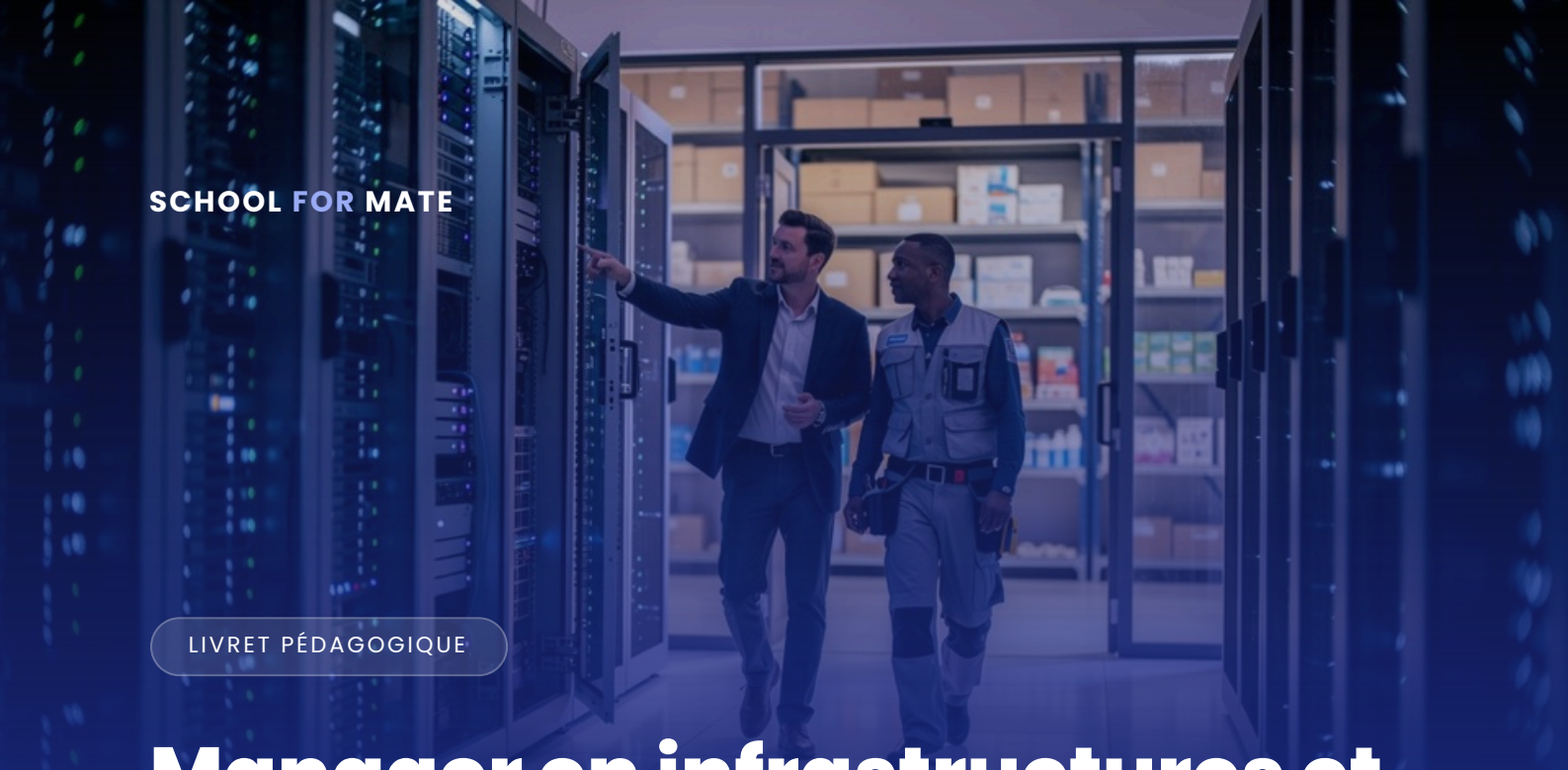


SCHOOL FOR MATE

LIVRET PÉDAGOGIQUE

Manager en infrastructures et cybersécurité des systèmes d'information

RNCP38779 · Certification RNCP · Niveau 7

Ce parcours de 440 heures prépare au titre RNCP38779 de niveau 7 « Manager en infrastructures et cybersécurité des systèmes d'information » en couvrant l'intégralité de ses quatre blocs de compétences : management des équipes et de la transformation du SI, supervision du portefeuille projets, conception d'infrastructures et sécurisation des accès, réseaux et données. Il suit pas à pas une responsable infrastructures et sécurité au sein d'une entreprise fictive, afin que chaque notion soit immédiatement mise en pratique dans un contexte professionnel réaliste.

VOLUME HORAIRE	COURS	BLOCS
440 h	20	4

01 · PRÉSENTATION

La formation en bref

Intitulé	Manager en infrastructures et cybersécurité des systèmes d'information
Code	RNCP38779
Type	Certification RNCP
Niveau	Niveau 7
Certificateur	CESI
Durée	440 h, 20 cours
Modalité	Formation à distance (e-learning), tutorat assuré par l'organisme de formation
Formats	SCORM 1.2 / 2004, xAPI, sources éditables
Mise à jour	Novembre 2026
Fin d'enregistrement de la certification	27/03/2029

Le métier et les compétences visées

Le Manager en infrastructures et cybersécurité des systèmes d'information conçoit et met en œuvre des architectures réseaux sécurisées dans le respect des normes et règlements en vigueur. Il pilote des projets de migration ou de sécurisation du SI et évalue, à l'aide de méthodes et d'outils d'audit, les vulnérabilités et le niveau de résilience de l'infrastructure. Il encadre une équipe, hiérarchiquement ou fonctionnellement, et conduit le changement au sein de son organisation. Il supervise le portefeuille projets de la DSI, conseille la direction sur les investissements technologiques et de cybersécurité au moyen de tableaux de bord, et prépare l'organisation à anticiper, gérer et surmonter une crise cyber. Il exerce dans tous les secteurs, notamment en ESN.

