Devenir Ingénieur·e Systèmes Réseaux & Cybersécurité

Document mis à jour le 31/12/2024

Dispositif de formation : **Alternance et Apprentissage**
Date de formation :

L'Ingénieur systèmes réseaux et cybersécurité est responsable de la mise en place, de l'intégration et de la maintenance des matériels et logiciels d'un système d'exploitation sur des serveurs internes ou situés dans des data centers hors de l'entreprise. Il peut intervenir dans le cadre de la mise en service de plateformes informatiques et de traitements distants, à la demande et mutualisés. Il définit les besoins et l'architecture informatique de l'entreprise. Il est garant du bon fonctionnement, de la stabilité et de la qualité du réseau, participe à son évolution, pilote l'accès aux utilisateurs et assure l'équilibre entre le matériel, l'intégralité du système et les logiciels associés.

De manière générale, la fonction d'Ingénieur systèmes, réseaux et cybersécurité varie selon le type de structure et l'organisation de la DSI de l'entreprise, on peut distinguer trois types d'activités : il peut travailler pour des entreprises, des constructeurs ou pour des SSII.

OBJECTIFS DE FORMATION

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

- Piloter la conception d'une infrastructure systèmes, réseaux sécurisée et respectueuse de la politique RSE d'une organisation
- Suivre et mettre en œuvre le déploiement de l'infrastructure systèmes et réseaux sécurisée adaptée aux besoins
- Elaborer la stratégie de sécurisation de l'infrastructure informatique
- Manager la performance des systèmes et réseaux d'une organisation
- Elaborer une stratégie de gestion des nouveaux projets informatiques d'une organisation

La certification complète s'obtient par la validation des 5 blocs qui la constituent, complétée de la validation d'une compétence transversale en anglais technique : « Maîtriser l'anglais technique dans son activité professionnelle afin de mener une veille efficace et comprendre une information technique relative à l'infrastructure systèmes et réseaux en anglais », établie par l'évaluation de la capacité du candidat à rédiger un compte-rendu de veille technologique ou réglementaire en français depuis des sources anglophones.
La validation partielle d'un bloc de compétences n'est pas possible. La validation partielle de la certification est constituée des blocs dont la totalité des compétences est validée. Les blocs de compétences sont capitalisables.
L'évaluation de chaque bloc de compétences est réalisée via des modalités spécifiques d'évaluation détaillées dans le référentiel de la certification.
La réussite aux modalités d'évaluation de ce bloc de compétences fait l'objet de la remise d'un certificat de délivrance d'un bloc de compétences.

Possibilité de valider un ou plusieurs blocs de compétences de la certification professionnelle. EN SAVOIR PLUS

PRÉREQUIS

Être titulaire d'une certification professionnelle de niveau 6 (équivalent niveau Bac +3 / Bac +4).
OU
Justifier d'une expérience professionnelle de 2 ans minimum dans les métiers de l'informatique.
OU
Sous conditions dérogatoires, être titulaire d'un titre de niveau 5 RNCP dans le domaine de l'informatique.

Cette formation est adaptée aux candidats disposant des atouts suivants :

- Connaissance en développement informatique (connaissance d'au moins un langage de scripting ou programmation)
- Aptitude à la direction et gestion opérationnelle
- Pratique de l'anglais technique souhaitable
- Intérêt pour la cybersécurité et les systèmes d'information
- Polyvalence et adaptabilité

Modalités et délai d'accès

- Modalités d'accès : cliquez ici pour connaître le processus d'admission en détail
- Inscription possible tout au long de l'année en fonction des dates de rentrée et jusqu'à 3 mois maximum après le démarrage de la formation (sous réserve de la validation par le service pédagogique)

PUBLIC CONCERNÉ ET FINANCEMENT

Tout public, aussi bien les étudiants en formation initiale, apprentis, jeunes diplômés, demandeurs d'emploi, salariés en reconversion professionnelle, entreprises, personnes en formation continue.

Toutes nos formations sont accessibles aux personnes en situation de handicap.

