

SCHOOL FOR MATE

LIVRET PÉDAGOGIQUE

Expert IS : Option Manager cybersécurité

RNCP40573 · Certification RNCP · Niveau 7

Ce parcours de 440 heures prépare au titre RNCP40573 Expert en informatique et systèmes d'information (niveau 7), option Manager cybersécurité, en couvrant l'intégralité des blocs de compétences du référentiel. Le parcours suit la progression d'une ingénieure SI dans une mutuelle d'assurance fictive, de la stratégie SI au management de la cybersécurité. Vos apprenants y développent les réflexes d'un expert capable de concevoir, piloter et sécuriser un système d'information.

VOLUME HORAIRE	COURS	BLOCS
440 h	20	6

01 · PRÉSENTATION

La formation en bref

Intitulé	Expert IS : Option Manager cybersécurité
Code	RNCP40573
Type	Certification RNCP
Niveau	Niveau 7
Certificateur	3W ACADEMY
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	30/04/2030

Le métier et les compétences visées

L'expert en informatique et systèmes d'information spécialisé en management de la cybersécurité définit la stratégie SI. Il pilote des projets de transformation digitale et conçoit des applications en plaçant la sécurité au cœur de chaque décision. Il cartographie les risques qui pèsent sur la confidentialité, l'intégrité et la disponibilité des actifs. Il élabore une stratégie de cybersécurité conforme aux normes, aux accords de niveaux de service, au RGPD et aux obligations légales en cas de cyberattaque. Il fait évaluer les protections par des tests d'intrusion et conduit les investigations forensic après un incident. Il alimente aussi des indicateurs qui éclairent la direction. Il exerce en ESN, en société de conseil, chez un constructeur informatique ou dans le secteur tertiaire (banque, assurance).

Public visé

- Titulaires d'un diplôme ou titre de niveau 6 en informatique souhaitant évoluer vers un poste d'expert en cybersécurité
- Développeurs, administrateurs systèmes et réseaux ou chefs de projet IT justifiant d'une expérience professionnelle équivalente
- Diplômés de niveau 7 en spécialité scientifique en reconversion vers les métiers de la sécurité des systèmes d'information
- Salariés d'ESN, de sociétés de conseil ou de DSI du secteur tertiaire engagés dans un projet de montée en compétences
- Candidats à une démarche de reconversion professionnelle accompagnée par un organisme de formation ou un CFA

Prérequis

- Être titulaire d'un diplôme ou titre de niveau 6 en spécialité informatique, ou justifier d'une expérience professionnelle équivalente
- Ou être titulaire d'un diplôme ou titre de niveau 7 en spécialité scientifique, ou justifier d'une expérience professionnelle équivalente
- Disposer d'un poste informatique avec une connexion internet stable permettant l'accès à la plateforme et aux environnements de travaux pratiques

Objectifs pédagogiques

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

- Concevoir une veille technologique et réglementaire et la restituer sous forme de recommandations argumentées aux parties prenantes
- Élaborer une stratégie informatique à partir d'une cartographie du SI et d'une analyse de risques
- Comparer et recommander des architectures SI selon leurs critères de performance, de scalabilité, de sécurité et d'éco-conception
- Rédiger une étude d'opportunité, un cahier des charges technique conforme au RGPD et accessible aux PSH, ainsi qu'une note de cadrage
- Planifier et piloter un projet informatique en mobilisant les parties prenantes et en organisant la capitalisation des compétences
- Concevoir et développer une application métier sécurisée, testée et suivie par un cycle qualité automatisé
- Cartographier les risques de sécurité d'un SI et élaborer une stratégie de cybersécurité conforme aux normes, aux SLA et aux obligations légales
- Évaluer l'efficacité des mesures de protection au moyen de tests d'intrusion et formaliser un plan de remédiation
- Mener une analyse forensic après incident pour identifier les vulnérabilités exploitées et mesurer l'impact
- Construire et alimenter des indicateurs de sécurité qui soutiennent les décisions de la direction

02 · FIL ROUGE PÉDAGOGIQUE

Groupe Vériane Assurances

IM

Inès Marchetti

Ingénieure SI. Elle devient cheffe de projet du programme Vériane Connect, puis responsable cybersécurité du groupe.

Assurance mutualiste (secteur tertiaire)

Le Groupe Vériane Assurances est une mutuelle d'assurance de 850 salariés répartis dans 14 agences régionales. Elle protège des particuliers et des professionnels. Son SI s'est construit par strates successives : un progiciel de gestion des contrats vieillissant, des applications métiers développées en interne et des services cloud adoptés sans gouvernance commune. La direction générale lance le programme « Vériane Connect », un espace client en ligne pour déclarer et suivre les sinistres. Le comité de direction exige un projet sûr, conforme au RGPD, accessible aux personnes en situation de handicap et sobre en ressources. Une tentative d'hameçonnage ciblant la comptabilité vient de rappeler la fragilité de l'existant. Inès Marchetti, ingénieure SI recrutée à la DSI, reçoit trois missions : bâtir la feuille de route SI, piloter le projet, puis structurer la fonction cybersécurité du groupe.

