Devenir Administrateur·rice d'Infrastructures Sécurisées

MaCarrière

m2i Formation

En partenariat avec :

La Région Grand Est

Document mis à jour le 17/09/2025

Dispositif de formation :	**Programme Régional de Formation (PRF)**
Date de formation :	**Du 14 octobre 2024 au 27 juin 2025**
Période de stage :	**Du 19 mars au 19 juin 2025**
Lieu(x) de formation :	**Reims**
Réunion d'Information :	**Le 15 juillet 2024 ou le 29 août 2024**
Date limite d'envoi de candidature :	**Le 30 septembre 2024**

L'administrateur d'infrastructures sécurisées met en oeuvre, administre et sécurise les infrastructures informatiques locales et dans le cloud. Il conçoit et met en production des solutions répondant à des besoins d'évolution. Il implémente et optimise les dispositifs de supervision.

OBJECTIFS DE FORMATION

A l'issue de cette formation, vous serez capable de :

- Administrer et sécuriser les infrastructures
- Concevoir et mettre en oeuvre une solution en réponse à un besoin d'évolution
- Participer à la gestion de la cybersécurité

PRÉREQUIS

- Niveau 5 (Bac +2) en systèmes et réseaux (TSSR, BTS...) et/ou avoir l'expérience professionnelle et les connaissances équivalentes
- Esprit logique, curiosité technique, rigueur, bonne maitrise de la langue française, niveau A2 en anglais

PUBLIC CONCERNÉ ET FINANCEMENT

Cette formation financée à 100% par la Région Grand Est et le Fonds Social Européen est à destination des demandeur·se·s d'emploi inscrit·e·s à France Travail et résidant en Région Grand Est.

COMPÉTENCES ET TECHNOLOGIES ABORDÉES

Module	Contenu	Durée (heures)
Réseaux : Switching & Routing	Maitriser l'adressages IP v4 Calculer des adresses de réseau, des broadcasts, des sous réseaux à taille fixe Comprendre et mémoriser le modèle OSI, l'encapsulation Installer et utiliser Packet Tracer Comprendre et mettre en œuvre l'interconnexion de réseau et le fonctionnement des routeurs Comprendre la commutation de trame, les VLAN Implémenter les VLAN et le routage interVlan dans un réseau local Comprendre et mettre en œuvre l'adressage IP v6 dans une réseau local simple Implémenter des VLAN et du routage statique	28
Windows Server : Administration	Décrire les fonctionnalités de Windows Server et son intégration dans un environnement Utiliser les différentes consoles de gestion Déployer et configurer les principaux services Définir, implémenter et configurer Active Directory Identifier les notions de base de sécurité Utiliser PowerShell Monitorer et dépanner des serveurs Windows Server	28
Linux : Administration	Installer une distribution Linux et effectuer les tâches post-installation Administrer les comptes et les groupes utilisateurs Gérer les disques et le système de fichiers Gérer le processus de démarrage et d'arrêt Analyser l'activité du système Installer des logiciels depuis la distribution ou installer depuis les sources Configurer le client réseau Administrer à distance	28
Windows PowerShell	Décrire les concepts de base de PowerShell Administrer des ordinateurs localement et à distance à l'aide de PowerShell Lister les fonctions PowerShell Utiliser PowerShell pour l'administration d'un parc Windows, macOS ou Linux Identifier les meilleures pratiques relatives aux scripts et fonctions PowerShell Exploiter les fonctionnalités multiplateformes de PowerShell pour gérer des tâches planifiées Utiliser les différents composants PowerShell ensemble Exécuter des tâches en arrière-plan	21
Linux Shell Bash	Développer des scripts Shell Programmer avec Shell Bash	21
Gestion de projet et Méthodes agiles	Utiliser le vocabulaire et les concepts de base en gestion de projets Planifier les étapes d'un projet Suivre l'exécution des travaux Evaluer les risques Manager et communiquer dans le projet Démarche agile	14
MS Project / JIRA	Identifier les fonctions de base de Microsoft Project Online, en tant que planificateur occasionnel ainsi que la démarche méthodologique du chemin critique Identifier tous les aspects de gestion du système de tracking de bugs Jira Utiliser les fonctionnalités basiques de Jira Gérer des utilisateurs et des projets Affecter et suivre des demandes Visualiser les principaux tableaux de bord Administrer des workflows Générer des rapports Effectuer des recherches fines dans la base de données Jira	14

