Devenir Consultant·e Cloud DevSecOps

En partenariat avec :

Document mis à jour le 04/04/2025

Dispositif de formation :	**Programme Régional de Formation (PRF)**
Date de formation :	**Du 24 avril au 6 octobre 2025**
Période de stage :	**Du 9 septembre au 6 octobre 2025**
Lieu(x) de formation :	**Villeneuve d'Ascq**
Réunion d'Information :	**Le 10 avril 2025**
Date limite d'envoi de candidature :	**Le 9 avril 2025**

Vous êtes intéressée par les métiers de la sécurité informatique ?
Votre objectif est d'exercer un métier d'avenir aux missions variées dans un environnement collaboratif et dynamique ?

Devenez Consultant Cloud DevSecOps avec M2i Formation en partenariat avec la région Hauts-de-France !

Un Consultant Cloud DevSecOps c'est quoi ?
Le Consultant Cloud DevSecOps accompagne les entreprises dans l'intégration de la sécurité dès les premières étapes du cycle de développement en environnement Cloud. Il assure l'automatisation de la sécurité dans les pipelines CI/CD, la protection des infrastructures et la mise en conformité avec les normes de cybersécurité.

Ses missions principales sont :

- Sécurisation du Cycle DevOps
- Sécurisation des Infrastructures Cloud
- Automatisation et Observabilité

A l'issue d'une formation intensive animée par des formateurs experts métier/terrain d'une durée de 80 jours vous aurez acquis toutes les compétences nécessaires pour exceller dans ce domaine.
Vous apprendrez à utiliser des outils et des pratiques DevOps, à automatiser les processus de développement et de déploiement, et à assurer la sécurité et la performance des systèmes.

Dispensée en présentiel dans nos locaux de Villeneuve d'Ascq du 24 avril au 06 octobre 2025, vous bénéficierez d'un accompagnement dans votre retour à l'emploi et d'une environnement propice pour votre montée en compétences.

Participez à notre visioconférence d'information sans engagement le 10/04/2025 à 10h30 !

OBJECTIFS DE FORMATION

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

– Expliquer le but, les avantages, les concepts et le vocabulaire de DevSecOps
– Discerner les différences entre les pratiques de sécurité DevOps et les autres approches de sécurité
– Déceler les stratégies et bonnes pratiques de sécurité axées sur l'entreprise
– Définir et appliquer les sciences des données et de la sécurité
– Intégrer les parties prenantes de l'entreprise dans les pratiques DevSecOps
– Améliorer la communication entre les équipes Dev, Sec et Ops
– Expliquer comment les rôles DevSecOps s'intègrent à une culture et une organisation DevOps

PRÉREQUIS

– Bac +2 informatique ou scientifique/technique avec une appétence pour la technique
– Expérience pour les systèmes et réseaux (Linux recommandé)
– Intérêt pour l'apprentissage des stratégies et l'automatisation DevSecOps, ou impliquée dans les architectures de la chaîne d'outils de livraison continue
– Appétence pour le développement et idéalement connaissance d'un langage de programmation
– Bonne connaissance des outils informatiques
– Excellent relationnel et êtes capable de vous adapter à différents interlocuteurs clients, interlocuteurs techniques, etc.
– Bonne communication, goût pour le travail en équipe, excellentes capacités rédactionnelles
– La maîtrise de l'anglais professionnel ainsi qu'une appétence pour le secteur numérique associée à des notions réseaux seraient un plus
– Organisation, efficacité et agilité

PUBLIC CONCERNÉ ET FINANCEMENT

Cette formation financée à 100%* est à destination des demandeur·se·s d'emploi inscrit·e·s à France Travail et résidant en région Hauts-de-France.