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. BC01 : Inès organise la veille de la DSI et cartographie le SI de Vériane. Elle présente au comité de direction une stratégie informatique et une architecture cible pour Vériane Connect.
2. BC02 : Inès rédige l'étude d'opportunité, les cahiers des charges et la note de cadrage. Elle pilote ensuite une équipe pluridisciplinaire composée de développeurs internes, d'un prestataire offshore et de représentants des agences.
3. BC03 : Inès supervise la conception et le développement de l'espace client. Elle impose des pratiques de développement sécurisé, des tests systématiques et une chaîne qualité automatisée.
4. BC04 : Inès est nommée responsable cybersécurité. Elle cartographie les risques, formalise la stratégie de sécurité du groupe et commande un test d'intrusion. Elle conduit aussi l'investigation d'une attaque par rançongiciel sur une agence, puis présente un tableau de bord sécurité à la direction.
5. BC05 : Inès accompagne la direction actuarielle dans un projet de détection de fraude aux sinistres fondé sur les données massives et en sécurise les traitements.
6. BC06 : Inès intègre la sécurité dans la chaîne DevOps de Vériane Connect (approche DevSecOps), de l'intégration continue jusqu'à l'observabilité en production.

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
RNCP40573BC01 · Définir une stratégie de systèmes d'information.		**88 h**
1	Concevoir et structurer une veille technologique et réglementaire	22 h
2	Synthétiser la veille et recommander des solutions innovantes	22 h
3	Cartographier le SI et élaborer la stratégie informatique	22 h
4	Comparer, analyser et recommander des architectures SI	22 h
RNCP40573BC02 · Piloter des projets informatiques.		**88 h**
5	Étude d'opportunité et priorisation des fonctionnalités	22 h
6	Rédiger le cahier des charges technique : RGPD, accessibilité et processus métier	22 h
7	Cadrer et planifier le projet informatique	22 h
8	Maîtriser les risques projet et fédérer les parties prenantes	22 h
RNCP40573BC03 · Concevoir et développer une application informatique.		**88 h**
9	Concevoir l'architecture applicative et schématiser les processus métier	22 h
10	Recommander un environnement technique écoresponsable et justifier les design patterns	22 h
11	Développer une application métier sécurisée	22 h
12	Tester l'application et automatiser le suivi de la qualité	22 h
RNCP40573BC04 · (Option) Manager la cybersécurité des systèmes, applications et bases de données		**132 h**
13	Cartographier les risques de sécurité du SI	22 h
14	Élaborer la stratégie de cybersécurité : normes, SLA et souveraineté	22 h
15	Intégrer RGPD, accessibilité et obligations légales en cas de cyberattaque	22 h
16	Évaluer les protections par des tests d'intrusion	22 h
17	Conduire une analyse forensic après une attaque	22 h
18	Piloter la cybersécurité par les indicateurs	22 h
RNCP40573BC05 · (Option) Construire et implémenter des modèles de big data et d'IA		**22 h**
19	Big data et IA : concevoir, exploiter et sécuriser les traitements de données	22 h
RNCP40573BC06 · (Option) Concevoir et déployer des infrastructures DevOps automatisées		**22 h**

20	DevSecOps : stratégie, pipelines CI/CD, conteneurs et observabilité	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

RNCP40573BC01 · 88 h

Définir une stratégie de systèmes d'information.

Cours 1 · Concevoir et structurer une veille technologique et réglementaire

22 h

OBJECTIFS

- Structurer un dispositif de veille ciblant les technologies sobres et sécurisantes ainsi que les évolutions réglementaires
- Évaluer la fiabilité des sources d'information selon des critères normés

ÉVALUATION FORMATIVE

QCM de fin de cours et production d'un plan de veille commenté, avec grille d'évaluation des sources

CONTENUS

- Enjeux de la veille : évolutions du marché, obsolescence du SI, numérique responsable
- Typologie des sources : institutionnelles, normatives, éditeurs, communautés, publications scientifiques
- Grilles d'évaluation de la fiabilité et de la pertinence d'une source
- Veille réglementaire : RGPD, cadre européen de cybersécurité, accessibilité numérique, green IT
- Outillage et automatisation de la collecte : agrégateurs, alertes, flux
- Organisation du processus de veille : rôles, fréquence, circuits de diffusion
- Étude de cas : bâtir le plan de veille d'une DSI du secteur tertiaire

Fil rouge · Le DSI de Vériane demande à Inès de mettre en place une veille structurée sur l'obsolescence du progiciel de gestion des contrats et sur les nouvelles obligations de sécurité du secteur assurantiel.