Public visé

- Administrateurs systèmes et réseaux souhaitant évoluer vers des fonctions d'encadrement et d'architecture
- Techniciens supérieurs et développeurs titulaires d'un niveau 5 ou 6 en informatique visant un poste de niveau 7
- Chefs de projet infrastructures ou SI souhaitant renforcer leurs compétences en cybersécurité
- Consultants en ESN intervenant sur des missions d'infrastructure, de migration ou de sécurisation
- Professionnels en reconversion ou en évolution interne relevant du dispositif dérogatoire, après étude de leur dossier

Prérequis

- Être titulaire d'un niveau 5 en informatique (cycle de préparation en 36 mois)
- Ou être titulaire d'un niveau 6 en informatique (cycle de préparation en 24 mois)
- Ou être titulaire d'un niveau 6 en informatique avec 3 ans d'expérience professionnelle en informatique (cycle de préparation en 12 mois) ; tout autre profil relève du dérogatoire
- Sélection par l'organisme de formation : dossier de candidature avec CV et lettre de motivation, tests de positionnement et entretien individuel

Objectifs pédagogiques

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

- Encadrer et piloter une équipe IT, en responsabilité hiérarchique comme fonctionnelle, en adaptant son style de management et en s'appuyant sur des outils collaboratifs accessibles
- Analyser et modéliser le système d'information existant pour proposer aux décideurs des améliorations alignées sur la stratégie de l'entreprise
- Conduire le changement induit par la stratégie de la DSI à travers un plan d'accompagnement structuré (formation, communication, régulation, mesure)
- Prioriser, ordonnancer et défendre le portefeuille projets de la DSI à partir de critères de cotation explicites
- Planifier, piloter, recetter et clôturer des projets IT dans le respect du triangle qualité, coût, délai et des obligations réglementaires
- Auditer une infrastructure et concevoir une architecture sécurisée (réseaux, cloud, ERP, data, sauvegarde) conforme aux préconisations de l'ANSSI
- Réaliser un audit de sécurité avec outils de pentesting et bâtir un plan de sécurisation et de supervision conforme au RGPD, à l'ISO 27001 et à la directive NIS 2
- Superviser l'efficacité des mesures de sécurité via des indicateurs et un SIEM, et organiser une veille active sur les technologies et les menaces
- Conseiller la direction sur les investissements SI et cybersécurité au moyen de tableaux de bord formalisés
- Anticiper, détecter et gérer une crise cyber, puis évaluer les dommages pour renforcer durablement la résilience du SI

02 · FIL ROUGE PÉDAGOGIQUE

Groupe Altiméa

CR

Camille Rouvière

Responsable infrastructures et sécurité du SI, rattachée au DSI

Distribution de matériel médical et paramédical (ETI multisite)

Le Groupe Altiméa distribue du matériel médical auprès d'hôpitaux, de cliniques et de pharmacies. Il compte environ 1 200 salariés répartis entre un siège lyonnais, deux plateformes logistiques et une douzaine d'agences régionales. Après plusieurs rachats, son SI s'est construit par couches successives : un ERP vieillissant, des serveurs hébergés sur site, des accès distants hétérogènes et une sauvegarde peu testée. La direction générale engage un plan de transformation sur trois ans et souhaite moderniser l'infrastructure, rationaliser les projets et élever le niveau de cybersécurité, d'autant que ses clients hospitaliers durcissent leurs exigences. Camille Rouvière, ancienne ingénieure systèmes, vient d'être promue pour porter ce chantier. Elle prend la tête d'une équipe de huit personnes et travaille avec une ESN prestataire, Orvéa Conseil.

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

La progression

1. Bloc 1 : Camille prend ses fonctions, structure son équipe, cartographie le SI d'Altiméa et conduit l'adhésion des équipes métiers et techniques à la transformation.
2. Bloc 2 : Camille met en place un référentiel projets commun, arbitre le portefeuille de la DSI devant le comité de direction et pilote de bout en bout le projet de migration de l'ERP.
3. Bloc 3 : Camille audite l'infrastructure, compare les offres d'hébergement, conçoit la nouvelle architecture hybride sécurisée et présente à la direction la feuille de route d'évolution.
4. Bloc 4 : Camille fait réaliser un test d'intrusion, déploie un plan de sécurisation et un SIEM, prépare le plan de crise cyber puis le met à l'épreuve lors d'une attaque par rançongiciel sur une agence régionale.