VMware : ICM	Installer et configurer les hôtes ESXi Déployer et configurer vCenter Utiliser le vSphere Client pour créer l'inventaire vCenter et attribuer des rôles aux utilisateurs de vCenter Créer des réseaux virtuels à l'aide de commutateurs standards et de commutateurs distribués vSphere Créer et configurer des datastores à l'aide des technologies de stockage prises en charge par vSphere Utiliser le vSphere Client pour créer des machines virtuelles, des modèles, des clones et des snapshots Créer des bibliothèques de contenu pour gérer les modèles et déployer les machines virtuelles Gérer l'allocation des ressources des machines virtuelles Migrer des machines virtuelles avec VMware vSphere vMotion et VMware vSphere Storage vMotion Créer et configurer un cluster vSphere activé avec VMware vSphere HA (High Availability) et VMware vSphere DRS (Distributed Resource Scheduler) Gérer le cycle de vie de vSphere pour maintenir vCenter, les hôtes ESXi et les machines virtuelles à jour	21
Python	Identifier les usages courants du langage Mettre en pratique le scripting en Python Structurer votre code en fonction, classes et modules Utiliser des modules existants Décrire la programmation réseau avec Python	21
Audit & Pentesting	Définir les enjeux et contraintes du test d'intrusion dans l'objectif de définir les scénarios les plus probables ainsi que l'obtention du consentement légal. Appliquer une méthodologie de test d'intrusion claire et reproductible afin de pouvoir restituer des éléments comparables dans leurs approches. Concevoir et réaligner des outils d'intrusion dans l'objectif de répondre aux différents besoins d'un test d'intrusion. Identifier les différentes vulnérabilités présentes en réalisant les différentes phases des tests d'intrusion évoqués dans les enjeux initiaux dans le but de découvrir les points de faiblesse de l'organisation. Remonter et restituer les différentes vulnérabilités identifiées ainsi qu'un plan d'actions contenant les mesures de sécurité permettant à l'organisation de corriger ses failles	21
Réseaux : Sécurisé l'infrastructure réseaux	Identifier les enjeux de la sécurité des systèmes d'information, ainsi que ses acteurs et ses limites Proposer des solutions pour pouvoir faire transiter des données sur un réseau d'entreprise de façon sécurisée Installer et paramétrer un pare-feu approprié au réseau d'une entreprise Installer et configurer un proxy Mettre en place un filtrage Utiliser différents outils permettant de détecter une intrusion sur un réseau	70
Docker/Kubernetes	Expliquer les avantages et inconvénients de la conteneurisation Déployer et administrer la plateforme Docker Configurer et utiliser le moteur Docker Décrire la création des images Docker et "Dockerfile" Interagir avec le Docker Hub et registry privés Mettre en oeuvre et configurer des conteneurs Déployer des applications dans les conteneurs Organiser la gestion des réseaux et du stockage Maintenir et surveiller une infrastructure de conteneurs en production Créer et mettre en oeuvre Kubernetes	28
Ansible	Identifier les apports des solutions d'automatisation et de gestion de configuration Expérimenter l'utilisation et le fonctionnement d'Ansible Piloter votre infrastructure de serveurs à partir d'Ansible	14
Supervision	Identifier les différents outils Azure permettant de superviser et de gérer une infrastructure on-premise Mettre en oeuvre Azure Monitor et Azure Sentinel Utiliser les bonnes pratiques associées	14

ITIL	Distinguer les concepts-clés du management des services Identifier les principes directeurs d'ITIL 4 pouvant aider une organisation à adopter et adapter le management des services Lister les 4 dimensions de la gestion des services Reconnaître le but et les composants du Système de Valeur des Services ITIL (ITIL SVS) Distinguer les activités de la Chaîne de Valeur des Services ITIL (ITIL SVC) et leurs interconnexions Mettre en oeuvre les pratiques ITIL, leurs buts et leurs principaux termes	14
GLPI (SLA, ESCALADE, Doc Tech, Vieille Techo)	Installer, configurer et utiliser les outils OCS et GLPI	14
Cloud : Administration (ex. AWS ou Azure)	Prendre des décisions architecturales conformément aux bonnes pratiques et aux principes recommandés Utiliser les services pour rendre votre infrastructure évolutive, fiable et hautement disponible Exploiter les services pour conférer davantage de flexibilité et de résilience à une infrastructure Optimiser une infrastructure afin d'améliorer les performances et de diminuer les coûts Utiliser le Well-Architected Framework pour améliorer les architectures existantes (exemple AWS)	28
ISO 27001	Présenter la norme ISO 27001 (2013, les processus de sécurité qui lui sont associés et la démarche de certification) Reconnaître les mesures de sécurité de la norme ISO 27002 (2013) Expliquer les contextes d'implémentation des mesures de sécurité et leur intégration dans l'organisation générale de la sécurité Vous exercer à la sélection et l'approfondissement de mesures de sécurité depuis l'appréciation des risques, les pièges à éviter et l'audit de ces mesures Proposer une vue globale des référentiels existants, des guides d'implémentation ou de bonnes pratiques des mesures de sécurité	14
EBIOS	Pratiquer la gestion des risques avec la méthode EBIOS Risk Manager	14
SOC/SIEM	Comprendre, implémenter et manipuler un SOC (Security Operation Center) dans un environnement complet Mettre en place le Prelude SIEM	14
Infrastructure Cloud hybride	Identifier les acteurs majeurs et les usages d'un Cloud hybride Provisionner un Cloud public avec AWS Implémenter l'hybridation Cloud Décrire et mettre en oeuvre l'automatisation et l'orchestration d'infrastructure Présenter la culture DevOps et faire évoluer la DSI vers ce modèle	21
Autres modules transverses et préparation/passage des examens	Apprendre à apprendre, Soft Skills, Techniques de Recherche d'Entreprises, Création d'entreprise, RGPD, Laïcité/Citoyenneté, Anglais professionnel, Bureautique, GreenIT, Usage des IA...	287