Cours 2 · Synthétiser la veille et recommander des solutions innovantes

22 h

OBJECTIFS

- Produire une synthèse de veille qui qualifie fiabilité, impact environnemental, gains et risques
- Formuler des recommandations innovantes adaptées aux enjeux de l'entreprise et à la réglementation

ÉVALUATION FORMATIVE

Rédaction d'une note de synthèse de veille et simulation de présentation évaluée par grille critériée

CONTENUS

- Méthodes de synthèse : matrices gains et risques, analyse multicritère
- Évaluation de l'impact environnemental d'une technologie (cycle de vie, consommation, durabilité)
- Formats de restitution adaptés aux publics : DSI, équipes techniques, clients, direction
- Construction d'un argumentaire de recommandation aligné sur la stratégie d'entreprise
- Intégration des contraintes réglementaires dans la recommandation
- Présentation orale des préconisations et gestion des objections
- Étude de cas : arbitrer entre deux solutions de modernisation du SI

Fil rouge · Inès présente au comité de direction de Vériane une note de synthèse comparant la refonte du progiciel de gestion des contrats et sa migration vers une solution hébergée. Elle y intègre l'impact environnemental et les exigences du RGPD.

Cours 3 · Cartographier le SI et élaborer la stratégie informatique

22 h

OBJECTIFS

- Schématiser une cartographie du SI en s'appuyant sur une méthode d'analyse de risques
- Élaborer une stratégie informatique et des axes d'évolution à partir de la cartographie validée

ÉVALUATION FORMATIVE

Exercice de cartographie guidé et livrable intermédiaire du dossier stratégique (veille et diagnostic critique)

CONTENUS

- Niveaux de cartographie : métier, fonctionnel, applicatif, infrastructure
- Méthodes et formalismes de modélisation du SI
- Intégration de l'analyse de risques dans la cartographie
- Diagnostic critique de l'existant : dette technique, obsolescence, dépendances
- Construction d'un schéma directeur et d'une feuille de route SI
- Alignement stratégique entre SI et objectifs métier
- Présentation des préconisations et des spécifications associées aux parties prenantes
- Étude de cas : du diagnostic au schéma directeur

Fil rouge · Inès réalise la cartographie complète du SI de Vériane et repère les applications critiques exposées. Elle en tire une feuille de route sur trois ans qu'elle soumet à la validation du DSI.

Cours 4 · Comparer, analyser et recommander des architectures SI

22 h

OBJECTIFS

- Comparer les types d'architectures et schématiser leurs interactions
- Recommander une architecture cible selon la performance, la scalabilité, la sécurité et l'éco-conception

ÉVALUATION FORMATIVE

QCM et production d'un dossier d'architecture SI argumenté, préparant l'épreuve du bloc

CONTENUS

- Panorama des architectures : monolithique, n-tiers, orientée services, microservices, événementielle, cloud et hybride
- Analyse des composants : fonctions, interactions et dépendances
- Évaluation de la performance et de la scalabilité
- Sécurité by design et principes de défense en profondeur dans l'architecture
- Éco-conception des architectures et sobriété des ressources
- Formalisation d'un dossier d'architecture SI
- Étude de cas : choisir l'architecture d'un espace client en ligne

Fil rouge · Pour Vériane Connect, Inès compare une architecture en microservices et une architecture n-tiers modernisée. Elle justifie son choix auprès du DSI au regard de la sécurité et de la consommation des ressources.

RNCP40573BC02 · 88 h

Piloter des projets informatiques.

Cours 5 · Étude d'opportunité et priorisation des fonctionnalités

22 h

OBJECTIFS

- Analyser la problématique d'un client dans un contexte de transformation digitale et formaliser une étude d'opportunité
- Évaluer et prioriser les fonctionnalités selon leur importance et leur impact

ÉVALUATION FORMATIVE

Étude de cas notée : rédaction d'une étude d'opportunité et d'une matrice de priorisation

CONTENUS

- Diagnostic de transformation digitale : défis actuels, enjeux, maturité numérique
- Recueil des besoins : entretiens, ateliers, observation des usages
- Structure d'une étude d'opportunité : contexte, scénarios, coûts, bénéfices, risques
- Méthodes de priorisation : MoSCoW, matrice valeur et effort, notation pondérée
- Rédaction du cahier des charges fonctionnel
- Étude de cas : formaliser l'opportunité d'un portail de déclaration de sinistres

Fil rouge · Inès anime des ateliers avec les gestionnaires de sinistres et les conseillers en agence. Elle rédige ensuite l'étude d'opportunité de Vériane Connect et classe les fonctionnalités par priorité.