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
RNCP38779BC01 · Manager les équipes et la transformation du SI		**88 h**
1	Encadrer et développer une équipe IT en responsabilité hiérarchique	22 h
2	Piloter des équipes projet et manager les relations clients et fournisseurs	22 h
3	Analyser, modéliser et optimiser le système d'information	22 h
4	Conduire le changement et accompagner la transformation portée par la DSI	22 h
RNCP38779BC02 · Superviser le portefeuille projets de la DSI et sa mise en œuvre		**110 h**
5	Élaborer le référentiel documentaire des projets IT	22 h
6	Prioriser, ordonnancer et défendre le portefeuille projets du SI	22 h
7	Cadrer et planifier un projet IT : du besoin au plan de management	22 h
8	Piloter l'exécution : livrables, tableaux de bord et recettes	22 h
9	Clôturer un projet IT et capitaliser l'expérience	22 h
RNCP38779BC03 · Concevoir l'infrastructure du système d'Information		**88 h**
10	Auditer l'infrastructure du SI au regard des standards et des préconisations ANSSI	22 h
11	Étudier et comparer les solutions technologiques d'infrastructure	22 h
12	Concevoir une infrastructure sécurisée et bâtir le portefeuille d'évolution	22 h
13	Veille technologique, indicateurs d'infrastructure et conseil à la direction	22 h
RNCP38779BC04 · Sécuriser les infrastructures du système d'Information (accès, réseaux et données)		**154 h**
14	Auditer la sécurité du SI : méthodologie et outils de pentesting	22 h
15	Cadre juridique et normatif de la sécurité des SI	22 h
16	Concevoir le plan de sécurisation et de supervision du SI	22 h
17	Piloter les projets de sécurisation en agile et superviser leur efficacité	22 h
18	Veille cyber, analyse des indicateurs et gouvernance de la sécurité	22 h
19	Anticiper la crise cyber : risques, continuité et organisation	22 h
20	Détecter, répondre à l'incident et renforcer la résilience du SI	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

RNCP38779BC01 · 88 h

Manager les équipes et la transformation du SI

Cours 1 · Encadrer et développer une équipe IT en responsabilité hiérarchique

22 h

OBJECTIFS

- Organiser la répartition des tâches en cohérence avec les compétences et les contraintes d'accessibilité de chaque collaborateur
- Construire un plan de développement des compétences de l'équipe au service de l'organisation du SI

ÉVALUATION FORMATIVE

QCM de fin de chapitre et étude de cas notée : réalisation d'une matrice de compétences et d'un plan d'affectation des tâches argumenté

CONTENUS

- Posture et responsabilités du manager hiérarchique en DSI
- Cartographie des compétences et matrice de polyvalence de l'équipe
- Affectation des tâches, charge de travail et accessibilité des postes (handicap, télétravail, astreintes)
- Entretiens annuels, professionnels et fixation d'objectifs
- Plan de développement des compétences et parcours de montée en expertise
- Organisation du support, de l'exploitation et des astreintes
- Prévention des risques psychosociaux et qualité de vie au travail dans les équipes IT

Fil rouge · Camille hérite d'une équipe de huit personnes aux profils hétérogènes, dont un administrateur en situation de handicap. Elle réalise la matrice de compétences de l'équipe, réorganise les astreintes et rédige le plan de développement des compétences de l'année.

Cours 2 · Piloter des équipes projet et manager les relations clients et fournisseurs

22 h

OBJECTIFS

- Adapter son style de management à une équipe projet transverse sans lien hiérarchique
- Choisir et paramétrer des outils collaboratifs et de communication adaptés et accessibles
- Piloter la relation avec les clients internes et les prestataires pour optimiser la mise en œuvre des projets IT

ÉVALUATION FORMATIVE

Mise en situation interactive de management (choix de réponses argumentés) et QCM

CONTENUS

- Management fonctionnel : influence, délégation et leadership situationnel
- Animation d'équipes distribuées et hybrides
- Outils collaboratifs : gestion de tâches, messagerie d'équipe, espaces documentaires, critères d'accessibilité
- Rituels d'équipe et gouvernance de la communication projet
- Relation maîtrise d'ouvrage et clients internes : recueil des attentes, engagements de service
- Pilotage des fournisseurs et ESN : comitologie, conventions de service, plans de progrès
- Gestion des tensions et des conflits en contexte projet

Fil rouge · Camille pilote une équipe projet mêlant ses administrateurs, deux référents métiers de la logistique et trois consultants d'Orvéa Conseil. Elle met en place les rituels, l'espace collaboratif commun et le comité de pilotage fournisseur après un premier retard de livraison.

Cours 3 · Analyser, modéliser et optimiser le système d'information

22 h

OBJECTIFS

- Analyser l'environnement technique et métier pour identifier processus, workflows et technologies en place
- Modéliser le SI sous une forme synthétique compréhensible par les décideurs
- Identifier des améliorations du SI répondant aux enjeux stratégiques de l'entreprise

ÉVALUATION FORMATIVE

Étude de cas notée : production d'une cartographie de processus et d'une note de synthèse décisionnelle, complétée d'un QCM

CONTENUS

- Méthodes de collecte : documentations techniques, rapports d'activité, audits existants, interviews
- Cartographie des processus métiers et des flux d'information
- Urbanisation du SI : vues métier, fonctionnelle, applicative et infrastructure
- Notations et outils de modélisation (BPMN, schémas d'architecture, principes d'ArchiMate)
- Synthèse décisionnelle : de la cartographie au support de présentation pour le comité de direction
- Identification des irritants, redondances et points de rupture des flux
- Alignement stratégique et feuille de route d'optimisation du SI

Fil rouge · Camille mène une série d'interviews dans les agences et les plateformes logistiques, cartographie le processus de commande hospitalière et présente au comité de direction une vue simplifiée du SI accompagnée de cinq pistes d'amélioration priorisées.

