

SCHOOL FOR MATE

LIVRET PÉDAGOGIQUE

Administrateur systèmes, réseaux et cybersécurité

RNCP39611 · Certification RNCP · Niveau 6

Ce parcours de 440 heures prépare à l'ensemble des compétences du titre RNCP39611 « Administrateur systèmes, réseaux et cybersécurité » (niveau 6), de l'administration des serveurs à la conduite de projets d'infrastructure sécurisée. Construit autour d'un fil rouge professionnel continu, il couvre les quatre blocs de compétences du référentiel et entraîne l'apprenant aux mises en situation reconstituées prévues pour la certification.

VOLUME HORAIRE	COURS	BLOCS
440 h	20	4

01 · PRÉSENTATION

La formation en bref

Intitulé	Administrateur systèmes, réseaux et cybersécurité
Code	RNCP39611
Type	Certification RNCP
Niveau	Niveau 6
Certificateur	ASSOCIATION POUR LA GESTION DE 3IL
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	01/10/2029

Le métier et les compétences visées

L'administrateur systèmes, réseaux et cybersécurité garantit le bon fonctionnement, la sécurité et la performance des infrastructures informatiques d'une organisation. Il administre les systèmes d'exploitation Linux, Unix et Windows, les annuaires, les environnements virtualisés et les bases de données, et met en place la haute disponibilité et l'automatisation. Il configure et supervise le réseau, déploie des solutions de conteneurisation et des chaînes d'intégration et de déploiement continus. Il élabore les politiques de sécurité, conduit des audits, administre pare-feux, IDS/IPS et IAM, pilote sauvegardes et plans de reprise et veille à la conformité RGPD. Enfin, il conduit des projets d'infrastructure en méthode agile, gère leur budget et anime une veille technologique multilingue.

Public visé

- Titulaires d'un baccalauréat souhaitant s'orienter vers les métiers de l'infrastructure et de la cybersécurité (cursus en 3 ans)
- Techniciens supérieurs systèmes et réseaux titulaires d'une certification de niveau 5 en informatique (cursus en 1 an)
- Alternants en contrat d'apprentissage ou de professionnalisation au sein d'une DSI ou d'une entreprise de services numériques
- Professionnels de l'IT en reconversion ou en évolution vers des fonctions d'administration sécurisée
- Salariés en parcours de validation par blocs de compétences

Prérequis

- Cursus en 3 ans : être titulaire d'un baccalauréat
- Cursus en 1 an : être titulaire d'une certification de niveau 5 dans le domaine informatique
- Maîtriser l'environnement bureautique et la navigation sur un poste de travail connecté
- Disposer d'un niveau d'anglais permettant la lecture de documentation technique simple

Objectifs pédagogiques

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

- Administrer et optimiser des systèmes Linux, Unix et Windows Server selon les bonnes pratiques de qualité de service
- Concevoir une topologie d'annuaire et des environnements virtualisés on-premise ou cloud adaptés aux besoins de l'entreprise
- Mettre en œuvre la haute disponibilité, la supervision des performances et l'automatisation par scripts Python, Shell et Bash
- Configurer, déployer et superviser une infrastructure réseau, données et voix sécurisée
- Déployer des applications conteneurisées et orchestrées au sein de pipelines CI/CD intégrant la sécurité
- Élaborer une politique de sécurité à partir d'une analyse de risques, conduire des audits et piloter les actions correctives
- Implémenter et administrer pare-feux, IDS/IPS et systèmes IAM avec authentification multifacteur accessible
- Superviser sauvegardes, restaurations et plans de reprise d'activité dans le respect des RTO, RPO et SLA
- Garantir la conformité des traitements de données au RGPD et aux recommandations de l'ANSSI
- Conduire un projet d'infrastructure en méthode agile, de l'étude de faisabilité au suivi budgétaire, en s'appuyant sur une veille multilingue

02 · FIL ROUGE PÉDAGOGIQUE

Ardenvia Santé

LM

Léa Morvan

Administratrice systèmes, réseaux et cybersécurité au sein de la DSI, évoluant vers la responsabilité de l'infrastructure

Santé privée : réseau de quatre cliniques et d'un centre d'imagerie médicale répartis sur deux régions

Ardenvia Santé regroupe quatre cliniques et un centre d'imagerie, soit environ 1 200 postes utilisateurs, un dossier patient informatisé, une téléphonie multisite et des équipements biomédicaux connectés. Son infrastructure, construite par strates successives, souffre de serveurs vieillissants, d'un annuaire mal structuré, d'une supervision partielle et d'une sauvegarde jamais testée en conditions réelles. La direction générale a lancé un programme de modernisation baptisé « Socle 2027 » : consolider le datacenter, ouvrir un environnement cloud hybride, sécuriser les données de santé et se mettre en conformité avec le RGPD et les recommandations de l'ANSSI. Léa Morvan rejoint la DSI dirigée par Karim Delaunay. Elle travaille avec Hugo Ferrand, technicien réseau, Nadia Belkacem, déléguée à la protection des données, et l'équipe de développement du portail patient.