Cours 6 · Rédiger le cahier des charges technique : RGPD, accessibilité et processus métier

22 h

OBJECTIFS

- Construire un cahier des charges technique conforme au RGPD et intégrant l'accessibilité aux PSH
- Décrire et prioriser chaque fonctionnalité au moyen d'une méthode de modélisation des processus métier

ÉVALUATION FORMATIVE

Exercice de modélisation BPMN et livrable du cahier des charges technique évalué par grille

CONTENUS

- Du cahier des charges fonctionnel au cahier des charges technique : coordination des processus clés
- Protection des données dès la conception : minimisation, durées de conservation, analyse d'impact
- Accessibilité numérique : référentiel national, critères et intégration dans les spécifications
- Modélisation des processus métier (BPMN) et priorisation des fonctionnalités
- Prise en compte des contraintes et de l'existant technique
- Rédaction des exigences non fonctionnelles : sécurité, performance, sobriété
- Étude de cas : spécifier le parcours de déclaration de sinistre

Fil rouge · Inès modélise en BPMN le processus de déclaration de sinistre. Elle rédige le cahier des charges technique de Vériane Connect avec le délégué à la protection des données et une association représentant des assurés en situation de handicap.

Cours 7 · Cadrer et planifier le projet informatique

22 h

OBJECTIFS

- Rédiger une note de cadrage précisant démarche, objectifs, délais, budget, ressources et exigences de qualité
- Planifier le projet et coordonner les méthodes de gestion de projet adaptées au contexte

ÉVALUATION FORMATIVE

Rédaction d'une note de cadrage et d'un planning détaillé, intégrés au dossier de planification du bloc

CONTENUS

- Structure et contenu d'une note de cadrage
- Méthodologies de conduite de projet : prédictive, agile, hybride, et critères de choix
- Décomposition du projet : organigramme des tâches, jalons, livrables
- Allocation des ressources internes et externes et construction du budget
- Outils de planification et de suivi : diagramme de Gantt, backlog, tableaux de bord
- Travail en réseau et coordination d'équipes distribuées
- Étude de cas : planifier un projet mêlant équipes internes et prestataires

Fil rouge · Inès rédige la note de cadrage de Vériane Connect et retient une démarche hybride. Elle planifie les itérations entre l'équipe interne et le prestataire de développement offshore.

Cours 8 · Maîtriser les risques projet et fédérer les parties prenantes

22 h

OBJECTIFS

- Identifier, évaluer et traiter les risques et menaces pesant sur la sécurité du projet
- Coordonner la communication, gérer l'engagement des parties prenantes et organiser la capitalisation des compétences

ÉVALUATION FORMATIVE

Mise en situation de comité de pilotage et production d'un registre des risques assorti d'un plan de communication

CONTENUS

- Registre des risques projet : identification, cotation, plans de mitigation
- Sécurité du projet : menaces liées aux sous-traitants, aux accès et aux données de test
- Cartographie des parties prenantes et plan de communication
- Communication interculturelle et pluridisciplinaire
- Gestion de l'engagement : DSI, MOA, clients, consultants, sous-traitants
- Valorisation des réussites individuelles et maintien de la motivation
- Capitalisation et partage du savoir-faire de manière inclusive : bases de connaissances, binômes, retours d'expérience
- Étude de cas : redresser un projet en dérive

Fil rouge · À mi-projet, le prestataire offshore accumule du retard et des tensions apparaissent avec les agences. Inès réactualise le registre des risques, organise un comité de pilotage et met en place un dispositif de partage des connaissances.

RNCP40573BC03 · 88 h

Concevoir et développer une application informatique.

Cours 9 · Concevoir l'architecture applicative et schématiser les processus métier

22 h

OBJECTIFS

- Concevoir une architecture applicative adaptée au SI existant et aux exigences de sécurité
- Produire des maquettes et des schémas de processus intégrant contraintes et vulnérabilités

ÉVALUATION FORMATIVE

Exercice de modélisation UML et livrable de maquettes, intégrés au dossier de conception

CONTENUS

- Analyse des besoins fonctionnels et des exigences de sécurité
- Architecture applicative : couches, services, interfaces et intégration au SI existant
- Modélisation UML : cas d'utilisation, séquences, classes
- Schématisation des processus métier et identification des vulnérabilités
- Maquettage et prototypage pour la validation par le commanditaire
- Accessibilité et ergonomie dans les maquettes
- Étude de cas : du besoin validé au dossier de conception

Fil rouge · Inès fait valider par la direction des sinistres les maquettes de l'espace client. Elle repère dans les schémas de processus les points d'exposition des données personnelles.

Cours 10 · Recommander un environnement technique écoresponsable et justifier les design patterns

22 h

OBJECTIFS

- Recommander un environnement informatique cohérent à partir de critères comparatifs, dont l'impact écologique
- Justifier le choix de patterns logiciels et de classes pour une architecture modulaire et maintenable

ÉVALUATION FORMATIVE

QCM et rédaction d'une note de choix techniques argumentée

CONTENUS

- Interactions entre composants d'infrastructure et composants applicatifs
- Grilles comparatives de langages, frameworks, bases de données et hébergements
- Techniques d'éco-conception logicielle et de réduction de l'empreinte
- Patterns d'architecture : MVC, hexagonal, microservices
- Patterns de conception orientée objet : création, structure, comportement
- Principes de modularité, de réutilisabilité et de maintenabilité
- Étude de cas : argumenter des choix techniques devant un comité d'architecture

Fil rouge · Le prestataire propose une pile technique que Inès juge surdimensionnée. Elle construit une grille comparative intégrant la sobriété et justifie les patterns retenus pour le module de suivi des sinistres.

