

SCHOOL FOR MATE

LIVRET PÉDAGOGIQUE

Administrateur d'infrastructures sécurisées

RNCP37680 · Titre professionnel · Niveau 6

Ce parcours de 550 heures prépare au titre professionnel Administrateur d'infrastructures sécurisées (RNCP37680, niveau 6) en couvrant intégralement ses trois blocs de compétences : administration et sécurisation des infrastructures, conception et mise en production d'évolutions, participation à la gestion de la cybersécurité. Construit autour d'un fil rouge professionnel continu, il fait progresser l'apprenant de l'administration courante jusqu'au traitement d'incidents de sécurité, avec une préparation ciblée aux épreuves du titre.

VOLUME HORAIRE	COURS	BLOCS
550 h	25	3

01 · PRÉSENTATION

La formation en bref

Intitulé	Administrateur d'infrastructures sécurisées
Code	RNCP37680
Type	Titre professionnel
Niveau	Niveau 6
Certificateur	MINISTERE DU TRAVAIL DU PLEIN EMPLOI ET DE L' INSERTION
Durée	550 h, 25 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	28/02/2027

Le métier et les compétences visées

L'administrateur d'infrastructures sécurisées met en œuvre, administre et sécurise les réseaux, les serveurs, les services d'infrastructure, les plateformes de virtualisation et les ressources de cloud public. Responsable du maintien en condition opérationnelle (MCO) et du maintien en condition de sécurité (MCS), il assure un support de niveau 2 et 3, conçoit des solutions répondant aux besoins d'évolution, les teste, les présente aux décideurs puis les met en production en s'assurant que les plans de reprise et de continuité informatique sont validés. Il déploie la supervision, analyse les risques, conduit des audits internes, contribue à la politique de sécurité, sensibilise les utilisateurs et réagit aux incidents. Il travaille en équipe, peut piloter des techniciens et exploite une documentation technique en anglais (niveau B1).

Public visé

- Techniciens supérieurs systèmes et réseaux souhaitant évoluer vers un poste d'administrateur de niveau 6
- Administrateurs systèmes ou réseaux en poste désirant formaliser et certifier leurs compétences en sécurité
- Personnes en reconversion disposant d'une première expérience technique en informatique
- Alternants en contrat d'apprentissage ou de professionnalisation au sein d'une DSI ou d'une ESN
- Salariés engagés dans un projet de VAE ou de certification par blocs de compétences

Prérequis

- Le référentiel ne fixe pas de prérequis officiel : l'OF reste libre de définir ses conditions d'admission
- Maîtrise recommandée des fondamentaux des réseaux (modèle OSI, adressage IP) et de l'administration d'un poste de travail
- Expérience conseillée en support ou en exploitation informatique, ou diplôme de niveau 5 dans le domaine
- Niveau d'anglais permettant de lire une documentation technique, en vue d'atteindre le niveau B1 du CECRL attendu par le métier

Objectifs pédagogiques

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

- Appliquer les bonnes pratiques d'exploitation (documentation, gestion des changements, gestion des incidents) dans l'administration des infrastructures
- Administrer et sécuriser les équipements actifs du réseau : commutation, routage, filtrage, accès distants
- Administrer et durcir des serveurs Windows et Linux ainsi que les services d'infrastructure associés
- Déployer et sécuriser des plateformes de virtualisation et des ressources de cloud public
- Concevoir une solution technique répondant à un besoin d'évolution, la tester selon des critères définis et la présenter aux décideurs
- Planifier et réaliser une mise en production en vérifiant la validité des plans de reprise et de continuité informatique
- Mettre en œuvre une supervision des infrastructures et définir indicateurs et tableaux de suivi de performance et de disponibilité
- Mesurer le niveau de sécurité d'une infrastructure par l'analyse de risques, l'audit interne et la gestion des vulnérabilités
- Contribuer à l'élaboration et au déploiement de la politique de sécurité, y compris la sensibilisation des utilisateurs
- Détecter, qualifier et traiter des incidents de sécurité, puis adapter les règles de détection en fonction de la veille

02 · FIL ROUGE PÉDAGOGIQUE

Norvalis Logistique

KD

Karim Delorme

Administrateur d'infrastructures sécurisées au sein de la DSI, rattaché au RSI et en lien étroit avec la RSSI

Transport et logistique (entreprise de taille intermédiaire, 1 200 salariés, 14 plateformes régionales)

Norvalis Logistique exploite des entrepôts répartis sur le territoire, un datacenter principal à Orléans et une salle de secours à Tours. Après une forte croissance, son système d'information est devenu hétérogène : réseau peu segmenté, serveurs vieillissants, cluster de virtualisation saturé et premiers usages de cloud public mal maîtrisés. Une tentative d'hameçonnage ayant visé le service comptable a convaincu la direction d'investir dans la sécurité. Karim Delorme rejoint la DSI, dirigée par Sophie Marchetti, pour fiabiliser l'existant, accompagner le projet de modernisation baptisé « Horizon » et contribuer, aux côtés de la RSSI Élodie Vasseur, à structurer la cybersécurité. Il encadre deux techniciens de proximité et travaille avec un prestataire d'infogérance, ce qui l'oblige à documenter, communiquer et arbitrer en permanence.