COMPÉTENCES ET TECHNOLOGIES ABORDÉES

- Voyage dans le Cyberespace
- Cyber Threat Intelligence (CTI)
- Outils et méthodes de gestion de projets
- Durcissement des systèmes et réseaux – Hardening
- Pentest en Python
- Techniques d'attaques
- Préparation et passage de la certification Pentester
- Le métier de RSSI
- SIEM & SOC
- Gestion de crises IT/SSI
- Gestion des opérations de cybersécurité avec Splunk
- Investigation numérique (Computer Forensics)
- OSINT : Recherche d'informations en source ouverte
- Analyse Malwares
- ByPass, antivirus et EndPoint Detection Response (EDR)
- Reporting
- Introduction à la Cybersécurité des systèmes industriels (SCADA)
- Sécurité RF
- DevSecOps
- CTF
- ISO 27001/27002 – Fondamentaux et gestion des mesures de sécurité
- ISO 27032 – Lead Cybersecurity Manager
- RedTeam vs BlueTeam
- ISO 27005 – Risk Manager
- RGPD et Cybersécurité

Le contenu de ce programme peut faire l'objet d'adaptation selon les niveaux, prérequis et besoins des apprenants. Consultez-nous pour obtenir le programme détaillé, module par module.

CERTIFICATION

- Certification professionnelle Ingénieur systèmes, réseaux et cybersécurité de niveau 7 (Bac +5) inscrit au RNCP par France Compétences lors de la commission du 18/10/2023, sous le code RNCP38117, code NSF 326. Certification sous l'autorité et délivrée par l'Institut Européen F2I (en savoir plus). Date d'échéance de l'enregistrement : 18/10/2028.

Taux indicateurs performance & réussite
Nouveau parcours. Les premiers indicateurs de résultats chiffrés sur le niveau de performance et d'accomplissement de la prestation, seront disponibles à partir de 2025 (sous réserve de réalisation).
Cliquez ici pour découvrir les chiffres-clés de l'institut F2I.

MODALITÉS, MOYENS ET MÉTHODES PÉDAGOGIQUES

Formation délivrée en présentiel ou présentiel à distance* : l'acquisition des connaissances se fera aussi bien en centre de formation que pendant les semaines en entreprise. Le contenu peut varier en fonction de l'évolution des technologies et du niveau de l'apprenant.

Le formateur alterne entre méthode** démonstrative, interrogative et active (via des travaux pratiques et/ou des mises en situation).

* Consultez-nous pour la faisabilité de la formation en distanciel.
** Ratio variable selon le cours suivi.

Prérequis techniques fortement conseillés pour suivre cette formation à distance

– Connexion internet « Haut débit », 15 mégabits par seconde minimum
– Fibre non obligatoire
– Relier sa box à son ordinateur via un câble réseau
– Résider en France Métropolitaine
– Être muni d'un casque audio/micro
– PC/MAC i7, SSD, 32 Go de RAM

Configuration nécessaire pour travailler sur des environnements virtualisés.

FINANCEMENT

Le coût global de cette formation est de 15 400€ TTC.

Il n'y a pas de frais de formation ni d'inscription à la charge du bénéficiaire.
Dans le cadre d'un contrat d'apprentissage le coût de la formation est financé via l'entreprise et son OPCO (selon niveau de prise en charge établi par France Compétences / coût contrat défini par les branches professionnelles selon le titre préparé).
Dans le cadre d'un contrat de professionnalisation, le coût de la formation est pris en charge intégralement ou partiellement par l'OPCO de l'entreprise sur la base d'un forfait horaire.

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 ?