Cours 11 · Développer une application métier sécurisée

22 h

OBJECTIFS

- Appliquer des pratiques de développement sécurisé pour protéger les données et les systèmes
- Améliorer la visibilité et l'efficacité des développeurs par des conventions et outils partagés

ÉVALUATION FORMATIVE

Travaux pratiques notés de correction de vulnérabilités et QCM

CONTENUS

- Principales vulnérabilités applicatives (référentiel OWASP) et contre-mesures
- Authentification, gestion des sessions et contrôle d'accès
- Validation des entrées, chiffrement et gestion des secrets
- Sécurisation des API et des échanges
- Revue de code, conventions et gestion de versions
- Analyse statique du code et gestion des dépendances vulnérables
- Travaux pratiques : corriger les failles d'une application métier

Fil rouge · Une revue de code menée par Inès révèle une injection possible dans le formulaire de déclaration de sinistre. Elle fait corriger la faille et instaure une charte de développement sécurisé pour toutes les équipes.

Cours 12 · Tester l'application et automatiser le suivi de la qualité

22 h

OBJECTIFS

- Rédiger et exécuter des scénarios de tests selon des procédures définies
- Concevoir un cycle automatisé de suivi de la qualité et de l'exécution de l'application

ÉVALUATION FORMATIVE

Rédaction d'un plan de tests et exécution de scénarios sur une application fournie, intégrées au dossier technique

CONTENUS

- Stratégie de tests : unitaires, intégration, fonctionnels, non-régression, performance, sécurité
- Rédaction de scénarios et de cahiers de recette
- Tests d'accessibilité
- Gestion des anomalies et cycle de correction
- Intégration continue et automatisation des tests
- Indicateurs qualité : couverture, dette technique, stabilité, performance
- Étude de cas : préparer la mise en production et livrer le dossier technique

Fil rouge · Avant l'ouverture de Vériane Connect aux assurés, Inès pilote la recette avec les agences pilotes. Elle met en place un tableau de bord qualité alimenté automatiquement à chaque livraison.

(Option) Manager la cybersécurité des systèmes, applications et bases de données

Cours 13 · Cartographier les risques de sécurité du SI

22 h

OBJECTIFS

- Cartographier les risques affectant la confidentialité, l'intégrité et la disponibilité des actifs
- Mettre en évidence vulnérabilités et scénarios de risques en réponse à une demande interne ou externe

ÉVALUATION FORMATIVE

Atelier d'analyse de risques guidé et livrable de cartographie, intégré au dossier technique du bloc

CONTENUS

- Fondamentaux de la sécurité de l'information : actifs, menaces, vulnérabilités, impacts
- Critères de confidentialité, d'intégrité et de disponibilité et classification des actifs
- Méthodes d'analyse de risques : EBIOS Risk Manager, ISO/IEC 27005
- Cartographie de l'infrastructure, des applications et des bases de données
- Scénarios stratégiques et opérationnels, référentiel MITRE ATT&CK
- Cotation des risques et matrice de criticité
- Étude de cas : analyse de risques d'un SI assurantiel

Fil rouge · Nommée responsable cybersécurité après la tentative d'hameçonnage, Inès conduit une analyse de risques sur le SI de Vériane. Elle identifie la base des contrats et l'annuaire comme actifs les plus critiques.

Cours 14 · Élaborer la stratégie de cybersécurité : normes, SLA et souveraineté

22 h

OBJECTIFS

- Élaborer une stratégie de cybersécurité conforme aux normes et aux accords de niveaux de service
- Intégrer les enjeux de souveraineté numérique dans les choix de sécurisation

ÉVALUATION FORMATIVE

Rédaction d'un extrait de politique de sécurité et QCM sur les normes

CONTENUS

- Gouvernance de la sécurité : rôles, comitologie, système de management ISO/IEC 27001
- Politique de sécurité du SI et plan de traitement des risques
- Mesures de sécurité de référence : ISO/IEC 27002 et guides d'hygiène informatique
- Accords de niveaux de service, exigences de sécurité contractuelles et gestion des tiers
- Continuité et reprise d'activité
- Souveraineté numérique : hébergement, dépendances, qualifications de prestataires
- Feuille de route sécurité et budget associé

Fil rouge · Inès rédige la politique de sécurité du groupe Vériane. Elle renégocie les clauses de sécurité et de disponibilité avec l'hébergeur de Vériane Connect.