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

La progression

1. Bloc 1 : Karim reprend en main l'infrastructure existante, documente le parc, segmente le réseau, durcit les serveurs Windows et Linux, sécurise le cluster de virtualisation et encadre les premiers usages du cloud public.
2. Bloc 2 : Karim conduit le projet « Horizon » de modernisation, de l'expression du besoin à la mise en production, en passant par la maquette de test, la présentation au comité de direction, la validation du PRI et du PCI et le déploiement d'une supervision unifiée.
3. Bloc 3 : Karim participe avec la RSSI à l'analyse de risques et à l'audit interne, contribue à la PSSI, anime la sensibilisation des équipes d'entrepôt, puis met en place la détection et gère un incident de rançongiciel sur une plateforme 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
RNCP37680BC01 · Administrer et sécuriser les infrastructures		**220 h**
1	Bonnes pratiques d'exploitation et maintien en condition opérationnelle	22 h
2	Anglais technique et communication professionnelle de l'administrateur	22 h
3	Architecture réseau et commutation sécurisée	22 h
4	Routage, filtrage et pare-feu	22 h
5	Accès distants, interconnexions et réseaux sans fil sécurisés	22 h
6	Administration et sécurisation des serveurs Windows et de l'annuaire	22 h
7	Administration et sécurisation des serveurs Linux	22 h
8	Services d'infrastructure sécurisés	22 h
9	Virtualisation et hyperviseurs sécurisés	22 h
10	Cloud public, conteneurs et automatisation de l'infrastructure	22 h
RNCP37680BC02 · Concevoir et mettre en œuvre une solution en réponse à un besoin d'évolution		**154 h**
11	Analyse du besoin et conception d'une solution technique	22 h
12	Critères d'évaluation, maquettage et présentation aux décideurs	22 h
13	Planification et pilotage d'un projet d'infrastructure	22 h
14	Sauvegarde, plan de reprise et plan de continuité informatique	22 h
15	Mise en production et industrialisation des déploiements	22 h
16	Mise en œuvre de la supervision des infrastructures	22 h
17	Tableaux de suivi, niveaux de service et optimisation de la supervision	22 h
RNCP37680BC03 · Participer à la gestion de la cybersécurité		**176 h**
18	Panorama des menaces et cadre de la cybersécurité	22 h
19	Analyse de risques de l'infrastructure	22 h
20	Audit de sécurité interne et gestion des vulnérabilités	22 h
21	Politique de sécurité et mesures de sécurisation	22 h
22	Gestion des identités, des accès et sensibilisation des utilisateurs	22 h

23	Détection des événements de sécurité	22 h
24	Traitement des incidents de sécurité	22 h
25	Veille sur les menaces et projet de synthèse	22 h
Total du parcours		**550 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 : 165 h
- Cours texte et infographies : 173 h
- Études de cas et mises en situation : 135 h
- QCM et évaluations : 77 h

04 · PROGRAMME DÉTAILLÉ

Contenu des cours

RNCP37680BC01 · 220 h

Administrer et sécuriser les infrastructures

Cours 1 · Bonnes pratiques d'exploitation et maintien en condition opérationnelle

22 h

OBJECTIFS

- Organiser l'exploitation d'une infrastructure selon les processus de gestion des services (incidents, problèmes, changements)
- Produire et maintenir une documentation d'exploitation fiable et exploitable par une équipe

ÉVALUATION FORMATIVE

QCM de validation et étude de cas : rédaction d'une procédure de gestion de changement et d'une fiche de diagnostic

CONTENUS

- Rôle de l'administrateur : MCO, MCS, périmètre de délégation et interlocuteurs
- Processus de gestion des services informatiques : incidents, problèmes, changements, configuration
- Support de niveau 2 et 3 : diagnostic méthodique, escalade, base de connaissances
- Inventaire du parc et base de données de configuration
- Documentation d'exploitation : procédures, schémas, fiches d'intervention
- Planification de la maintenance et pilotage des interventions des techniciens
- Respect des normes et politiques de sécurité dans les tâches courantes

Fil rouge · Dès son arrivée chez Norvalis Logistique, Karim découvre un parc sans inventaire à jour : il bâtit la cartographie de l'existant, formalise le circuit de traitement des tickets et répartit les interventions entre ses deux techniciens.