Cours 4 · Conduire le changement et accompagner la transformation portée par la DSI

22 h

OBJECTIFS

- Choisir une méthode de conduite du changement adaptée aux leviers de motivation et d'engagement des parties prenantes
- Définir et piloter un plan d'accompagnement complet (acteurs, formation, communication, régulation, mesure)

ÉVALUATION FORMATIVE

Exercice de construction d'un plan d'accompagnement avec grille d'autoévaluation et préparation à une soutenance orale simulée

CONTENUS

- Fondamentaux de la conduite du changement et principaux modèles
- Cartographie des parties prenantes et analyse des résistances
- Leviers de motivation et d'engagement des utilisateurs et des équipes IT
- Construction du plan d'accompagnement : acteurs, relais, calendrier
- Plan de formation et de communication accessibles à tous les publics
- Régulation, gestion des irritants et boucles de retour utilisateurs
- Indicateurs d'adoption et mesure de l'appropriation

Fil rouge · Le déploiement d'un nouvel outil de gestion des demandes suscite des résistances fortes dans les agences régionales. Camille identifie des ambassadeurs locaux, construit le plan d'accompagnement et suit les indicateurs d'adoption pendant trois mois.

RNCP38779BC02 · 110 h

Superviser le portefeuille projets de la DSI et sa mise en œuvre

Cours 5 · Élaborer le référentiel documentaire des projets IT

22 h

OBJECTIFS

- Concevoir un référentiel documentaire harmonisant la formalisation et la gestion des projets de la DSI
- Articuler le référentiel avec les pratiques de l'entreprise et les méthodologies existantes (cycle en V, agilité)

ÉVALUATION FORMATIVE

Production notée d'un extrait de référentiel documentaire (formulaire de demande et grille de faisabilité) et QCM

CONTENUS

- Cycle de vie d'un projet IT : de la réception de la demande à la clôture
- Méthodologies de référence : cycle en V, Scrum, Kanban, approches hybrides
- Formulaire de demande, fiche d'opportunité et analyse de faisabilité
- Modèles de livrables : note de cadrage, cahier des charges, backlog, dossier d'architecture
- Gouvernance documentaire : versionnage, droits d'accès, cycle de validation
- Diffusion et appropriation du référentiel par les acteurs projet

Fil rouge · Chaque service d'Altiméa formalise ses demandes à sa façon. Camille conçoit un référentiel commun (formulaire de demande, grille de faisabilité, modèles de livrables adaptés au cycle en V comme aux projets agiles) et l'expérimente sur deux projets pilotes.

Cours 6 · Prioriser, ordonnancer et défendre le portefeuille projets du SI

22 h

OBJECTIFS

- Définir des critères de choix pertinents intégrant les règles législatives, normatives, culturelles et éthiques
- Ordonnancer les projets proposés et présenter les cotations aux instances hiérarchiques et fonctionnelles

ÉVALUATION FORMATIVE

Étude de cas notée : cotation d'un portefeuille fictif et rédaction d'une note d'arbitrage argumentée

CONTENUS

- Principes de la gestion de portefeuille projets
- Construction d'une grille de cotation multicritère : valeur, risque, effort, conformité, alignement stratégique
- Prise en compte des contraintes réglementaires et éthiques dans la priorisation
- Ordonnancement, dépendances et capacité à faire de la DSI
- Feuille de route pluriannuelle et arbitrages budgétaires
- Préparation et animation d'un comité d'arbitrage
- Argumentation et défense des choix devant la direction

Fil rouge · Dix-sept demandes de projets remontent à la DSI pour l'exercice à venir. Camille construit la grille de cotation, ordonnance le portefeuille en tenant compte des obligations de conformité exigées par les clients hospitaliers, puis défend ses arbitrages en comité de direction.

Cours 7 · Cadrer et planifier un projet IT : du besoin au plan de management

22 h

OBJECTIFS

- S'approprier le contexte, le périmètre, les objectifs, les enjeux et les contraintes d'un projet IT
- Établir un plan de management de projet complet et le suivre à l'aide des outils de gestion de projet

ÉVALUATION FORMATIVE

Exercice noté de rédaction d'une note de cadrage et d'un registre des risques, avec QCM

CONTENUS

- Analyse du besoin de la maîtrise d'ouvrage et note de cadrage
- Périmètre, découpage en lots et structure de découpage du projet
- Planification : jalons, chemin critique, diagramme de Gantt, planification agile
- Budget prévisionnel et suivi des coûts
- Gestion des risques : identification, cotation, plan de traitement
- Organisation, rôles et matrice des responsabilités
- Indicateurs de suivi, parties prenantes et plan de communication

Fil rouge · Le projet de migration de l'ERP est arbitré en priorité. Camille rédige la note de cadrage avec la direction financière et logistique, puis établit le plan de management du projet (planning, budget, registre des risques, plan de communication).

Cours 8 · Piloter l'exécution : livrables, tableaux de bord et recettes

22 h

OBJECTIFS

- Contrôler et valider les livrables en garantissant le respect du triangle qualité, coût, délai
- Organiser les recettes fonctionnelles et techniques à partir de cahiers de recette structurés

ÉVALUATION FORMATIVE

Cas pratique noté : analyse d'un tableau de bord dégradé et rédaction d'un extrait de cahier de recette

CONTENUS

- Critères d'acceptation et contrôle qualité des livrables
- Tableaux de bord de suivi : avancement, consommation budgétaire, écarts de délai
- Gestion des changements de périmètre et arbitrages en cours de projet
- Stratégie de recette : recette fonctionnelle, technique, de non-régression et de performance
- Rédaction des cahiers et scénarios de recette
- Gestion des anomalies et qualification des correctifs
- Décision de mise en production et plan de bascule

Fil rouge · À mi-parcours, le lot interfaces logistiques de l'ERP accuse trois semaines de retard. Camille met à jour le tableau de bord, négocie un réajustement avec Orvéa Conseil, puis organise la recette fonctionnelle avec les utilisateurs clés des plateformes.