Cours 15 · Intégrer RGPD, accessibilité et obligations légales en cas de cyberattaque

22 h

OBJECTIFS

- Intégrer les exigences du RGPD et les critères d'accessibilité PSH dans la stratégie de cybersécurité
- Organiser le respect des obligations légales en cas de cyberattaque

ÉVALUATION FORMATIVE

Exercice de crise sur table évalué et QCM réglementaire

CONTENUS

- RGPD et sécurité des traitements : mesures techniques et organisationnelles
- Notification des violations de données à l'autorité de contrôle et information des personnes
- Obligations des entités régulées dans le cadre européen de cybersécurité (directive NIS 2)
- Dépôt de plainte, conservation des preuves et relations avec les autorités
- Accessibilité des dispositifs de sécurité : authentification, sensibilisation, interfaces
- Plan de gestion de crise cyber et communication de crise
- Étude de cas : exercice de crise sur table

Fil rouge · Inès vérifie que le nouveau dispositif d'authentification renforcée reste utilisable par les assurés malvoyants. Elle organise ensuite un exercice de crise simulant une fuite de données clients.

Cours 16 · Évaluer les protections par des tests d'intrusion

22 h

OBJECTIFS

- Planifier et conduire des tests d'intrusion pour évaluer l'efficacité des mesures de protection
- Restituer les vulnérabilités identifiées et prioriser la remédiation

ÉVALUATION FORMATIVE

Simulation de hacking en environnement de laboratoire et rédaction d'un rapport de test d'intrusion

CONTENUS

- Cadre d'un pentest : périmètre, convention, aspects légaux et éthiques
- Approches boîte noire, grise et blanche
- Méthodologie : reconnaissance, énumération, exploitation, post-exploitation
- Tests sur infrastructures, applications web et bases de données
- Ingénierie sociale et tests de sensibilisation
- Rédaction du rapport de pentest et plan de remédiation
- Travaux pratiques en laboratoire isolé : simulation de hacking

Fil rouge · Inès cadre un test d'intrusion sur Vériane Connect et en réalise une partie en laboratoire. Elle présente au DSI les vulnérabilités découvertes et le plan de correction priorisé.

Cours 17 · Conduire une analyse forensic après une attaque

22 h

OBJECTIFS

- Structurer et mener une investigation forensic après une intrusion
- Identifier les vulnérabilités exploitées et déterminer l'impact de l'incident

ÉVALUATION FORMATIVE

Étude de cas forensic sur jeu de preuves fourni et rédaction d'un rapport d'investigation

CONTENUS

- Cycle de réponse à incident : détection, confinement, éradication, restauration
- Préservation des preuves et chaîne de traçabilité
- Acquisition et analyse de mémoire, de disques et de journaux
- Reconstitution de la chronologie de l'attaque
- Analyse des indicateurs de compromission
- Évaluation de l'impact sur les actifs et les données
- Rapport d'investigation et retour d'expérience

Fil rouge · Un rançongiciel chiffre les postes d'une agence Vériane. Inès dirige l'investigation : elle reconstitue l'accès initial par un compte de prestataire compromis et mesure l'étendue des données touchées.

Cours 18 · Piloter la cybersécurité par les indicateurs

22 h

OBJECTIFS

- Identifier et alimenter des indicateurs d'activité pertinents pour la décision
- Produire des analyses et des rapports réguliers sur les performances et les tendances

ÉVALUATION FORMATIVE

Conception d'un tableau de bord sécurité et soutenance blanche du dossier technique du bloc

CONTENUS

- Indicateurs opérationnels, de conformité et stratégiques
- Sources de données : journaux, supervision de sécurité, outils de gestion des vulnérabilités
- Construction de tableaux de bord adaptés à chaque public
- Analyse de tendances et détection de signaux faibles
- Reporting à la direction et aux instances de gouvernance
- Amélioration continue du dispositif de sécurité
- Étude de cas : soutenance du dossier technique du bloc

Fil rouge · Un an après sa nomination, Inès présente au comité de direction un tableau de bord sécurité. Elle s'en sert pour obtenir les moyens de la phase suivante de sa feuille de route.

RNCP40573BC05 · 22 h

(Option) Construire et implémenter des modèles de big data et d'IA

Cours 19 · Big data et IA : concevoir, exploiter et sécuriser les traitements de données

22 h

OBJECTIFS

- Analyser une problématique de big data et concevoir une stratégie d'analyse et une base adaptée aux traitements d'IA
- Évaluer des modèles d'apprentissage automatique et schématiser un programme d'IA respectant le RGPD

ÉVALUATION FORMATIVE

Étude de cas guidée avec livrable de conception d'un traitement de données et QCM

CONTENUS

- Caractérisation d'une problématique big data : volume, vélocité, variété
- Stratégie d'analyse et architecture de traitement des données
- Chaînes d'extraction, de transformation et de chargement, et contrôle de la qualité des données
- Conception de bases de données pour les traitements analytiques et l'IA
- Modèles statistiques, apprentissage automatique et apprentissage profond : principes et évaluation
- Schématisation et conception d'un programme d'IA
- Protection des données, éthique et sécurité des modèles
- Étude de cas : détection de fraude et retour d'expérience

Fil rouge · La direction actuarielle de Vériane veut détecter les déclarations de sinistres frauduleuses. Inès participe à la conception de la chaîne de données et du modèle, et veille à la pseudonymisation des données.