Cours 2 · Anglais technique et communication professionnelle de l'administrateur

22 h

OBJECTIFS

- Comprendre une documentation technique et des échanges de support rédigés en anglais (niveau B1)
- Rédiger en anglais des réponses courtes et précises sur un sujet technique
- Adapter sa communication écrite et orale à des interlocuteurs techniques et non techniques

ÉVALUATION FORMATIVE

Exercice d'entraînement au format du questionnaire professionnel : documentation en anglais, questions fermées en français et questions ouvertes en anglais

CONTENUS

- Vocabulaire anglais des réseaux, systèmes, virtualisation et sécurité
- Lecture structurée d'une documentation constructeur ou d'un bulletin de sécurité
- Rédaction en anglais : ticket de support, réponse courte, compte rendu d'incident
- Utiliser forums techniques et services support anglophones
- Communication écrite : courriel, note technique, compte rendu d'intervention
- Communication orale : expliquer un incident à un utilisateur, rendre compte au RSI

Fil rouge · Karim doit ouvrir un ticket en anglais auprès du support d'un éditeur pour un dysfonctionnement de commutateur, puis expliquer simplement l'impact de l'intervention au responsable d'un entrepôt.

Cours 3 · Architecture réseau et commutation sécurisée

22 h

OBJECTIFS

- Concevoir et administrer un réseau local segmenté
- Sécuriser la couche d'accès et la commutation contre les attaques courantes

ÉVALUATION FORMATIVE

Travaux pratiques guidés sur environnement simulé et QCM de validation

CONTENUS

- Rappels d'architecture : modèle hiérarchique, adressage IPv4 et IPv6, plan d'adressage
- VLAN, trunking et segmentation des usages (bureautique, entrepôt, serveurs, administration)
- Protocoles de redondance de niveau 2 et prévention des boucles
- Sécurisation des ports : contrôle d'accès 802.1X, sécurité des ports, protections DHCP et ARP
- Administration sécurisée des équipements : SSH, comptes nominatifs, réseau d'administration dédié
- Sauvegarde et gestion de version des configurations réseau

Fil rouge · Le réseau de la plateforme de Tours mélange postes de bureau, terminaux de préparation de commandes et caméras dans un seul segment : Karim conçoit et déploie un nouveau plan de VLAN avec contrôle d'accès des équipements.

Cours 4 · Routage, filtrage et pare-feu

22 h

OBJECTIFS

- Configurer le routage statique et dynamique entre sites
- Définir et appliquer une politique de filtrage cohérente sur les pare-feu

ÉVALUATION FORMATIVE

Étude de cas : analyse d'une matrice de flux et rédaction des règles corrigées, QCM

CONTENUS

- Routage statique et protocoles de routage dynamique
- Routage inter-VLAN et architecture multi-sites
- Listes de contrôle d'accès et principe du moindre privilège réseau
- Pare-feu à états : zones, DMZ, règles, traduction d'adresses
- Revue et nettoyage d'une matrice de flux
- Journalisation des flux et lecture des logs de pare-feu

Fil rouge · Karim découvre que les règles du pare-feu du datacenter autorisent des flux trop larges vers les serveurs de gestion d'entrepôt : il établit une matrice de flux et propose un plan de réduction des règles validé par la RSSI.

Cours 5 · Accès distants, interconnexions et réseaux sans fil sécurisés

22 h

OBJECTIFS

- Mettre en œuvre des interconnexions et des accès distants chiffrés
- Sécuriser un réseau sans fil d'entreprise

ÉVALUATION FORMATIVE

Mise en situation pratique sur maquette et quiz de validation

CONTENUS

- Principes cryptographiques appliqués aux réseaux : chiffrement, intégrité, authentification
- VPN site à site entre plateformes et datacenter
- VPN d'accès nomade et authentification multifacteur
- Wi-Fi d'entreprise : authentification centralisée, séparation des réseaux invités et métiers
- Proxy, filtrage web et sécurisation des accès sortants
- Diagnostic des problèmes de connectivité distante

Fil rouge · Les commerciaux itinérants de Norvalis se connectent encore via un accès distant non chiffré : Karim met en place un VPN nomade avec authentification forte et sécurise le Wi-Fi des quais de chargement.

Cours 6 · Administration et sécurisation des serveurs Windows et de l'annuaire

22 h

OBJECTIFS

- Administrer un domaine d'annuaire et ses stratégies de groupe
- Durcir des serveurs Windows selon des recommandations reconnues

ÉVALUATION FORMATIVE

Travaux pratiques et étude de cas sur un audit simplifié d'annuaire, QCM

CONTENUS

- Installation et rôles d'un serveur Windows
- Services d'annuaire : structure, comptes, groupes, délégation
- Stratégies de groupe pour la configuration et la sécurité des postes et serveurs
- Modèle d'administration par niveaux et protection des comptes à privilèges
- Durcissement : services, correctifs, journalisation, protection des identifiants
- Automatisation des tâches d'administration par scripts PowerShell

Fil rouge · Karim constate que de nombreux comptes de service disposent de droits d'administration du domaine : il restructure l'annuaire, sépare les comptes d'administration et déploie des stratégies de durcissement.