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

La progression

1. Bloc 1 : Léa reprend en main les serveurs, restructure l'annuaire, virtualise le datacenter, fiabilise les bases du dossier patient et automatise l'exploitation après un premier incident majeur.
2. Bloc 2 : Léa refond le réseau multisite et la téléphonie, met en place la supervision réseau puis accompagne l'équipe du portail patient vers les conteneurs et une chaîne CI/CD sécurisée.
3. Bloc 3 : face à une tentative d'intrusion, Léa formalise la PSSI, conduit un audit, durcit le périmètre, déploie l'IAM avec MFA accessible et pilote le PRA et la mise en conformité RGPD avec la DPO.
4. Bloc 4 : promue cheffe de projet du programme « Socle 2027 », Léa conduit l'étude de faisabilité, anime l'équipe en agile, pilote le budget et installe une veille multilingue au service de la DSI.

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
RNCP39611BC01 · Administrer et optimiser les systèmes d'exploitation et la virtualisation pour la sécurité et la performance		**132 h**
1	Administration et optimisation des systèmes Linux, Unix et Windows Server	22 h
2	Annuaires, topologies systèmes et gestion des identités	22 h
3	Virtualisation on-premise et environnements cloud	22 h
4	Administration des bases de données relationnelles et NoSQL	22 h
5	Haute disponibilité, continuité et supervision des performances	22 h
6	Gestion des incidents et automatisation de l'administration	22 h
RNCP39611BC02 · Configurer et administrer l'infrastructure réseau et les solutions cloud		**110 h**
7	Conception et configuration de l'infrastructure réseau	22 h
8	Déploiement des solutions de télécommunications, données et voix	22 h
9	Supervision et maintenance du réseau	22 h
10	Conteneurisation et orchestration des applications	22 h
11	Intégration et déploiement continus, pratiques DevSecOps sur le cloud	22 h
RNCP39611BC03 · Élaborer et mettre en œuvre des stratégies de cybersécurité et de protection des données		**110 h**
12	Politique de sécurité, analyse de risques et ethical hacking	22 h
13	Audits de sécurité, actions correctives et conformité RGPD	22 h
14	Sécurité périmétrique : pare-feux, IDS/IPS et protection des réseaux	22 h
15	Gestion des identités et des accès, authentification forte et accessibilité	22 h
16	Sauvegarde, plan de reprise d'activité et gestion des incidents de sécurité	22 h
RNCP39611BC04 · Conduire la gestion de projets d'infrastructure systèmes et réseaux sécurisée		**88 h**
17	Étude de faisabilité, exigences et spécifications techniques	22 h
18	Pilotage agile de projets d'infrastructure	22 h
19	Gestion budgétaire et pilotage financier du projet	22 h
20	Veille technologique et réglementaire multilingue	22 h

Total du parcours	440 h

Répartition des modalités pédagogiques

Chaque sous-chapitre s'ouvre sur une vidéo de 3 à 5 minutes. La vidéo représente 30 % du volume horaire, complétée par du cours texte enrichi, des infographies, des études de cas, des mises en situation et des QCM.



- Vidéos : 132 h
- Cours texte et infographies : 138 h 30
- Études de cas et mises en situation : 108 h
- QCM et évaluations : 61 h 30

04 · PROGRAMME DÉTAILLÉ

Contenu des cours

RNCP39611BC01 · 132 h

Administrer et optimiser les systèmes d'exploitation et la virtualisation pour la sécurité et la performance

Cours 1 · Administration et optimisation des systèmes Linux, Unix et Windows Server — 22 h

OBJECTIFS

- Installer, configurer et maintenir des serveurs Linux, Unix et Windows Server
- Optimiser les systèmes selon les bonnes pratiques de qualité de service et de durcissement

ÉVALUATION FORMATIVE

QCM par sous-chapitre et étude de cas : rapport de diagnostic et plan d'optimisation d'un serveur

CONTENUS

- Architecture des systèmes d'exploitation serveurs et cycle de vie
- Administration Linux : arborescence, utilisateurs, droits, services systemd, paquets
- Spécificités des environnements Unix et interopérabilité
- Administration Windows Server : rôles, fonctionnalités, PowerShell, stratégies locales
- Gestion des mises à jour et des correctifs de sécurité
- Qualité de service : indicateurs de performance, dimensionnement, tuning noyau et services
- Durcissement des systèmes selon les guides de l'ANSSI
- Documentation d'exploitation et collaboration avec les équipes techniques

Fil rouge · Léa reprend six serveurs hétérogènes de la clinique principale, dont l'un ralentit le dossier patient aux heures de pointe : elle diagnostique, optimise et rédige les fiches d'exploitation.