RNCP40573BC06 · 22 h

(Option) Concevoir et déployer des infrastructures DevOps automatisées

Cours 20 · DevSecOps : stratégie, pipelines CI/CD, conteneurs et observabilité

22 h

OBJECTIFS

- Élaborer une stratégie DevOps alignée sur les objectifs business et l'éco-responsabilité
- Concevoir des pipelines CI/CD sécurisés, orchestrer des conteneurs et déployer une stratégie d'observabilité

ÉVALUATION FORMATIVE

Travaux pratiques sur un pipeline fourni et QCM

CONTENUS

- Diagnostic de l'infrastructure et des processus de développement existants
- Stratégie DevOps : culture, organisation, indicateurs et éco-responsabilité
- Pipelines CI/CD et pratiques GitOps
- Intégration de la sécurité dans le pipeline : analyse de code, des dépendances et des images
- Conteneurisation et orchestration : portabilité, scalabilité, résilience
- Optimisation de la consommation des ressources
- Monitoring et observabilité : métriques, journaux, traces, alertes
- Étude de cas : projet DevOps et retour d'expérience

Fil rouge · Inès intègre des contrôles de sécurité automatisés dans la chaîne de déploiement de Vériane Connect. Elle met en place une supervision qui alerte l'équipe avant toute dégradation du service.

05 · CONFORMITÉ AU RÉFÉRENTIEL

Couverture des compétences

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

Compétence	Bloc	Cours
Concevoir et structurer une veille technologique et réglementaire	RNCP40573BC01	1
Synthétiser les données de veille (fiabilité, impact environnemental, gains, risques)	RNCP40573BC01	1, 2
Recommander des solutions innovantes issues de la veille	RNCP40573BC01	2
Schématiser une cartographie du SI avec une méthode d'analyse de risques	RNCP40573BC01	3
Élaborer la stratégie informatique à partir de la cartographie	RNCP40573BC01	3
Présenter les préconisations du projet SI aux parties prenantes	RNCP40573BC01	2, 3
Comparer les types d'architectures et schématiser leurs interactions	RNCP40573BC01	4
Analyser les composants des architectures (fonctions, dépendances, performance)	RNCP40573BC01	4
Recommander l'architecture adaptée (performance, scalabilité, sécurité, éco-conception)	RNCP40573BC01	4
Analyser la problématique client et formaliser une étude d'opportunité	RNCP40573BC02	5
Évaluer et prioriser les fonctionnalités requises	RNCP40573BC02	5, 6
Construire un cahier des charges technique conforme au RGPD et accessible aux PSH	RNCP40573BC02	6
Décrire les fonctionnalités par une méthode de modélisation des processus métier	RNCP40573BC02	6
Rédiger une note de cadrage	RNCP40573BC02	7
Planifier le projet et allouer les ressources	RNCP40573BC02	7
Coordonner les méthodes de gestion de projet et de travail en réseau	RNCP40573BC02	7, 8
Développer des stratégies de mitigation des risques projet	RNCP40573BC02	8
Coordonner la communication entre parties prenantes pluridisciplinaires et multiculturelles	RNCP40573BC02	8
Gérer l'engagement des parties prenantes	RNCP40573BC02	7, 8
Organiser la capitalisation et le partage inclusif des compétences	RNCP40573BC02	8
Concevoir une architecture applicative et produire des maquettes	RNCP40573BC03	9
Schématiser les processus métier (contraintes, existant, vulnérabilités)	RNCP40573BC03	9
Recommander un environnement informatique réduisant l'impact écologique	RNCP40573BC03	10
Justifier l'utilisation de patterns logiciels et de classes	RNCP40573BC03	10
Développer des applications métiers sécurisées	RNCP40573BC03	11

Rédiger et exécuter les scénarios de tests	RNCP40573BC03	12
Concevoir un suivi qualité par un cycle automatisé	RNCP40573BC03	11, 12
Cartographier les risques de sécurité du SI (confidentialité, intégrité, disponibilité)	RNCP40573BC04	13
Élaborer une stratégie de cybersécurité (normes, SLA, PSH, RGPD, obligations légales, souveraineté)	RNCP40573BC04	14, 15
Évaluer les mesures de protection par des tests d'intrusion	RNCP40573BC04	16
Mener une analyse forensic après une intrusion ou une attaque	RNCP40573BC04	17
Identifier et alimenter des indicateurs d'activité pour la décision	RNCP40573BC04	18
Analyser une problématique big data (volume, vélocité, variété) et définir une stratégie d'analyse	RNCP40573BC05	19
Concevoir et évaluer des modèles statistiques et d'apprentissage automatique	RNCP40573BC05	19
Optimiser l'exploitation des données (ETL, qualité, RGPD)	RNCP40573BC05	19
Concevoir une base de données pour les traitements analytiques et d'IA	RNCP40573BC05	19
Schématiser et concevoir un programme d'IA	RNCP40573BC05	19
Analyser l'existant et élaborer une stratégie DevOps écoresponsable	RNCP40573BC06	20
Concevoir et implémenter des pipelines CI/CD et des pratiques GitOps	RNCP40573BC06	20
Orchestrer des environnements conteneurisés	RNCP40573BC06	20
Mettre en œuvre une stratégie de monitoring et d'observabilité	RNCP40573BC06	20