Cours 7 · Administration et sécurisation des serveurs Linux

22 h

OBJECTIFS

- Administrer des serveurs Linux en ligne de commande
- Appliquer des mesures de durcissement et d'automatisation sur des serveurs Linux

ÉVALUATION FORMATIVE

Travaux pratiques notés automatiquement et QCM de validation

CONTENUS

- Installation, arborescence, gestion des paquets et des services
- Gestion des utilisateurs, des droits et de l'élévation de privilèges
- Accès SSH sécurisé par clés et restrictions d'accès
- Pare-feu local, journalisation et rotation des logs
- Durcissement : réduction de la surface d'attaque, mises à jour, contrôle d'intégrité
- Scripts Bash et automatisation de la configuration

Fil rouge · Le serveur d'échange de données avec les transporteurs partenaires tourne sur un Linux jamais mis à jour : Karim planifie sa remise à niveau, sécurise ses accès et automatise sa configuration.

Cours 8 · Services d'infrastructure sécurisés

22 h

OBJECTIFS

- Déployer et sécuriser les services d'infrastructure essentiels
- Mettre en place une infrastructure de gestion de certificats

ÉVALUATION FORMATIVE

Étude de cas et travaux pratiques, QCM

CONTENUS

- DNS : architecture interne et externe, sécurisation, diagnostic
- DHCP : haute disponibilité et protections associées
- Infrastructure de gestion de clés et cycle de vie des certificats
- Partage de fichiers, droits d'accès et traçabilité
- Service de messagerie : protections contre l'usurpation et l'hameçonnage
- Gestion des correctifs et des mises à jour à l'échelle du parc

Fil rouge · Suite à la tentative d'hameçonnage du service comptable, Karim renforce les mécanismes d'authentification des courriels et met en place une autorité de certification interne pour les services web internes.

Cours 9 · Virtualisation et hyperviseurs sécurisés

22 h

OBJECTIFS

- Administrer une plateforme de virtualisation en cluster
- Sécuriser les hyperviseurs, le stockage et les réseaux virtuels

ÉVALUATION FORMATIVE

Mise en situation pratique sur laboratoire virtuel et QCM

CONTENUS

- Principes de la virtualisation et types d'hyperviseurs
- Cluster, haute disponibilité et migration de machines virtuelles
- Stockage partagé : protocoles, performances et redondance
- Réseaux virtuels et segmentation des flux de gestion
- Sécurisation de l'hyperviseur et de la console d'administration
- Gestion de capacité et plan de charge de la plateforme

Fil rouge · Le cluster de virtualisation du datacenter d'Orléans arrive à saturation et sa console d'administration est accessible depuis le réseau bureautique : Karim isole les flux de gestion et établit un plan de capacité.

Cours 10 · Cloud public, conteneurs et automatisation de l'infrastructure

22 h

OBJECTIFS

- Administrer et sécuriser des ressources de cloud public
- Déployer des conteneurs et automatiser la configuration de l'infrastructure

ÉVALUATION FORMATIVE

Travaux pratiques et étude de cas sur la sécurisation d'un environnement cloud, QCM

CONTENUS

- Modèles de services cloud et responsabilité partagée
- Identités et accès dans le cloud : rôles, moindre privilège, authentification forte
- Réseaux virtuels cloud, groupes de sécurité et connexion hybride
- Conteneurs : principes, images, sécurisation, orchestration
- Infrastructure en tant que code et gestion de configuration
- Maîtrise des coûts et gouvernance des ressources cloud

Fil rouge · Le service marketing a ouvert un abonnement cloud sans contrôle de la DSI : Karim reprend la gouvernance, restreint les droits et déploie la nouvelle application de suivi des colis en conteneurs.

RNCP37680BC02 · 154 h

Concevoir et mettre en œuvre une solution en réponse à un besoin d'évolution

Cours 11 · Analyse du besoin et conception d'une solution technique

22 h

OBJECTIFS

- Recueillir et formaliser un besoin d'évolution de l'infrastructure
- Concevoir une architecture cible et comparer plusieurs scénarios

ÉVALUATION FORMATIVE

Étude de cas : production d'un dossier de conception à partir d'un cahier des besoins

CONTENUS

- Recueil du besoin auprès des métiers et de la direction
- Analyse de l'existant et identification des contraintes techniques, financières et réglementaires
- Exigences de sécurité intégrées dès la conception
- Élaboration de scénarios d'architecture
- Étude comparative de solutions et sollicitation des fournisseurs
- Rédaction d'un dossier de conception technique

Fil rouge · La direction de Norvalis lance le projet « Horizon » pour accueillir trois nouvelles plateformes : Karim conduit les entretiens avec les métiers et rédige deux scénarios d'architecture, sur site et hybride.