COMPÉTENCES ET TECHNOLOGIES ABORDÉES

Compétences	Module et objectifs opérationnels	Durée (Jours)	Durée (Heures)
Prendre connaissance du cursus	Présentation du cursus / Linux : Présentation générale du programme, explication des objectifs pédagogiques, et prise en main des environnements Linux pour préparer les apprenants aux prochains modules.	0,5	3,5
Méthodes	Linux Bash : Maîtrise des commandes de base du système Linux, création et exécution de scripts Bash pour automatiser les tâches répétitives dans un environnement serveur ou local.	3,5	24,5
Méthodes	Linux Administration : Administration de systèmes Linux : gestion des utilisateurs, configurations réseau, services critiques, gestion des permissions, et dépannages de base. sécurisation des systèmes, optimisation des performances.	3	21
Méthodes	Bases du réseau & sécurité réseau: Comprendre les protocoles, ports, VPN, pare-feux, Zero Trust.	3	21
Versionning et test	Git : Gestion de dépôts : Présentation des principes de versionning, utilisation de Git pour gérer les versions des projets, collaboration via GitLab ou GitHub et gestion des branches.	2	14
Développement	Python Algo : Programmation d'algorithmes : Initiation aux algorithmes et structures de données avec Python, compréhension des bases logiques et résolution de problèmes simples, Programmation fonctionnelle et objet en Python.	4	28
Développement back	Python et base de données : Développement de scripts pour interagir avec les bases de données relationnelles (MySQL, PostgreSQL), réalisation d'opérations CRUD et intégration dans des projets Python.	3	21
Développement back	Scripting Python pour DevSecOps: Automatiser des tâches, manipuler des API et des fichiers de configuration	4	28
DevOps	Docker : Introduction à la conteneurisation avec Docker, création d'images, gestion des conteneurs, optimisation de la mise en production d'applications isolées et portables.	4	28
DevOps	Kubernetes : Découverte et utilisation de Kubernetes pour orchestrer des conteneurs. Déploiement d'applications à grande échelle, gestion de clusters, et configuration des pods et services.	5	35
DevOps	GitLab CI/CD : Implémentation d'une chaîne CI/CD (intégration continue/déploiement continu) via GitLab pour automatiser les tests et déploiements.	3	21
DevOps	Openshift : Déploiement d'applications conteneurisées avec OpenShift. Gestion des ressources, configuration des environnements, et scalabilité des projets.	3	21
Développement Cloud	Cloud Public et Privé (AWS/Azure/OpenStack) : Prise en main des plateformes cloud publiques comme AWS et OpenStack, configuration des services, gestion des machines virtuelles, et stockage cloud.	11	77
DevOps	Terraform : Introduction à l'Infrastructure as Code (IaC) avec Terraform pour automatiser la création et la gestion d'infrastructures cloud.	2	14
DevOps	Ansible : Utilisation d'Ansible pour l'automatisation des déploiements, gestion des configurations, et orchestration des serveurs de manière déclarative.	3	21

Monitoring	Prometheus et Grafana : Mise en place de la surveillance et du monitoring avec Prometheus et Grafana pour collecter, analyser et visualiser les métriques des applications.	3	21
DevOps	Orchestration et Monitoring : Techniques avancées pour orchestrer des applications complexes avec surveillance automatisée pour garantir la performance et la fiabilité.	4	28
Sécurité	Sécurité dans le pipeline (SAST, DAST, secrets, SCA): Intégrer la sécurité dans chaque étape du DevOps.	2	14
Sécurité	SIEM, EDR, détection et réponse aux incidents :Déployer des outils de détection et de réponse aux menaces.	2	14
Sécurité	API Security & OWASP: Protéger les API, comprendre les risques, appliquer OWASP Top 10.	3	21
Sécurité	Tests, audits et forensic pour DevSecOps: Faire un audit de sécurité, analyser des journaux, simuler une attaque.	3	21
Méthodes Agiles	Scrum Agile : Mise en pratique de la méthodologie agile Scrum pour organiser des équipes, prioriser les tâches, et livrer des projets de manière itérative et incrémentale.	2	14
Validation des acquis	Projet fin de formation : Réalisation d'un projet complet intégrant l'ensemble des compétences DevOps acquises : automatisation, cloud, sécurité, CI/CD, et monitoring.	5	68
Techniques recherches d'emploi	Refonte CV, Pitch mail/entretien, mener sa recherche d'emploi, simulations d'entretien, posture...	2	14

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 M2i Learning 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).