Cours 2 · Annuaires, topologies systèmes et gestion des identités — 22 h

OBJECTIFS

- Concevoir une topologie d'annuaire structurant ressources, identités et accès
- Appliquer les politiques d'accès et de sécurité de l'entreprise via l'annuaire

ÉVALUATION FORMATIVE

Exercice de conception : schéma de topologie d'annuaire commenté et matrice de délégation

CONTENUS

- Principes des services d'annuaire : LDAP, Active Directory, OpenLDAP
- Conception de forêts, domaines, sites et unités d'organisation
- Modèle de délégation et principe du moindre privilège
- Stratégies de groupe et gestion centralisée des postes
- Gestion des comptes, groupes, cycles d'arrivée et de départ
- Intégration des systèmes Linux à l'annuaire
- Sécurisation de l'annuaire et modèle d'administration en tiers

Fil rouge · L'annuaire d'Ardenvia contient des comptes orphelins et des droits hérités incohérents : Léa conçoit une nouvelle topologie d'unités d'organisation par site et par métier, puis planifie la migration.

Cours 3 · Virtualisation on-premise et environnements cloud

22 h

OBJECTIFS

- Concevoir et déployer une infrastructure virtualisée on-premise ou chez un cloud provider
- Rationaliser les ressources et anticiper l'évolutivité des besoins

ÉVALUATION FORMATIVE

Étude de cas : dossier d'architecture de virtualisation avec justification des choix

CONTENUS

- Concepts de virtualisation : hyperviseurs de type 1 et 2, ressources virtuelles
- Conception d'un cluster de virtualisation : calcul, stockage, réseau virtuel
- Déploiement et gestion des machines virtuelles, modèles et snapshots
- Modèles de services cloud IaaS, PaaS, SaaS et architectures hybrides
- Déploiement d'instances et de réseaux virtuels chez un fournisseur cloud
- Souveraineté et qualification SecNumCloud : critères de choix d'un hébergeur
- Capacity planning et optimisation des coûts d'infrastructure
- Collaboration avec les architectes système et documentation d'architecture

Fil rouge · Léa propose à Karim Delaunay la consolidation de vingt serveurs physiques sur un cluster virtualisé et l'ouverture d'un environnement cloud qualifié pour le portail patient.

Cours 4 · Administration des bases de données relationnelles et NoSQL

22 h

OBJECTIFS

- Concevoir, administrer et optimiser des SGBD relationnels et NoSQL
- Garantir la cohérence, la sécurité et la disponibilité permanente des données

ÉVALUATION FORMATIVE

Travaux pratiques guidés et QCM : optimisation de requêtes et plan de sécurisation d'une base

CONTENUS

- Modèle relationnel, normalisation et langage SQL d'administration
- Installation et configuration d'un SGBD relationnel
- Bases NoSQL : document, clé-valeur, colonnes, graphes, cas d'usage
- Optimisation : index, plans d'exécution, paramétrage mémoire
- Sécurité des bases : rôles, privilèges, chiffrement, journalisation
- Sauvegarde et restauration des bases de données
- Collaboration avec développeurs et analystes de données

Fil rouge · Les requêtes du dossier patient dépassent plusieurs secondes et le service d'imagerie souhaite une base NoSQL pour ses métadonnées : Léa optimise l'existant et cadre la nouvelle base avec les développeurs.

Cours 5 · Haute disponibilité, continuité et supervision des performances

22 h

OBJECTIFS

- Mettre en œuvre redondance, réplication et clustering au service de la continuité d'activité
- Surveiller et optimiser les performances à l'aide d'outils de monitoring et d'analyse

ÉVALUATION FORMATIVE

Étude de cas : compte-rendu d'amélioration d'une architecture et de son PCA

CONTENUS

- Notions de disponibilité, points uniques de défaillance et PCA
- Redondance matérielle, RAID, alimentation et liens réseau
- Réplication de données synchrone et asynchrone
- Clustering actif/passif et actif/actif, répartition de charge
- Mise en place d'une solution de monitoring : métriques, seuils, alertes
- Analyse des journaux et corrélation d'événements
- Tableaux de bord de performance et coordination avec l'exploitation
- Analyse d'une architecture existante et propositions d'amélioration

Fil rouge · Une panne de stockage interrompt le bloc opératoire pendant deux heures : Léa analyse l'architecture et le PCA, met en cluster les services critiques et déploie une supervision proactive.