Cours 12 · Critères d'évaluation, maquettage et présentation aux décideurs

22 h

OBJECTIFS

- Définir des critères d'évaluation et monter un environnement de test
- Présenter et argumenter la solution retenue auprès des décideurs

ÉVALUATION FORMATIVE

Soutenance simulée avec diaporama et grille d'évaluation, préparant à l'épreuve de présentation de projet

CONTENUS

- Définition de critères d'évaluation techniques, économiques et de sécurité
- Construction d'une maquette ou preuve de concept
- Protocole de tests et recette technique
- Analyse des résultats et grille de décision
- Estimation des coûts et du retour sur investissement
- Construction d'un support de présentation et soutenance devant un comité

Fil rouge · Karim monte une maquette des deux scénarios d'« Horizon », mesure leurs performances, puis présente la solution retenue au comité de direction présidé par la DSI Sophie Marchetti.

Cours 13 · Planification et pilotage d'un projet d'infrastructure

22 h

OBJECTIFS

- Planifier l'intégration d'une solution dans l'environnement de production
- Coordonner les acteurs internes et les prestataires du projet

ÉVALUATION FORMATIVE

Étude de cas : élaboration d'un planning de mise en production et d'un plan de retour arrière, QCM

CONTENUS

- Découpage du projet en lots et planification
- Gestion des risques projet et plan de retour arrière
- Coordination des techniciens, prestataires et fournisseurs
- Gestion du changement : comité de changement, fenêtres d'intervention
- Communication projet auprès des utilisateurs
- Suivi d'avancement et reporting

Fil rouge · Karim établit le planning de migration d'« Horizon » en tenant compte des pics d'activité logistique de fin d'année et organise les interventions avec le prestataire d'infogérance.

Cours 14 · Sauvegarde, plan de reprise et plan de continuité informatique

22 h

OBJECTIFS

- Concevoir une stratégie de sauvegarde adaptée aux besoins de l'entreprise
- Tester et valider les plans de reprise et de continuité informatique

ÉVALUATION FORMATIVE

Mise en situation : conduite d'un exercice de reprise simulé et rédaction du rapport de test

CONTENUS

- Analyse d'impact et objectifs de durée et de perte de données maximales admissibles
- Stratégies de sauvegarde, externalisation et sauvegardes protégées contre l'altération
- Réplication et site de secours
- Rédaction du PRI et du PCI
- Organisation et conduite d'un test de reprise
- Retour d'expérience et mise à jour des plans

Fil rouge · Avant la bascule d'« Horizon », Karim organise un test de reprise sur la salle de secours de Tours et constate qu'une application critique ne redémarre pas : il corrige la procédure et fait valider le PRI.

Cours 15 · Mise en production et industrialisation des déploiements

22 h

OBJECTIFS

- Mettre en production une évolution de l'infrastructure en maîtrisant les risques
- Industrialiser les déploiements par l'automatisation

ÉVALUATION FORMATIVE

Étude de cas sur un déroulé de mise en production et QCM de validation

CONTENUS

- Préparation de la mise en production : prérequis, contrôles, validation
- Migration de services et de données
- Déploiement automatisé et gestion de configuration
- Recette de production et vérification de non-régression
- Documentation de l'infrastructure livrée et transfert aux équipes d'exploitation
- Bilan de projet et capitalisation

Fil rouge · Karim pilote la bascule des services d'« Horizon » pendant une fenêtre de nuit, vérifie la recette avec les chefs de plateforme et transmet la documentation au support.

Cours 16 · Mise en œuvre de la supervision des infrastructures

22 h

OBJECTIFS

- Déployer une solution de supervision couvrant réseaux, systèmes et services
- Choisir les indicateurs et événements pertinents à superviser

ÉVALUATION FORMATIVE

Travaux pratiques sur laboratoire de supervision et QCM

CONTENUS

- Principes de la supervision et de la métrologie
- Protocoles et agents de collecte
- Déploiement d'une solution de supervision et découverte des équipements
- Choix des indicateurs et des événements à surveiller
- Seuils, alertes et gestion des notifications
- Supervision des environnements virtualisés et cloud

Fil rouge · Les pannes à Norvalis sont aujourd'hui signalées par les utilisateurs : Karim déploie une supervision unifiée couvrant le datacenter, les plateformes et les ressources cloud d'« Horizon ».