Cours 9 · Clôturer un projet IT et capitaliser l'expérience

22 h

OBJECTIFS

- Établir les documents administratifs, contractuels et techniques de clôture conformément aux règlements en vigueur
- Animer la capitalisation d'expérience à partir des indicateurs de performance du projet

ÉVALUATION FORMATIVE

Rédaction notée d'un bilan de projet et d'un procès-verbal de recette, préparation au dossier écrit du bloc

CONTENUS

- Procès-verbaux de recette, réserves et levée des réserves
- Solde des contrats et points de vigilance en droit commercial
- Obligations RGPD en fin de projet : registre des traitements, sort des données de test, sous-traitance
- Documentation technique et transfert vers l'exploitation
- Bilan de projet : avancement, économies réalisées, avancées techniques
- Animation d'un retour d'expérience et base de connaissances
- Amélioration continue du référentiel projets

Fil rouge · La migration ERP est en production. Camille signe le procès-verbal de recette avec réserves, solde le contrat d'Orvéa Conseil, vérifie la purge des données personnelles de test et anime l'atelier de retour d'expérience avec toute l'équipe projet.

RNCP38779BC03 · 88 h

Concevoir l'infrastructure du système d'Information

Cours 10 · Auditer l'infrastructure du SI au regard des standards et des préconisations ANSSI

22 h

OBJECTIFS

- Conduire un audit d'infrastructure pour identifier limites et points faibles
- Vérifier la conformité aux standards technologiques, organisationnels et de cybersécurité (ANSSI, principaux éditeurs)

ÉVALUATION FORMATIVE

Étude de cas notée : analyse d'un inventaire fictif et rédaction d'une synthèse d'écarts priorisée

CONTENUS

- Périmètre et méthodologie d'un audit d'infrastructure
- Inventaire des actifs : serveurs, réseaux, postes, applications, flux
- Guide d'hygiène informatique de l'ANSSI et guides de configuration des éditeurs
- Audit de l'annuaire, des réseaux, de la virtualisation et des sauvegardes
- Capacité, performance, obsolescence et dette technique
- Restitution : rapport d'audit, cotation des écarts et recommandations

Fil rouge · Camille réalise l'audit de l'infrastructure d'Altiméa en confrontant l'existant aux mesures du guide d'hygiène de l'ANSSI. Elle découvre des serveurs hors support, un réseau à plat entre agences et des sauvegardes jamais restaurées.

Cours 11 · Étudier et comparer les solutions technologiques d'infrastructure

22 h

OBJECTIFS

- Comparer les solutions technologiques (hébergement, réseau, ERP, data, sauvegarde) au regard des besoins métiers
- Formaliser un choix argumenté intégrant coûts, risques, réversibilité et sécurité

ÉVALUATION FORMATIVE

Exercice noté : grille comparative de solutions et note de recommandation

CONTENUS

- Expression des besoins métiers en exigences techniques
- Modèles d'hébergement : sur site, cloud public, cloud privé, hybride ; IaaS, PaaS, SaaS
- Critères de souveraineté et qualifications de sécurité des prestataires (dont SecNumCloud)
- Solutions réseau : SD-WAN, VPN, segmentation, accès distants
- Solutions de données et de sauvegarde : stratégie 3-2-1, sauvegarde immuable
- Coût total de possession et étude comparative
- Consultation des fournisseurs et grille d'analyse des offres

Fil rouge · Pour héberger le nouvel ERP et les données de santé indirectement manipulées, Camille compare trois offres d'hébergement et deux solutions de sauvegarde. Elle construit une grille d'analyse intégrant coût total, réversibilité et niveau de qualification sécurité.

Cours 12 · Concevoir une infrastructure sécurisée et bâtir le portefeuille d'évolution

22 h

OBJECTIFS

- Concevoir une architecture informatique sécurisée (réseaux, cloud, ERP, data, sauvegarde) conforme aux standards d'architecture
- Identifier les projets qui composeront le portefeuille d'évolution et de migration du SI

ÉVALUATION FORMATIVE

Production notée d'un schéma d'architecture cible commenté et d'une liste de projets de migration

CONTENUS

- Principes d'architecture sécurisée : défense en profondeur, cloisonnement, moindre privilège
- Conception réseau : zones de sécurité, DMZ, segmentation, filtrage
- Architecture d'annuaire et modèle d'administration en tiers
- Intégration cloud et hybride, gestion des identités fédérées
- Haute disponibilité, plan de reprise et architecture de sauvegarde
- Dossier d'architecture technique et schémas cibles
- Trajectoire de migration et découpage en projets du portefeuille

Fil rouge · Camille conçoit l'architecture cible hybride d'Altiméa : réseau segmenté entre siège, plateformes et agences, annuaire administré par niveaux, sauvegarde externalisée immuable. Elle traduit cette cible en six projets de migration intégrés au portefeuille de la DSI.