Cours 6 · Gestion des incidents et automatisation de l'administration

22 h

OBJECTIFS

- Piloter le processus de gestion des incidents avec un outil de ticketing dans le respect des SLA
- Automatiser les tâches d'administration en Python, Shell et Bash

ÉVALUATION FORMATIVE

Exercice pratique : traitement d'un lot de tickets et livraison d'un script commenté

CONTENUS

- Processus de gestion des incidents selon les bonnes pratiques ITIL
- Outil de ticketing : catégorisation, priorisation, escalade
- SLA, OLA et indicateurs de suivi des incidents
- Fondamentaux du scripting Bash et Shell pour l'exploitation
- Scripting Python pour l'administration système et réseau
- Automatisation de la maintenance : planification, rapports, remédiations
- Recherche de solutions dans la documentation technique anglophone
- Bonnes pratiques : versionnement, tests et documentation des scripts

Fil rouge · Le support de la DSI est saturé de tickets répétitifs : Léa refond la grille de priorisation et développe des scripts qui automatisent les contrôles quotidiens et la purge des journaux.

RNCP39611BC02 · 110 h

Configurer et administrer l'infrastructure réseau et les solutions cloud

Cours 7 · Conception et configuration de l'infrastructure réseau

22 h

OBJECTIFS

- Configurer l'infrastructure réseau avec les protocoles et équipements adaptés aux besoins
- Assurer une connectivité fluide et sécurisée du système d'information

ÉVALUATION FORMATIVE

Étude de cas : topologie commentée et fiches de test de configuration

CONTENUS

- Modèles OSI et TCP/IP, adressage IPv4 et IPv6
- Commutation : VLAN, agrégation de liens, Spanning Tree
- Routage statique et dynamique, protocoles OSPF et BGP
- Services réseau : DHCP, DNS, NTP
- Interconnexion de sites : VPN IPsec, SD-WAN
- Réseaux sans fil d'entreprise et sécurisation
- Rédaction de topologies et de fiches de tests

Fil rouge · Avec Hugo Ferrand, Léa redessine le réseau des quatre cliniques : segmentation en VLAN par usage (biomédical, administratif, invités) et interconnexion VPN entre sites.

Cours 8 · Déploiement des solutions de télécommunications, données et voix

22 h

OBJECTIFS

- Déployer en production des solutions de réseaux de données et de voix
- Coordonner l'installation avec les équipes techniques et les fournisseurs

ÉVALUATION FORMATIVE

Mise en situation : plan de déploiement et cahier de recette d'une solution voix

CONTENUS

- Architecture des télécommunications d'entreprise et offres opérateurs
- Téléphonie sur IP : protocoles SIP et RTP, IPBX
- Qualité de service réseau pour la voix et la vidéo
- Communications unifiées et visioconférence
- Préparation et conduite d'une mise en production
- Pilotage des fournisseurs et recette de l'installation
- Continuité des services de communication et secours

Fil rouge · L'ancien autocommutateur de la clinique principale arrive en fin de support : Léa pilote la migration vers une téléphonie IP multisite avec l'intégrateur retenu.

Cours 9 · Supervision et maintenance du réseau

22 h

OBJECTIFS

- Superviser le réseau à l'aide de systèmes de monitoring
- Organiser la maintenance préventive et corrective pour une performance optimale

ÉVALUATION FORMATIVE

QCM et étude de cas : analyse de tableaux de bord de supervision et préconisations

CONTENUS

- Protocoles de supervision : SNMP, NetFlow, syslog
- Déploiement d'une plateforme de supervision réseau
- Indicateurs de performance réseau : latence, gigue, perte, débit
- Diagnostic et résolution des incidents réseau
- Maintenance préventive, gestion des firmwares et des configurations
- Coordination avec les équipes sécurité et exploitation

Fil rouge · Des coupures intermittentes perturbent le centre d'imagerie : Léa installe une supervision réseau, identifie un lien saturé et met en place un plan de maintenance.