Cours 17 · Tableaux de suivi, niveaux de service et optimisation de la supervision

22 h

OBJECTIFS

- Définir des tableaux de suivi de la performance et de la disponibilité
- Optimiser la supervision et en exploiter les résultats

ÉVALUATION FORMATIVE

Étude de cas : conception d'un tableau de bord et d'un rapport de niveaux de service

CONTENUS

- Niveaux de service : engagements, indicateurs de disponibilité et de performance
- Conception de tableaux de bord adaptés aux différents interlocuteurs
- Réduction du bruit d'alerte et corrélation d'événements
- Analyse de tendances et anticipation de la capacité
- Automatisation des réactions aux alertes
- Reporting mensuel à la direction

Fil rouge · Trois mois après la mise en production, l'équipe reçoit trop d'alertes inutiles : Karim révise les seuils, construit un tableau de bord de disponibilité pour la DSI et présente le premier rapport mensuel.

Participer à la gestion de la cybersécurité

Cours 18 · Panorama des menaces et cadre de la cybersécurité

22 h

OBJECTIFS

- Identifier les principales menaces et modes opératoires des attaquants
- Situer son action dans le cadre réglementaire et organisationnel de la sécurité

ÉVALUATION FORMATIVE

QCM de validation et analyse d'un scénario d'attaque documenté

CONTENUS

- Notions de disponibilité, intégrité, confidentialité et traçabilité
- Typologie des menaces : rançongiciels, hameçonnage, compromission de comptes, attaques sur la chaîne d'approvisionnement
- Lecture des modes opératoires d'attaque et matrices de tactiques et techniques
- Cadre réglementaire : protection des données personnelles, directives européennes sur la sécurité des réseaux
- Référentiels et guides des autorités nationales de cybersécurité
- Organisation de la sécurité : rôle de la RSSI, de l'administrateur et des prestataires

Fil rouge · La RSSI Élodie Vasseur associe Karim à la préparation d'une note sur l'exposition de Norvalis aux menaces visant le secteur logistique, destinée au comité de direction.

Cours 19 · Analyse de risques de l'infrastructure

22 h

OBJECTIFS

- Participer à une analyse de risques selon une méthode reconnue
- Proposer des mesures de traitement des risques adaptées

ÉVALUATION FORMATIVE

Étude de cas : réalisation d'une analyse de risques simplifiée sur un périmètre fourni

CONTENUS

- Principes de l'analyse de risques et vocabulaire associé
- Méthodes d'analyse de risques et démarche par scénarios
- Identification des biens essentiels et des biens supports
- Évaluation de la vraisemblance et de la gravité
- Plan de traitement des risques et risques résiduels
- Restitution des résultats aux décideurs

Fil rouge · Karim participe aux ateliers d'analyse de risques de Norvalis et identifie le système de gestion d'entrepôt comme bien support critique, puis propose avec la RSSI des mesures de réduction.

Cours 20 · Audit de sécurité interne et gestion des vulnérabilités

22 h

OBJECTIFS

- Réaliser un audit de sécurité interne de configuration et d'architecture
- Mettre en place un processus de gestion des vulnérabilités

ÉVALUATION FORMATIVE

Travaux pratiques sur environnement vulnérable de laboratoire et rédaction d'un rapport d'audit

CONTENUS

- Types d'audits et cadre d'intervention autorisé
- Audit de configuration et comparaison aux référentiels de durcissement
- Scanners de vulnérabilités : usage, interprétation, faux positifs
- Évaluation de la criticité et priorisation des corrections
- Suivi des bulletins de sécurité et des vulnérabilités publiées
- Rapport d'audit et plan de remédiation

Fil rouge · Karim conduit le premier scan de vulnérabilités du périmètre « Horizon », trie les résultats, priorise les corrections et rédige un plan de remédiation partagé avec le prestataire d'infogérance.

Cours 21 · Politique de sécurité et mesures de sécurisation

22 h

OBJECTIFS

- Contribuer à l'élaboration d'une politique de sécurité du système d'information
- Participer au choix et à la mise en œuvre de solutions de sécurisation

ÉVALUATION FORMATIVE

Étude de cas : rédaction de règles opérationnelles et grille de comparaison de solutions

CONTENUS

- Structure d'une politique de sécurité et déclinaison en règles opérationnelles
- Charte informatique et règles d'usage
- Choix de solutions de sécurisation : protection des postes, filtrage, chiffrement
- Sécurisation des postes de travail et des terminaux mobiles
- Gestion de la sécurité des prestataires et des tiers
- Contrôle d'application et indicateurs de conformité

Fil rouge · Élodie Vasseur confie à Karim la rédaction des chapitres techniques de la nouvelle politique de sécurité de Norvalis et l'évaluation de solutions de protection des postes de travail.