DIPLÔME

Titre professionnel d'Administrateur d'Infrastructures Sécurisées (AIS), RNCP 37680, du Ministère de l'Emploi et de la Formation Professionnelle, de niveau 6 (Bac +3). Ce titre professionnel peut être validé en totalité ou partiellement (CCP1, CCP2 et/ou CCP3).

À PROPOS DES CERTIFICATIONS

Certification éditeur :

Les certifications éditeurs dépendent des éditeurs uniquement (PEGA, SAP, Salesforce, Microsoft, Red Hat...). Chaque éditeur a sa propre façon d'évaluer son candidat.

Cela se fait souvent par le biais d'un QCM chronométré. Sur cette base, il faut généralement obtenir un pourcentage de succès supérieur à 70%. Merci de prendre le temps de demander à vos interlocuteurs M2i le cadre et les conditions de ce passage.

Validation des acquis M2i :

La validation des acquis M2i se fait soit par un QCM chronométré, soit par un examen de fin de parcours ou les candidats passent par groupes de 2 ou 3 devant un jury qui déterminera vos acquis suite à votre cursus de formation. Généralement cette soutenance est précédée de 3 jours de travaux pratiques en groupe afin de préparer cette soutenance. Les équipes M2i pourront vous guider dans votre projet.

LES PLUS DE M2I FORMATION

Microsoft Teams Education, un outil de suivi et d'animation en présentiel et à distance :

- Espace de stockage collaboratif pour accéder aux différents supports de cours et cahiers d'exercices
- Fonctionnalités pour gérer des sessions à distance

La playlist e-learning : tous les apprenants ont accès avant, pendant et après le cursus à notre plateforme e-learning ACADEMIIC pour :

- Acquérir les connaissances prérequises avant de démarrer (sous condition de l'existence des modules pour combler les lacunes)
- Utiliser les modules conseillés par les formateurs pour faire de l'ancrage mémoriel sur des sujets abordés pendant la formation
- Revenir sur un sujet après la formation pour continuer à s'auto-former

MODALITÉS, MOYENS ET MÉTHODES PÉDAGOGIQUES

Formation délivrée en présentiel et/ou distanciel (e-learning, classe virtuelle, présentiel à distance).

Le formateur alterne entre des méthodes démonstratives et actives (via des travaux pratiques et/ou des mises en situation).
La validation des acquis peut se faire via des études de cas, des quiz et/ou une certification.

MODALITÉS D'ACCÈS

Nos équipes accorderont toute leur attention au traitement de votre candidature et s'engagent à vous faire un premier retour dans un délai de 7 jours.

ADMISSION

- Dossier de candidature
- Test de vérification des prérequis
- Entretien
- Validation et éligibilité France Travail (dans le cas de certains dispositifs)

Le groupe M2i s'engage pour faciliter l'accessibilité de ses formations. Les détails de l'accueil des personnes en situation en handicap sont consultables sur la page Accueil PSH.

POURQUOI CHOISIR M2I FORMATION ?

– Un apprentissage métier proactif axé sur l'emploi et basé sur le faire avec l'accompagnement de nos formateurs tout au long du parcours.
– Un accès à des experts : bénéficiez de l'expertise de nos formateurs.
– En présentiel ou à distance : accès individuel aux ressources de formation et progression personnalisée si besoin.
– Outils de suivi collectif et individuels (espaces d'échanges et de partage en ligne, salles virtuelles si en présentiel ou à distance, supports de cours, TP, exercices).