Cours 13 · Veille technologique, indicateurs d'infrastructure et conseil à la direction

22 h

OBJECTIFS

- Organiser et animer une veille active sur les technologies SI et les menaces auprès des éditeurs, prestataires et de l'ANSSI
- Définir des indicateurs d'activité et de détection pour identifier les besoins d'évolution
- Conseiller la direction à l'aide de tableaux de bord formalisés

ÉVALUATION FORMATIVE

Exercice noté de conception d'un tableau de bord et préparation à la soutenance orale du bloc (pitch simulé)

CONTENUS

- Organisation d'un dispositif de veille : sources, outils, rôles, diffusion
- Sources de référence : ANSSI, CERT-FR, bulletins éditeurs, prestataires
- Supervision d'infrastructure et indicateurs d'activité, de capacité et de disponibilité
- Indicateurs de détection de problèmes de sécurité sur l'infrastructure
- Analyse des solutions en place et identification des besoins de mise à jour
- Conception de tableaux de bord pour la direction
- Gouvernance du SI et présentation des investissements

Fil rouge · Camille met en place une veille partagée avec son équipe et un tableau de bord trimestriel de l'infrastructure. Elle s'en sert pour convaincre la direction générale de financer la deuxième phase de modernisation.

RNCP38779BC04 · 154 h

Sécuriser les infrastructures du système d'Information (accès, réseaux et données)

Cours 14 · Auditer la sécurité du SI : méthodologie et outils de pentesting

22 h

OBJECTIFS

- Mener un audit de sécurité selon une méthodologie structurée pour identifier les éléments à sécuriser
- Exploiter les résultats d'outils de pentesting pour déterminer le niveau de sécurité nécessaire (accès, données, réseaux)

ÉVALUATION FORMATIVE

Cas pratique en environnement simulé et QCM sur la méthodologie d'audit

CONTENUS

- Types d'audits de sécurité : organisationnel, configuration, architecture, test d'intrusion
- Cadre contractuel et éthique d'un test d'intrusion : convention, périmètre, autorisations
- Prestataires d'audit qualifiés (PASSI) et cahier des charges
- Phases d'un pentest : reconnaissance, scan, exploitation, post-exploitation
- Outils de reconnaissance, de scan de vulnérabilités et d'audit d'annuaire
- Classification des actifs et besoins de sécurité (disponibilité, intégrité, confidentialité, traçabilité)
- Lecture d'un rapport d'audit et priorisation des vulnérabilités

Fil rouge · Camille commande un test d'intrusion à un prestataire qualifié et en rédige le cahier des charges. Le rapport révèle des comptes d'administration partagés et un serveur exposé sur internet : elle classe les actifs et définit les niveaux de sécurité attendus.

Cours 15 · Cadre juridique et normatif de la sécurité des SI

22 h

OBJECTIFS

- Identifier les droits, obligations et normes applicables à la sécurisation du SI selon le contexte de l'organisation
- Évaluer la conformité réglementaire et normative du SI (RGPD, ISO 27001, recommandations CNIL, NIS 2)

ÉVALUATION FORMATIVE

Quiz réglementaire et étude de cas notée d'analyse d'écarts de conformité

CONTENUS

- RGPD et recommandations de la CNIL : sécurité des traitements, notification des violations
- Famille ISO 27000 : système de management de la sécurité de l'information, ISO 27001 et 27002
- Directives NIS et NIS 2 : entités concernées et obligations
- Règlement eIDAS et règlement européen sur la cybersécurité (ENISA, certification)
- Lois de programmation militaire, opérateurs d'importance vitale et opérateurs de services essentiels
- Référentiel général de sécurité, PSSIE et instructions interministérielles (dont II 901)
- Analyse d'écarts de conformité et feuille de route

Fil rouge · Un client hospitalier demande à Altiméa de prouver son niveau de sécurité. Camille détermine si le groupe entre dans le périmètre de NIS 2, réalise une analyse d'écarts par rapport à l'ISO 27001 et vérifie la conformité RGPD des traitements liés aux livraisons à domicile.

Cours 16 · Concevoir le plan de sécurisation et de supervision du SI

22 h

OBJECTIFS

- Concevoir un plan de sécurisation fondé sur les résultats d'audit et les obligations réglementaires
- Définir la stratégie de supervision de sécurité adaptée au niveau attendu

ÉVALUATION FORMATIVE

Production notée d'un extrait de plan de sécurisation priorisé et QCM

CONTENUS

- Du rapport d'audit au plan de traitement des risques
- Politique de sécurité du SI et chartes associées
- Sécurisation des accès : gestion des identités, authentification multifacteur, comptes à privilèges
- Sécurisation des réseaux : cloisonnement, filtrage, accès distants
- Sécurisation des données : chiffrement, classification, prévention des fuites, sauvegardes
- Durcissement des systèmes et gestion des correctifs
- Architecture de supervision : journalisation, collecte, corrélation

Fil rouge · À partir du rapport de pentest et de l'analyse d'écarts, Camille construit le plan de sécurisation d'Altiméa : authentification multifacteur pour tous les accès distants, bastion d'administration, chiffrement des postes nomades et politique de journalisation centralisée.

Cours 17 · Piloter les projets de sécurisation en agile et superviser leur efficacité

22 h

OBJECTIFS

- Identifier les opérations et les parties prenantes pour planifier les projets de sécurisation selon une méthodologie agile
- Suivre la mise en œuvre des solutions de sécurité à l'aide d'indicateurs et d'outils de surveillance de type SIEM

ÉVALUATION FORMATIVE

Exercice noté : constitution d'un backlog de sécurisation et définition d'indicateurs de suivi

CONTENUS

- Découpage des chantiers de sécurisation en épopées et histoires utilisateur
- Parties prenantes : métiers, exploitation, prestataires, délégué à la protection des données
- Animation des cérémonies agiles appliquées à la sécurité
- Fonctionnement d'un SIEM : collecte, normalisation, corrélation, alertes
- Centre opérationnel de sécurité interne ou externalisé
- Indicateurs de suivi : couverture, taux de correctifs, délais de détection et de traitement
- Mesure de l'efficacité et ajustement des mesures

Fil rouge · Camille organise les chantiers de sécurisation en sprints de deux semaines avec son équipe et le prestataire SOC. Elle définit les premières règles de corrélation du SIEM et suit chaque mois les indicateurs de couverture et de délai de traitement des alertes.

