie d'une soutenance orale devant un jury.
RNCP38140BC03	Études de cas donnant lieu à la remise de livrables.
RNCP38140BC04	Études de cas donnant lieu à la remise de livrables.

Le parcours reprend fidèlement les formats d'épreuves du référentiel. Les études de cas de chaque cours entraînent à produire des livrables individuels structurés, notamment pour les blocs 3 et 4, évalués exclusivement sur livrables. Les cours 7 et 11 préparent aux projets collectifs et aux soutenances orales des blocs 1 et 2 : méthodologie de soutenance, supports accessibles, argumentation devant un jury. Le fil rouge Aurévia Santé offre un cas complet et cohérent, de l'architecture à la réponse aux incidents, qui sert de modèle pour les projets demandés. SFM fournit le contenu pédagogique. L'organisme de formation reste seul responsable de l'inscription des candidats, de l'organisation des épreuves en lien avec le certificateur et de la délivrance de la certification.

06 · MOYENS ET PERSPECTIVES

Moyens pédagogiques et débouchés

Moyens pédagogiques et techniques

- Plateforme e-learning accessible 24 h/24, en marque blanche aux couleurs de l'organisme de formation, avec suivi de progression et traçabilité des connexions
- Une vidéo de 3 à 5 minutes par sous-chapitre, représentant 30 % du volume horaire du parcours
- Cours texte enrichi, infographies et schémas d'architecture représentant 70 % du volume horaire avec les activités associées
- Études de cas et mises en situation professionnelles construites autour du fil rouge Aurévia Santé
- QCM d'auto-évaluation corrigés et commentés à la fin de chaque sous-chapitre
- Modèles de livrables téléchargeables : note d'exigences, dossier de spécifications, plan de gestion de projet, analyse de risque, grille de benchmark, PCA/PRA
- Ressources de référence et fiches de synthèse sur les normes, méthodes et recommandations de l'ANSSI

Débouchés et évolutions

- Architecte des réseaux et de la cybersécurité
- Responsable de la sécurité des systèmes d'information (RSSI) ou manager de la sécurité et des risques de l'information
- Consultant en cybersécurité ou en réseaux télécoms
- Chef de projet sécurité
- Architecte du SI et des plates-formes de services
- Expert technique en réseaux télécoms et en cybersécurité

Accessibilité

Contenus sous-titrés en français, contrastes conformes WCAG AA, navigation au clavier sur les écrans interactifs. L'organisme de formation qui diffuse le parcours adapte les modalités d'accompagnement aux personnes en situation de handicap avec son référent handicap.

Livrables fournis à l'organisme de formation

- Package SCORM 1.2 / 2004 et xAPI, compatible avec les principaux LMS
- Sources éditables des cours, scripts vidéo et banques de QCM
- Livret apprenant et grilles d'évaluation
- Licence marque blanche à vie, stagiaires illimités, maintenance 24 mois

School For Mate
On crée vos formations, vous n'avez plus qu'à les diffuser.

contact@schoolformate.com · catalogue-2026-sfm.netlify.app

Référentiel RNCP38140 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.