Cours 10 · Conteneurisation et orchestration des applications

22 h

OBJECTIFS

- Développer des environnements conteneurisés pour standardiser le déploiement des applications
- Orchestrer les conteneurs pour assurer résilience et performance

ÉVALUATION FORMATIVE

Travaux pratiques : conteneurisation d'une application et fichier de déploiement commenté

CONTENUS

- Principes de la conteneurisation et différences avec la virtualisation
- Création d'images, Dockerfile et registres
- Composition d'applications multi-conteneurs
- Orchestration avec Kubernetes : pods, déploiements, services
- Gestion du stockage, du réseau et des secrets en environnement orchestré
- Mise à l'échelle, auto-réparation et mises à jour progressives
- Supervision des clusters de conteneurs

Fil rouge · L'équipe du portail patient livre ses versions à la main sur des serveurs différents : Léa conteneurise l'application et la déploie sur un cluster orchestré.

Cours 11 · Intégration et déploiement continus, pratiques DevSecOps sur le cloud

22 h

OBJECTIFS

- Mettre en place une chaîne d'intégration et de déploiement continus
- Intégrer la sécurité dans les processus de développement et d'exploitation cloud

ÉVALUATION FORMATIVE

Mise en situation individuelle : mise en place d'un pipeline CI/CD documenté

CONTENUS

- Culture DevOps et collaboration entre développement et exploitation
- Gestion de versions avec Git et stratégies de branches
- Conception d'un pipeline CI/CD : construction, tests, déploiement
- Infrastructure as Code et gestion de configuration
- Sécurité dans le pipeline : analyse de code, scan d'images, gestion des secrets
- Conformité des applications sur plateformes cloud
- Observabilité et retour arrière en cas d'échec de déploiement

Fil rouge · Léa construit pour le portail patient un pipeline qui teste, analyse la sécurité et déploie automatiquement chaque version dans l'environnement cloud qualifié.

RNCP39611BC03 · 110 h

Élaborer et mettre en œuvre des stratégies de cybersécurité et de protection des données

Cours 12 · Politique de sécurité, analyse de risques et ethical hacking

22 h

OBJECTIFS

- Évaluer les risques et définir des stratégies de mitigation avec un outil d'analyse de risques
- Rédiger et mettre en œuvre une politique de sécurité et ses procédures

ÉVALUATION FORMATIVE

Étude de cas : cartographie des risques et extrait de PSSI rédigé

CONTENUS

- Panorama des menaces et acteurs de la cybersécurité en France (ANSSI, CNIL)
- Normes et référentiels : ISO 27001, ISO 27005, guide d'hygiène de l'ANSSI
- Analyse de risques selon la méthode EBIOS Risk Manager
- Stratégies de traitement et de mitigation des risques
- Rédaction d'une PSSI et des procédures associées
- Ethical hacking : cadre légal, autorisation et méthodologie
- Tests d'intrusion : reconnaissance, exploitation, rapport
- Cadre réglementaire : NIS 2, loi Sapin II, protection des lanceurs d'alerte

Fil rouge · Après une campagne d'hameçonnage ciblant les secrétariats médicaux, Léa conduit l'analyse de risques d'Ardenvia et rédige la PSSI avec la gouvernance.

Cours 13 · Audits de sécurité, actions correctives et conformité RGPD

22 h

OBJECTIFS

- Conduire un audit de sécurité selon une méthodologie standardisée
- Élaborer un plan d'actions correctives et assurer la conformité au RGPD

ÉVALUATION FORMATIVE

Mise en situation : rapport d'analyse et préconisations sur une infrastructure d'entreprise

CONTENUS

- Types d'audits : organisationnel, technique, de configuration, de conformité
- Méthodologie d'audit : périmètre, preuves, entretiens, outils de scan
- Collaboration avec auditeurs externes et équipes internes
- Analyse des vulnérabilités et des non-conformités, priorisation
- Plan d'actions correctives et amélioration continue
- RGPD : principes, registre des traitements, droits des personnes
- Analyse d'impact relative à la protection des données et données de santé
- Audit de conformité RGPD et relation avec la DPO et les juristes

Fil rouge · Léa et Nadia Belkacem auditent l'infrastructure et les traitements du dossier patient, puis présentent à la direction un rapport d'analyse et un plan de remédiation priorisé.