Cours 18 · Veille cyber, analyse des indicateurs et gouvernance de la sécurité

22 h

OBJECTIFS

- Animer une veille active sur les menaces et solutions de sécurisation auprès de l'ANSSI, des CERT, des éditeurs et prestataires
- Analyser les indicateurs d'activité pour détecter les besoins d'évolution ou les failles
- Conseiller la direction et contribuer à la gouvernance de la sécurité au moyen de tableaux de bord

ÉVALUATION FORMATIVE

Étude de cas notée : analyse d'un bulletin de vulnérabilité et rédaction d'une note de recommandation à la direction

CONTENUS

- Veille sur les menaces : avis et alertes CERT-FR, bulletins éditeurs, renseignement sur la menace
- Gestion des vulnérabilités : qualification, criticité, priorisation des correctifs
- Exploitation croisée de la veille et des indicateurs d'activité
- Rôles de la gouvernance sécurité : RSSI, comité sécurité, direction, DPO
- Tableau de bord sécurité à destination de la direction
- Justification des investissements cybersécurité et arbitrages budgétaires

Fil rouge · Une alerte du CERT-FR signale une vulnérabilité critique sur la solution d'accès distant utilisée par Altiméa. Camille croise l'alerte avec les journaux du SIEM, déclenche un correctif d'urgence puis présente au comité sécurité le tableau de bord trimestriel et ses demandes d'investissement.

Cours 19 · Anticiper la crise cyber : risques, continuité et organisation

22 h

OBJECTIFS

- Évaluer les risques cyber selon une méthode reconnue
- Construire un plan de continuité d'activité, un plan de communication de crise et une organisation des rôles et responsabilités

ÉVALUATION FORMATIVE

Exercice noté de rédaction d'une fiche réflexe et d'un extrait de plan de continuité, QCM

CONTENUS

- Analyse de risques cyber : méthode EBIOS Risk Manager
- Bilan d'impact sur l'activité et définition des délais de reprise
- Plan de continuité et plan de reprise d'activité informatique
- Organisation de crise : cellule décisionnelle, cellule technique, rôles et suppléances
- Plan de communication de crise interne et externe, accessible à tous les acteurs
- Annuaire de crise, moyens de communication de secours, contrats d'assistance
- Exercices de crise : préparation, conduite, retour d'expérience

Fil rouge · Camille anime un atelier EBIOS Risk Manager avec la direction logistique, puis rédige le plan de continuité d'activité et le plan de communication de crise. Elle organise un premier exercice sur table simulant l'indisponibilité de l'ERP.

Cours 20 · Détecter, répondre à l'incident et renforcer la résilience du SI

22 h

OBJECTIFS

- Détecter et qualifier une attaque à partir des données de surveillance et des incidents de sécurité
- Gérer l'incident pour stopper sa progression et restaurer un SI sain
- Évaluer les dommages et mettre à jour les solutions techniques et le plan de crise

ÉVALUATION FORMATIVE

Simulation de crise interactive notée et rédaction d'un rapport post-incident, préparation au dossier écrit du bloc

CONTENUS

- Détection et qualification : alertes SIEM, indicateurs de compromission, triage
- Phases de réponse à incident : confinement, éradication, restauration
- Activation de la cellule de crise et du plan de communication
- Obligations de notification : CNIL, ANSSI, autorités compétentes, dépôt de plainte
- Restauration à partir des sauvegardes et remise en service contrôlée
- Évaluation des dommages : analyse de l'attaque, pertes subies, impacts métiers
- Retour d'expérience et mise à jour du plan de crise et des mesures techniques

Fil rouge · Un rançongiciel chiffre les serveurs d'une agence régionale d'Altiméa un vendredi soir. Camille qualifie l'attaque grâce au SIEM, active la cellule de crise, isole le site, restaure les données depuis la sauvegarde immuable, puis pilote l'évaluation des dommages et la mise à jour du plan de crise.

05 · CONFORMITÉ AU RÉFÉRENTIEL

Couverture des compétences

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

Compétence	Bloc	Cours
Gérer et encadrer son équipe en responsabilité hiérarchique	RNCP38779BC01	1
Organiser et piloter une équipe en responsabilité fonctionnelle	RNCP38779BC01	2
Manager les relations clients et fournisseurs	RNCP38779BC01	2
Analyser l'environnement technique et métier du SI	RNCP38779BC01	3
Modéliser le SI pour les décideurs	RNCP38779BC01	3
Identifier les améliorations possibles du SI	RNCP38779BC01	3
Identifier une méthode de gestion du changement	RNCP38779BC01	4
Définir et conduire le plan d'accompagnement de la transformation	RNCP38779BC01	4
Élaborer le référentiel documentaire des projets IT	RNCP38779BC02	5
Définir les critères de priorisation et ordonnancer le portefeuille projets	RNCP38779BC02	6
Exposer et défendre les choix de sélection des projets	RNCP38779BC02	6
S'approprier le contexte et le périmètre de chaque projet IT	RNCP38779BC02	7
Établir le plan de management de chaque projet IT	RNCP38779BC02	7
Contrôler et valider les livrables (qualité, coût, délai)	RNCP38779BC02	8
Organiser les recettes fonctionnelle et technique	RNCP38779BC02	8
Établir les documents administratifs, contractuels et techniques de clôture	RNCP38779BC02	9
Organiser et animer la capitalisation d'expérience	RNCP38779BC02	9
Auditer l'infrastructure du SI au regard des standards (ANSSI, éditeurs)	RNCP38779BC03	10
Étudier et comparer les solutions technologiques	RNCP38779BC03	11
Concevoir une infrastructure informatique sécurisée	RNCP38779BC03	11, 12
Identifier les projets du portefeuille d'évolution et de migration	RNCP38779BC03	12
Organiser et animer une veille sur les technologies SI et les menaces	RNCP38779BC03	13
Analyser les solutions implantées et définir des indicateurs	RNCP38779BC03	13
Conseiller la direction sur les projets et investissements SI	RNCP38779BC03	13
Auditer la sécurité du SI avec outils de pentesting et méthodologie d'audit	RNCP38779BC04	14
Identifier les droits, obligations et normes de sécurisation du SI	RNCP38779BC04	15