Évaluations formatives

Chaque cours intègre des évaluations formatives régulières. Des QCM de fin de sous-chapitre et de fin de cours vérifient l'acquisition des connaissances, avec une correction commentée. Des études de cas et des mises en situation ancrées dans le fil rouge Vériane mobilisent les compétences en contexte professionnel. Des travaux pratiques en environnement de laboratoire sont proposés pour le développement sécurisé, les tests d'intrusion, le forensic et le DevSecOps. Les livrables intermédiaires (plan de veille, cartographie, note de cadrage, cahier des charges, rapport de pentest, rapport d'investigation, tableau de bord) sont évalués par des grilles critériées alignées sur le référentiel. L'apprenant peut ainsi mesurer sa progression, et l'OF peut tracer les acquis conformément aux exigences Qualiopi.

Modalités de certification

Bloc	Modalité d'évaluation
RNCP40573BC01	Mise en situation professionnelle reconstituée : réalisation d'un dossier stratégique comprenant une veille et un diagnostic critique, et élaboration d'un dossier d'architecture SI.
RNCP40573BC02	Mise en situation professionnelle reconstituée : rédaction d'un dossier technique et opérationnel comprenant un cahier des charges fonctionnel, un cahier des charges technique et une note de cadrage, et élaboration d'un dossier de planification d'un projet informatique.

RNCP40573BC03	Mise en situation professionnelle reconstituée : construction d'un dossier de conception d'une application informatique, et livraison d'une application optimisée accompagnée d'un dossier technique.
RNCP40573BC04	Mise en situation professionnelle reconstituée : analyse des risques d'un système d'information et de son infrastructure avec élaboration d'un dossier technique, et évaluation sous forme de simulation de hacking et de tests d'intrusion.
RNCP40573BC05	Mise en situation professionnelle reconstituée : livraison d'un programme d'analyse de données (big data) et production d'un dossier de retour d'expérience (REX).
RNCP40573BC06	Mise en situation professionnelle reconstituée : livraison d'un projet DevOps complet et élaboration d'un dossier de retour d'expérience (REX).

Le parcours est construit pour que chaque livrable produit dans le fil rouge corresponde à une pièce attendue aux épreuves. Les cours 1 à 4 préparent le dossier stratégique et le dossier d'architecture. Les cours 5 à 8 préparent les cahiers des charges, la note de cadrage et le dossier de planification. Les cours 9 à 12 préparent le dossier de conception et le dossier technique de l'application. Les cours 13 à 18 préparent l'analyse de risques, le dossier technique de sécurité et la simulation de hacking, grâce à des travaux pratiques en laboratoire et à une soutenance blanche. Les cours 19 et 20 apportent une culture des blocs optionnels big data et IA ainsi que DevOps, indispensable au manager cybersécurité. La présentation aux épreuves des blocs BC05 et BC06, ainsi que l'organisation des sessions d'évaluation, relèvent des règles fixées par le certificateur et de la responsabilité de l'organisme de formation. SFM fournit le contenu pédagogique, et l'OF reste responsable de la certification.

06 · MOYENS ET PERSPECTIVES

Moyens pédagogiques et débouchés

Moyens pédagogiques et techniques

- Plateforme e-learning en marque blanche accessible 24 h sur 24, avec suivi de la progression et traçabilité des activités pour l'OF
- Une vidéo de 3 à 5 minutes par sous-chapitre, les vidéos représentant 30 % du volume horaire du parcours
- Cours texte enrichi, infographies, fiches de synthèse téléchargeables et modèles de livrables (note de cadrage, cahier des charges, rapport de pentest, rapport d'investigation)
- Études de cas et mises en situation fondées sur le fil rouge du Groupe Vériane Assurances
- Environnements de travaux pratiques isolés pour le développement sécurisé, les tests d'intrusion, l'analyse forensic et les pipelines DevSecOps
- QCM auto-corrigés avec feedback commenté, et grilles d'évaluation critériées alignées sur le référentiel
- Guide de mise en œuvre destiné à l'OF : matrice de couverture, préconisations d'accompagnement tutoré et de préparation aux épreuves

Débouchés et évolutions

- Expert en sécurité informatique
- Consultant en cybersécurité
- Ingénieur informatique / systèmes d'information (SI)
- Responsable de projet IT
- Ingénieur études et développement, ingénieur logiciel
- Consultant informatique (IT)

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 RNCP40573 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.