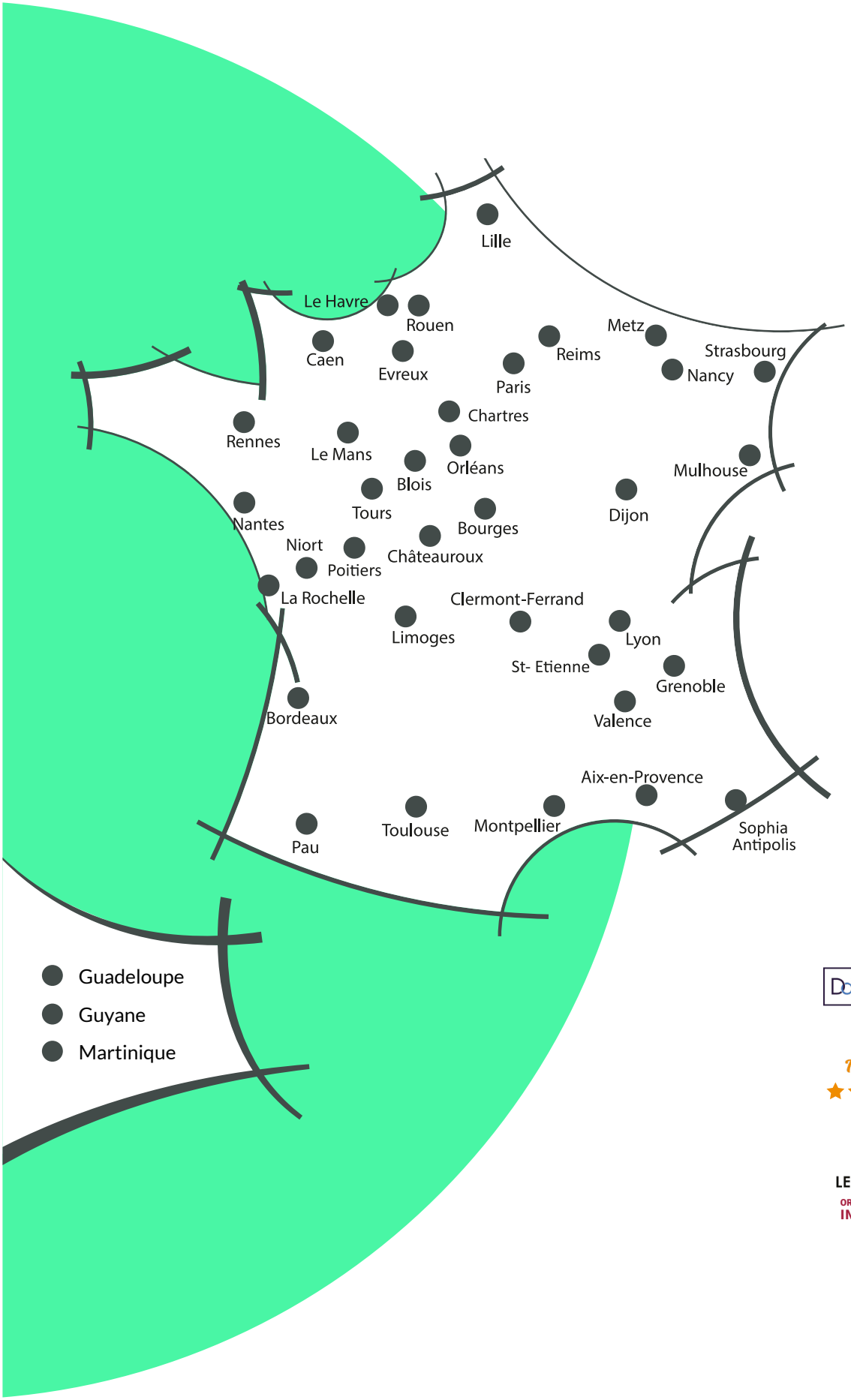
MODALITÉS D'ÉVALUATION

Exemples de validation des acquis de formation :

– Travaux dirigés dans chaque module
– Mise en situation via des cas pratiques et un mini projet
– Certification (si prévue dans le programme de formation)
– Soutenance devant un jury de 30 à 40 min

MaCarrière

m2i Formation



Datadock

Avis Vérifiés 4,6/5

LEADERS LEAGUE
ORGANISME DE FORMATION INCONTOURNABLE