Concevoir le plan de sécurisation et de supervision du SI	RNCP38779BC04	16
Organiser et planifier les projets de sécurisation en méthode agile	RNCP38779BC04	17
Suivre et superviser les solutions de sécurisation (indicateurs, SIEM)	RNCP38779BC04	17
Organiser et animer une veille sur les menaces et solutions de sécurisation	RNCP38779BC04	18
Analyser les indicateurs d'activité pour identifier mises à jour et failles	RNCP38779BC04	18
Conseiller la direction et contribuer à la gouvernance de la sécurité SI	RNCP38779BC04	18
Anticiper la crise cyber (risques, PCA, communication, rôles)	RNCP38779BC04	19
Détecter et identifier l'attaque	RNCP38779BC04	20
Gérer l'incident et répondre à la crise	RNCP38779BC04	20
Évaluer les dommages et améliorer la résilience du SI	RNCP38779BC04	20

Évaluations formatives

Chaque cours intègre des évaluations formatives régulières permettant à l'apprenant et au formateur de mesurer la progression : QCM de fin de sous-chapitre avec correction commentée, études de cas notées, mises en situation interactives dans le fil rouge du Groupe Altiméa et exercices de production de livrables professionnels (cartographies, notes d'arbitrage, cahiers de recette, schémas d'architecture, plans de sécurisation, rapports post-incident). Des grilles d'autoévaluation alignées sur les critères des compétences du référentiel accompagnent les productions. Les résultats sont consultables sur la plateforme et permettent à l'organisme de formation d'assurer le suivi individualisé, de repérer les difficultés et de proposer des remédiations ciblées.

Modalités de certification

Bloc	Modalité d'évaluation
RNCP38779BC01	Application professionnelle, réelle ou simulée, portant sur le management de la transformation du SI, donnant lieu à une soutenance orale.
RNCP38779BC02	Application professionnelle, réelle ou simulée, portant sur la supervision d'un portefeuille projets, donnant lieu à la production d'un document écrit.
RNCP38779BC03	Application professionnelle, réelle ou simulée, portant sur la conception d'une infrastructure informatique sécurisée, donnant lieu à une soutenance orale.
RNCP38779BC04	Application professionnelle, réelle ou simulée, portant sur la sécurisation d'une infrastructure informatique, donnant lieu à la production d'un document écrit.

Le parcours est construit pour préparer directement aux applications professionnelles exigées par le référentiel. Le fil rouge du Groupe Altiméa fournit un contexte d'entreprise complet et cohérent, utilisable comme base d'application simulée lorsque l'apprenant ne dispose pas d'un terrain réel. Les livrables produits dans chaque cours constituent les briques des épreuves : plan d'accompagnement et cartographie pour le bloc 1, note d'arbitrage, plan de management et bilan de projet pour le bloc 2, rapport d'audit et dossier d'architecture pour le bloc 3, plan de sécurisation, plan de crise et rapport post-incident pour le bloc 4. Les cours de fin de bloc proposent des exercices de soutenance orale ou de rédaction de dossier écrit selon la modalité officielle. School For Mate fournit le contenu pédagogique ;

l'organisme de formation reste responsable de l'inscription des candidats, de l'organisation des épreuves et de la relation avec le certificateur.

06 · MOYENS ET PERSPECTIVES

Moyens pédagogiques et débouchés

Moyens pédagogiques et techniques

- Plateforme e-learning en marque blanche accessible 24 h/24, sur ordinateur, tablette et mobile, avec suivi de progression et traçabilité des connexions
- Une vidéo de 3 à 5 minutes par sous-chapitre, représentant 30 % du volume horaire, soit environ 6 h 36 par cours de 22 heures
- Cours texte enrichi, infographies, schémas d'architecture et fiches de synthèse téléchargeables
- Études de cas et mises en situation interactives dans le fil rouge du Groupe Altiméa
- Modèles de livrables professionnels : note de cadrage, grille de cotation, cahier de recette, plan de sécurisation, fiches réflexes de crise
- QCM et évaluations formatives avec correction commentée et grilles d'autoévaluation
- Ressources de référence citées et commentées (guides de l'ANSSI, recommandations de la CNIL, textes réglementaires) et accompagnement par les formateurs de l'organisme de formation

Débouchés et évolutions

- Responsable de la sécurité du système d'information
- Architecte en systèmes d'information ou en cybersécurité
- Chef de projet infrastructures, systèmes d'information ou cybersécurité
- Consultant en système d'information ou cybersécurité
- Responsable des systèmes d'information ou manager du système d'information
- Directeur des systèmes d'information

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 RNCP38779 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.