Cours 14 · Sécurité périmétrique : pare-feux, IDS/IPS et protection des réseaux

22 h

OBJECTIFS

- Implémenter et configurer pare-feux et systèmes IDS/IPS
- Maintenir ces outils à jour pour prévenir les intrusions

ÉVALUATION FORMATIVE

Travaux pratiques : matrice de flux et jeu de règles de filtrage justifié

CONTENUS

- Architectures de sécurité réseau : zones, DMZ, segmentation
- Pare-feux nouvelle génération : règles, filtrage applicatif, journalisation
- Détection et prévention d'intrusion : signatures, comportement
- Proxy, filtrage web et sécurisation de la messagerie
- Protection des postes et serveurs : EDR et antivirus
- Centralisation des événements de sécurité et SIEM
- Gestion des mises à jour et revue périodique des règles

Fil rouge · L'IDS récemment installé signale un scan depuis un équipement biomédical : Léa isole le segment, ajuste les règles de filtrage et formalise la procédure de revue.

Cours 15 · Gestion des identités et des accès, authentification forte et accessibilité

22 h

OBJECTIFS

- Administrer un système IAM avec des politiques d'accès rigoureuses
- Déployer une authentification multifacteur adaptée aux personnes en situation de handicap

ÉVALUATION FORMATIVE

Étude de cas : politique d'accès et plan de déploiement MFA accessible

CONTENUS

- Principes de l'IAM : provisionnement, habilitations, revue des droits
- Modèles de contrôle d'accès : RBAC, ABAC
- Authentification unique et fédération d'identité
- Authentification multifacteur : facteurs, méthodes, déploiement
- Accessibilité des dispositifs d'authentification pour les personnes en situation de handicap
- Gestion des comptes à privilèges et bastion d'administration
- Indicateurs et audit des accès

Fil rouge · Léa déploie la MFA sur l'accès distant au dossier patient et prévoit, pour une secrétaire malvoyante, une méthode d'authentification alternative validée avec le référent handicap.

Cours 16 · Sauvegarde, plan de reprise d'activité et gestion des incidents de sécurité — 22 h

OBJECTIFS

- Superviser sauvegardes et restaurations et élaborer un plan de reprise après sinistre
- Piloter le support des incidents IT dans le respect des RTO et RPO

ÉVALUATION FORMATIVE

Mise en situation : plan de sauvegarde et de reprise élaboré à partir d'une étude de cas

CONTENUS

- Stratégies de sauvegarde : règle 3-2-1, sauvegardes immuables et externalisées
- Supervision et tests réguliers de restauration
- Analyse d'impact sur l'activité, définition des RTO et RPO
- Rédaction et exercice d'un plan de reprise d'activité
- Gestion de crise cyber et réponse à incident
- Communication avec les utilisateurs, la direction et les autorités
- Retour d'expérience et amélioration continue

Fil rouge · Lors d'un exercice de rançongiciel simulé, Léa coordonne la restauration des services prioritaires et mesure les écarts avec les RTO et RPO fixés par la DSI.

RNCP39611BC04 · 88 h
Conduire la gestion de projets d'infrastructure systèmes et réseaux sécurisée

Cours 17 · Étude de faisabilité, exigences et spécifications techniques — 22 h

OBJECTIFS

- Traduire les besoins opérationnels en exigences fonctionnelles et techniques
- Rédiger des spécifications techniques viables, rentables et conformes aux normes

ÉVALUATION FORMATIVE

Mise en situation : rédaction d'une étude d'avant-projet

CONTENUS

- Recueil des besoins : entretiens, ateliers, analyse de l'existant
- Exigences fonctionnelles et non fonctionnelles
- Étude de faisabilité technique, économique et organisationnelle
- Comparaison des options technologiques et matrice de décision
- Rédaction d'une étude d'avant-projet
- Spécifications techniques détaillées et conformité aux normes
- Présentation des choix aux décideurs

Fil rouge · Promue cheffe de projet du programme « Socle 2027 », Léa rédige l'étude d'avant-projet du futur datacenter hybride et la présente au comité de direction.

Cours 18 · Pilotage agile de projets d'infrastructure

22 h

OBJECTIFS

- Planifier, animer et suivre un projet informatique en méthodes agiles
- Optimiser avancement et priorités avec des outils comme JIRA ou Trello

ÉVALUATION FORMATIVE

Mise en situation : compte rendu d'activité d'un sprint et soutenance individuelle

CONTENUS

- Fondamentaux de l'agilité : Scrum, Kanban, adaptation aux projets d'infrastructure
- Rôles, cérémonies et artefacts agiles
- Construction et priorisation du backlog
- Outils de gestion de projet : JIRA, Trello, tableaux et indicateurs
- Suivi de l'avancement et gestion des ajustements
- Communication avec les parties prenantes, y compris en situation de handicap
- Animation d'équipe, gestion des tensions et qualité des livrables

Fil rouge · Léa organise le projet en sprints de deux semaines, anime les revues avec les cliniques et adapte les supports pour un collaborateur malentendant.