Cours 22 · Gestion des identités, des accès et sensibilisation des utilisateurs

22 h

OBJECTIFS

- Mettre en œuvre une gestion des identités et des accès maîtrisée
- Concevoir et animer des actions de sensibilisation et de formation à la cybersécurité

ÉVALUATION FORMATIVE

Mise en situation : conception d'un support de sensibilisation et présentation orale simulée

CONTENUS

- Cycle de vie des identités : arrivées, mobilités, départs
- Authentification multifacteur et gestion des mots de passe
- Gestion des comptes à privilèges et revue des habilitations
- Conception d'une campagne de sensibilisation adaptée aux publics
- Exercices de simulation d'hameçonnage et exploitation des résultats
- Formation des équipes d'exploitation aux bonnes pratiques de sécurité

Fil rouge · Karim conçoit un module de sensibilisation court pour les équipes d'entrepôt, organise une simulation d'hameçonnage et forme les techniciens aux procédures d'administration sécurisée.

Cours 23 · Détection des événements de sécurité

22 h

OBJECTIFS

- Mettre en place des dispositifs de collecte et de détection d'événements de sécurité
- Rédiger et ajuster des règles de détection

ÉVALUATION FORMATIVE

Travaux pratiques sur plateforme de détection de laboratoire et QCM

CONTENUS

- Politique de journalisation : sources, conservation, horodatage
- Centralisation des journaux et plateforme de gestion des événements de sécurité
- Sondes de détection d'intrusion réseau et sur les hôtes
- Écriture de règles de détection et de corrélation
- Qualification des alertes et réduction des faux positifs
- Relation avec un centre opérationnel de sécurité interne ou externalisé

Fil rouge · Karim centralise les journaux des contrôleurs de domaine, pare-feu et serveurs d'« Horizon » et crée des règles détectant les connexions anormales sur les comptes d'administration.

Cours 24 · Traitement des incidents de sécurité

22 h

OBJECTIFS

- Appliquer les mesures de réaction appropriées lors d'un incident de sécurité
- Contribuer au retour d'expérience et à l'amélioration des dispositifs

ÉVALUATION FORMATIVE

Exercice de gestion de crise simulé avec production d'un rapport d'incident

CONTENUS

- Cycle de gestion d'incident : préparation, détection, confinement, éradication, rétablissement
- Procédures de réaction et fiches réflexes
- Préservation des traces et premières investigations techniques
- Communication de crise et obligations de notification
- Coordination avec la RSSI, la direction et les intervenants externes
- Retour d'expérience et plan d'amélioration

Fil rouge · Un rançongiciel chiffre les serveurs de la plateforme de Lyon : Karim isole le site, préserve les traces, restaure depuis les sauvegardes protégées et participe au retour d'expérience avec la cellule de crise.

Cours 25 · Veille sur les menaces et projet de synthèse

22 h

OBJECTIFS

- Organiser une veille sur les menaces et vulnérabilités et adapter les règles de détection
- Construire le dossier de projet et préparer la présentation devant le jury

ÉVALUATION FORMATIVE

Soutenance blanche du dossier de projet, entretien technique simulé et questionnaire professionnel blanc

CONTENUS

- Sources de veille, y compris anglophones, et organisation de la veille
- Exploitation des indicateurs de compromission et du renseignement sur la menace
- Adaptation des règles de détection et des procédures de gestion des incidents
- Structure du dossier de projet couvrant les trois blocs
- Préparation du diaporama et entraînement à la présentation de 20 minutes
- Entraînement à l'entretien technique et au questionnaire professionnel en anglais

Fil rouge · Après l'incident de Lyon, Karim met en place une veille hebdomadaire et ajuste les règles de détection, puis présente à la DSI le bilan complet de ses réalisations chez Norvalis, de la reprise de l'existant au projet « Horizon ».

05 · CONFORMITÉ AU RÉFÉRENTIEL

Couverture des compétences

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

Compétence	Bloc	Cours
Appliquer les bonnes pratiques dans l'administration des infrastructures	RNCP37680BC01	1, 2
Administrer et sécuriser les infrastructures réseaux	RNCP37680BC01	3, 4, 5
Administrer et sécuriser les infrastructures systèmes	RNCP37680BC01	6, 7, 8
Administrer et sécuriser les infrastructures virtualisées	RNCP37680BC01	9, 10
Concevoir une solution technique répondant à des besoins d'évolution de l'infrastructure	RNCP37680BC02	11, 12
Mettre en production des évolutions de l'infrastructure	RNCP37680BC02	13, 14, 15
Mettre en œuvre et optimiser la supervision des infrastructures	RNCP37680BC02	16, 17
Participer à la mesure et à l'analyse du niveau de sécurité de l'infrastructure	RNCP37680BC03	18, 19, 20
Participer à l'élaboration et à la mise en œuvre de la politique de sécurité	RNCP37680BC03	21, 22
Participer à la détection et au traitement des incidents de sécurité	RNCP37680BC03	23, 24, 25