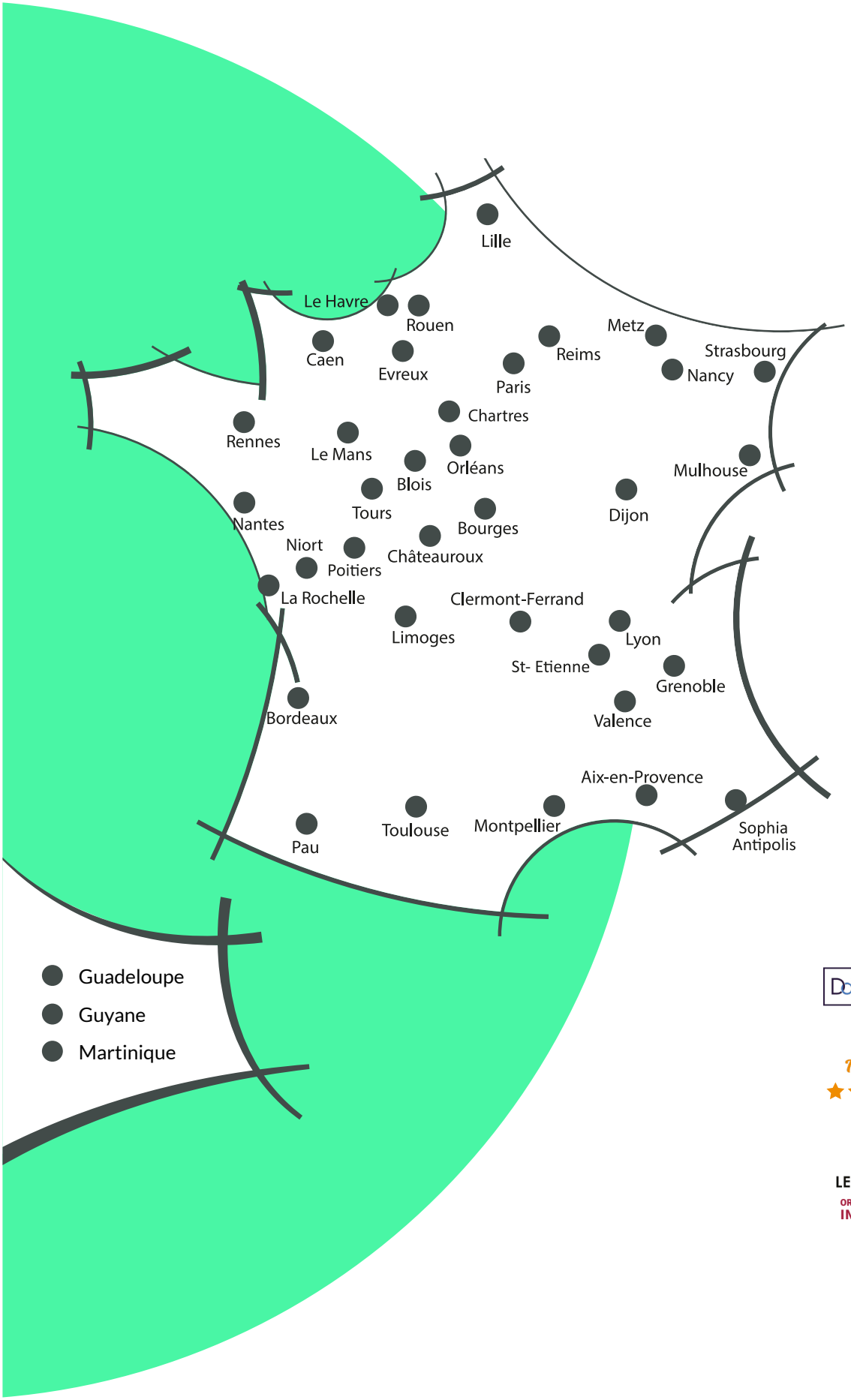
MODALITÉS D'ÉVALUATION

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