Cours 19 · Gestion budgétaire et pilotage financier du projet

22 h

OBJECTIFS

- Construire et suivre le budget d'un projet d'infrastructure
- Appliquer les techniques de répartition des coûts et d'analyse de la valeur acquise

ÉVALUATION FORMATIVE

Exercice pratique : tableau de suivi budgétaire et note d'arbitrage

CONTENUS

- Estimation des charges et des coûts d'un projet d'infrastructure
- Investissements et coûts récurrents, coût total de possession
- Construction du budget avec un tableur ou un outil de planification
- Répartition des coûts et suivi des engagements
- Analyse de la valeur acquise et indicateurs d'écart
- Arbitrages entre coûts, délais et périmètre
- Reporting financier au comité de pilotage

Fil rouge · À mi-parcours, le projet présente un dépassement sur le lot stockage : Léa calcule les indicateurs de valeur acquise et propose des arbitrages au comité de pilotage.

Cours 20 · Veille technologique et réglementaire multilingue

22 h

OBJECTIFS

- Mettre en place une veille multilingue fiable et l'organiser en base de connaissances
- Analyser les informations collectées, formuler des scénarios et les diffuser à l'équipe IT

ÉVALUATION FORMATIVE

Mise en situation : rapport de veille multilingue et présentation orale

CONTENUS

- Analyse de sources techniques anglophones pour résoudre un incident
- Identification et qualification de sources multilingues
- Vérification de la fiabilité et de la véracité des informations
- Outils de collecte avancés : flux, alertes, agrégateurs
- Structuration d'une base de connaissances technologiques
- Analyse comparative et construction de scénarios d'évolution
- Diffusion par outils collaboratifs et choix de la fréquence
- Rédaction et présentation orale d'un rapport de veille

Fil rouge · Léa crée la cellule de veille de la DSI, analyse des bulletins de sécurité en anglais et présente chaque mois des scénarios d'évolution de l'infrastructure à l'équipe.

05 · CONFORMITÉ AU RÉFÉRENTIEL

Couverture des compétences

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

Compétence	Bloc	Cours
Administrer et optimiser les systèmes Unix, Linux et Windows (QoS)	RNCP39611BC01	1
Concevoir des topologies systèmes à l'aide d'un annuaire	RNCP39611BC01	2, 15
Concevoir et déployer des environnements virtualisés on-premise ou cloud	RNCP39611BC01	3
Concevoir et administrer des bases de données relationnelles et NoSQL	RNCP39611BC01	4
Mettre en œuvre redondance, réplication et clustering	RNCP39611BC01	5
Surveiller et optimiser les performances des systèmes	RNCP39611BC01	5, 9
Manager la gestion des incidents par ticketing selon les SLA	RNCP39611BC01	6, 16
Automatiser les tâches d'administration en Python, Shell et Bash	RNCP39611BC01	6, 11
Configurer l'infrastructure réseau	RNCP39611BC02	7
Déployer les solutions de télécommunications, données et voix	RNCP39611BC02	8
Superviser et maintenir le réseau	RNCP39611BC02	9
Développer des environnements conteneurisés	RNCP39611BC02	10
Orchestrer les conteneurs au sein de pipelines CI/CD	RNCP39611BC02	10, 11
Intégrer la sécurité dans les processus DevOps sur le cloud	RNCP39611BC02	11
Développer et mettre en œuvre des politiques de sécurité à partir de l'analyse de risques	RNCP39611BC03	12
Conduire des audits de sécurité réguliers	RNCP39611BC03	12, 13
Élaborer et mettre en œuvre des actions correctives	RNCP39611BC03	13
Implémenter pare-feux et IDS/IPS	RNCP39611BC03	14
Administrer l'IAM avec MFA en tenant compte du handicap	RNCP39611BC03	15
Superviser sauvegardes, restaurations et plans de reprise après sinistre	RNCP39611BC03	16, 4
Assurer le support des incidents IT selon les RTO et RPO du PRA	RNCP39611BC03	16
Assurer la conformité au RGPD	RNCP39611BC03	13
Analyser les besoins et les traduire en exigences par une étude de faisabilité	RNCP39611BC04	17
Rédiger des documents de spécification technique	RNCP39611BC04	17
Orchestrer et animer des projets en méthodes agiles, y compris avec des parties prenantes en situation de handicap	RNCP39611BC04	18