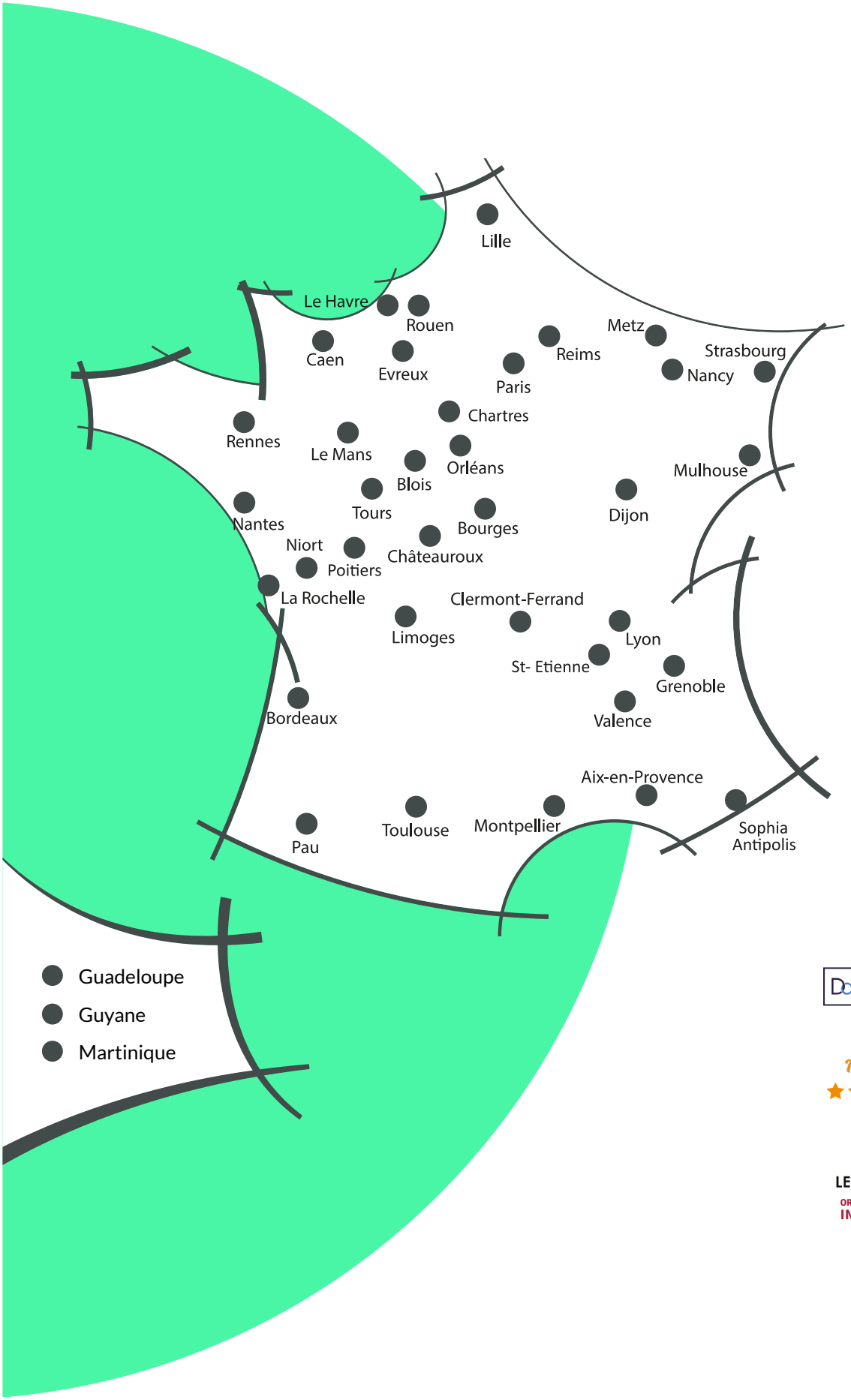
– Un apprentissage métier proactif axé sur l'emploi et basé sur le faire avec l'accompagnement de nos formateurs tout au long du parcours.
– Un accès à des experts : bénéficiez de l'expertise de nos formateurs.
– En présentiel ou à distance : accès individuel aux ressources de formation et progression 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

- Contrôle continu : travaux pratiques, quiz
- Évaluations en cours de formation via des études de cas sur chacune des compétences du titre
- Mémoire professionnel de management de projet Cybersécurité
- Entretien final avec un jury

MaCarrière

m2i Formation



Datadock

Avis Vérifiés 4,6/5

LEADERS LEAGUE
ORGANISME DE FORMATION INCONTOURNABLE