Évaluations formatives

Chaque cours intègre des évaluations formatives régulières : QCM à la fin de chaque sous-chapitre pour vérifier la compréhension immédiate, travaux pratiques sur environnements de laboratoire, études de cas et mises en situation tirées du fil rouge Norvalis Logistique, avec corrigés commentés. Chaque sous-chapitre s'appuie sur une vidéo de 3 à 5 minutes, qui représente 30 % du volume horaire, complétée par du cours texte enrichi, des infographies et des activités pratiques. Des exercices au format du questionnaire professionnel (documentation technique en anglais) jalonnent le parcours. Les résultats permettent à l'apprenant de mesurer sa progression et à l'OF d'assurer le suivi individualisé et les remédiations nécessaires.

Modalités de certification

Bloc	Modalité d'évaluation
RNCP37680BC01	Épreuve d'une durée totale de 1 h 30 : présentation de 20 minutes d'un ou plusieurs projets réalisés en amont de la session, appuyée sur un dossier de projet (pris en connaissance par le jury sous forme imprimée avant la présentation) et un diaporama ; entretien technique de 40 minutes portant sur le dossier et la présentation, complété par un questionnement sur les compétences non couvertes par le ou les projets ; questionnaire professionnel de 30 minutes, passé en présence d'un surveillant, à partir d'une documentation technique en anglais, comprenant deux questions fermées à choix unique en français et deux questions ouvertes en anglais appelant des réponses courtes rédigées en anglais.
RNCP37680BC02	Épreuve d'une durée totale de 1 h 30 : présentation de 20 minutes d'un ou plusieurs projets réalisés en amont de la session, appuyée sur un dossier de projet (pris en connaissance par le

	jury sous forme imprimée avant la présentation) et un diaporama ; entretien technique de 40 minutes portant sur le dossier et la présentation, complété par un questionnement sur les compétences non couvertes par le ou les projets ; questionnaire professionnel de 30 minutes, passé en présence d'un surveillant, à partir d'une documentation technique en anglais, comprenant deux questions fermées à choix unique en français et deux questions ouvertes en anglais appelant des réponses courtes rédigées en anglais.
RNCP37680BC03	Épreuve d'une durée totale de 1 h 30 : présentation de 20 minutes d'un ou plusieurs projets réalisés en amont de la session, appuyée sur un dossier de projet (pris en connaissance par le jury sous forme imprimée avant la présentation) et un diaporama ; entretien technique de 40 minutes portant sur le dossier et la présentation, complété par un questionnement sur les compétences non couvertes par le ou les projets ; questionnaire professionnel de 30 minutes, passé en présence d'un surveillant, à partir d'une documentation technique en anglais, comprenant deux questions fermées à choix unique en français et deux questions ouvertes en anglais appelant des réponses courtes rédigées en anglais.

Le parcours prépare directement aux trois composantes de chaque épreuve. Les mises en situation du fil rouge produisent, cours après cours, des livrables réutilisables (procédures, dossier de conception, rapports de test, plan de remédiation, rapport d'incident) qui servent de matière au dossier de projet. Le cours 12 entraîne à la soutenance devant des décideurs et le cours 25 organise une soutenance blanche de 20 minutes suivie d'un entretien technique simulé de 40 minutes. Le cours 2 et les exercices répartis dans le parcours préparent au questionnaire professionnel sur documentation anglaise. L'organisme de formation reste responsable de l'inscription des candidats, de l'organisation des sessions d'examen 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, avec suivi de progression et traçabilité des activités
- Vidéos pédagogiques de 3 à 5 minutes par sous-chapitre, représentant 30 % du volume horaire
- Cours texte enrichi, infographies, schémas d'architecture et fiches de synthèse téléchargeables
- Études de cas et mises en situation fondées sur le fil rouge Norvalis Logistique
- Énoncés de travaux pratiques conçus pour des environnements de laboratoire virtualisés (réseau, systèmes, virtualisation, supervision, détection), à mettre à disposition par l'OF
- QCM de validation, exercices au format du questionnaire professionnel et modèles de dossier de projet et de diaporama
- Documentation technique en anglais sélectionnée pour l'entraînement à la compréhension et à l'expression écrite

Débouchés et évolutions

- Administrateur systèmes et réseaux (et sécurité)
- Administrateur systèmes (et sécurité) ou administrateur réseaux (et sécurité)
- Administrateur infrastructures
- 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 RNCP37680 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.