Optimiser la gestion de projet avec JIRA ou Trello	RNCP39611BC04	18
Gérer le budget de projet et l'analyse de la valeur acquise	RNCP39611BC04	19
Analyser des sources spécialisées en anglais pour soutenir le SI	RNCP39611BC04	20, 6
Mettre en place une veille technologique et réglementaire multilingue	RNCP39611BC04	20
Analyser la base de connaissances et établir des scénarios d'évolution	RNCP39611BC04	20
Diffuser les scénarios à l'équipe IT avec des outils collaboratifs	RNCP39611BC04	20

Évaluations formatives

Chaque sous-chapitre se conclut par un QCM de validation des acquis, et chaque cours propose une évaluation formative en lien direct avec la mise en situation du fil rouge : étude de cas, exercice de conception, travaux pratiques ou production d'un livrable professionnel (rapport, topologie, script, plan, budget). Les résultats sont tracés sur la plateforme, ce qui permet à l'organisme de formation de suivre la progression de chaque apprenant, d'identifier les difficultés et de programmer des actions de remédiation avec le formateur référent. Un positionnement initial et une évaluation de fin de bloc complètent ce dispositif, conformément aux exigences Qualiopi en matière d'évaluation des acquis.

Modalités de certification

Bloc	Modalité d'évaluation
RNCP39611BC01	Mise en situation reconstituée : réalisation d'un dossier d'architecture technique et mise en place de la solution correspondante. Mise en situation reconstituée : analyse d'une architecture et de son PCA afin de proposer des améliorations et des outils de monitoring adaptés, formalisée dans un compte-rendu d'amélioration de l'architecture.
RNCP39611BC02	Mise en situation reconstituée à travers une étude de cas : production d'un dossier technique de la solution (topologie, fiches de test, etc.) et mise en service de la solution. Mise en situation reconstituée individuelle : mise en place d'un système d'automatisation de l'intégration et du déploiement continus.
RNCP39611BC03	Mise en situation reconstituée : rédaction d'un rapport d'analyse et de préconisations. Mise en situation reconstituée : à partir d'une étude de cas d'infrastructure réseau d'entreprise, proposition d'un rapport d'analyse et de préconisations d'amélioration de l'existant. Mise en situation reconstituée : mise en place d'un plan de sauvegarde à partir de l'étude de cas.
RNCP39611BC04	Mise en situation reconstituée : rédaction d'une étude d'avant-projet. Mise en situation professionnelle reconstituée : compte rendu d'activité (livrables collectifs) et soutenance individuelle. Mise en situation reconstituée : rédaction d'un rapport de veille multilingue et présentation orale de ce rapport.

Le parcours reproduit la logique des épreuves : chaque livrable attendu par le certificateur (dossier d'architecture, compte-rendu d'amélioration du PCA, dossier technique réseau, pipeline CI/CD, rapport d'analyse et de préconisations, plan de sauvegarde, étude d'avant-projet, compte rendu d'activité, rapport de veille multilingue) est travaillé au moins une fois dans les évaluations formatives, à partir de l'étude de cas Ardenvia Santé. Les apprenants disposent de modèles de livrables, de grilles d'auto-évaluation alignées sur les compétences du référentiel et d'entraînements à la soutenance orale. SFM fournit le contenu pédagogique ; l'organisme de formation reste responsable de l'inscription, de l'organisation et du déroulement de la certification auprès du certificateur.

Moyens pédagogiques et débouchés

Moyens pédagogiques et techniques

- Plateforme e-learning accessible 24 h/24 avec suivi de progression, traçabilité des connexions et des résultats
- Une vidéo de 3 à 5 minutes par sous-chapitre, représentant 30 % du volume horaire du parcours
- Cours texte enrichi, infographies, fiches de synthèse et glossaire technique français-anglais
- Études de cas et mises en situation professionnelles construites autour du fil rouge Ardenvia Santé
- Énoncés de travaux pratiques transposables sur un environnement de laboratoire virtualisé fourni par l'OF
- QCM de validation par sous-chapitre et grilles d'auto-évaluation alignées sur le référentiel
- Modèles de livrables professionnels : dossier d'architecture, PSSI, PRA, étude d'avant-projet, rapport de veille

Débouchés et évolutions

- Administrateur systèmes et réseaux (et sécurité)
- Administrateur systèmes (et sécurité)
- Administrateur réseaux (et sécurité)
- Administrateur d'infrastructures et cloud
- Administrateur cybersécurité
- Responsable infrastructure systèmes et réseaux

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 RNCP39611 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.