Devenir Développeur·se Cybersécurité

Document mis à jour le 03/07/2025

Dispositif de formation :	**Préparation Opérationnelle à l'Emploi (POE)**
Date de formation :	**Du 22 septembre au 16 décembre 2025**
Lieu(x) de formation :	**Aix-en-Provence**
Réunion d'Information :	**Le 23 juillet 2025**
Date limite d'envoi de candidature :	**Le 12 septembre 2025**

Domaine en constante évolution et riche en challenges, la Cybersécurité est un enjeu majeur dans les métiers de l'informatique.

Formez-vous pour devenir développeur cybersécurité avec M2i Formation et l'OPCO Atlas et donnez un nouveau souffle à votre carrière !

OBJECTIFS DE FORMATION

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

- Configurer un poste Linux pour développer en Python
- Identifier les risques et les menaces cyber
- Sécuriser un serveur PostgreSQL
- Développer des tests d'intrusion en Python
- Sécuriser des applications Web
- Déployer une application dans le cloud en toute sécurité

PRÉREQUIS

- Bac +3/+4 informatique/développement ou expérience équivalente
- Bonne connaissance des systèmes et réseaux
- Capacité d'analyse et de synthèse
- Curiosité et goût pour les défis
- Rigueur et sens de la méthode
- Connaissance de l'anglais et d'un langage de programmation

PUBLIC CONCERNÉ ET FINANCEMENT

Cette formation financée à 100%* est à destination des demandeur·se·s d'emploi inscrit·e·s à France Travail.
Après validation de votre candidature par l'entreprise, elle sera soumise à votre conseiller France Travail pour valider la cohérence entre votre profil et votre projet de formation.

COMPÉTENCES ET TECHNOLOGIES ABORDÉES

Catégorie	Module	Durée en jours	Durée en heures
Méthode	**Présentation :** Identifier les différents modules du cursus - Utiliser les plateformes pédagogiques - Décrire le métier de développeur cyber - Brise-glace	0,5	3,5
Fondamentaux	**Administrer un poste Linux :** TCP/IP - Identifier les principes fondamentaux du système d'exploitation – Utiliser interactivement le Shell et connaître les commandes essentielles – Gérer les fichiers et les dossiers - Gestion du réseau - Introduction aux différents services : DNS, mail, Firewall, VPN, Postgresql, apache – mettre en place un hyperviseur	4,5	31,5
Fondamentaux	**Connaitre l'état de l'art de la cybersécurité :** Appréhender la nomenclature cybersécurité - Distinguer les différents enjeux de sécurité - Analyser les risques et les menaces - Identifier les différents niveaux de sécurité : données, échanges de données, OS, réseau - Découvrir les lois et référentiels de la cybersécurité - Audit de sécurité	4	28
Développement	**Sécuriser efficacement une base de données PostgreSQL à l'aide du langage SQL :** Installation et configuration d'un serveur PostgreSQL - Gestion de l'accès aux données - Interroger une base de données avec la clause SQL SELECT - Utiliser les commandes SQL de mise à jour des données - identifier les commandes SQL de début et fin de transaction BEGIN, COMMIT et ROLLBACK - Présenter les concepts de gestion des privilèges systèmes et objets avec les commandes SQL GRANT et REVOKE - Créer, modifier et supprimer certaines catégories d'objets (table, index, vues...) avec CREATE, ALTER et DROP - Journaux applicatifs	3	21
Validation des acquis intermédiaire	Travaux pratiques : installation et paramétrage d'un serveur Linux avec accès sécurisé à PostgreSQL	1	7
Technique de recherche d'emploi	**CV et lettre de motivation :** Avoir le bon état d'esprit pour candidater - Faire sa cartographie des compétences - Concevoir un CV et une lettre de motivation - Publier sur les réseaux sociaux	1	7
DevOps	**Mette en œuvre une usine logicielle** Comprendre les principes DevOps - Mettre en place une solution de configuration logicielle basée sur Git - Gérer les versions des projets du dépôt de données - Mettre en œuvre et exploiter un serveur d'intégration continue	3	21
Développement	**Ecrire des scripts et programmes en 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 - Expérimenter la programmation objet en Python - interroger un service Web - Implémenter un service Web REST et avec Python - Développer des applications Web avec Flask ou Django - ORM - Maîtriser les éléments avancés du langage, le multi-threading et l'implémentation de tests	9	49
Validation des acquis intermédiaire	Travaux pratiques : Construire une API en Python et implémenter et sécuriser une couche d'accès aux données avec un ORM	3	14
Atelier IA	Aide au développement Python avec un outil d'IA	1	7

Développement	**Sécuriser les applications Web :** Intégrer la sécurité dès le début du cycle de développement (DevSecOps) - Utiliser les techniques de sécurisation des applications Web - Identifier et mettre en place des contre-mesures contre les vulnérabilités courantes.	3	21
Gestion de projets	**Gérer un projet avec les méthodes agiles :** Déterminer les situations où l'Agilité est adaptée - Appliquer les principales approches agiles - Conduire un projet Agile	2	14
Sécurité	**Sécuriser une plateforme DevOps :** Décrire les fondements du DevSecOps - Intégrer la sécurité dans un pipeline CI/CD (intégration et développement continu) - Identifier les vulnérabilités spécifiques aux technologies de conteneurisation - Effectuer des tests d'intrusion relatifs aux technologies de conteneurisation - Sécuriser les technologies de conteneurisation	3	21
Technique de recherche d'emploi	**Posture et entretien :** Savoir être & technique de recherche d'emploi : Travailler sa posture avant un entretien - Communication interpersonnelle - Questions/réponses types d'entretien - Simuler un entretien	1	7
Sécurité	**Développer des tests d'intrusion en Python :** Mettre en pratique les compétences nécessaires en scripting pour créer vos propres outils en Python pour un test d'intrusion	3	21
Validation des acquis intermédiaire	**Travaux pratique** : créer des programmes de pentest : attaque bruteforce sur un archive zip protégé par un mot de passe – campagne de pishing - Attaque de dictionnaire...	3	21
Sécurité	**Sécurité des applications Web avancée :** Sécuriser efficacement un serveur Web / Comprendre les attaques avancées contre les applications Web. Mettre en œuvre des mécanismes avancés d'authentification et d'autorisation. Appliquer les bonnes pratiques de gestion des sessions et des cookies - Mettre en place des contre-mesures avancées pour protéger les applications Web.	5	35
Sécurité	**Pratiques de DevOps dans le Cloud :** Comprendre les concepts de DevOps dans un environnement cloud - Utiliser des outils de déploiement continu (CI/CD) dans le contexte du cloud - Gérer l'infrastructure en tant que code (IaC) avec des outils cloud (par exemple, AWS CloudFormation, Azure Resource Manager) - Mettre en œuvre la surveillance et la gestion des journaux dans le cloud - Explorer les bonnes pratiques de sécurité pour les déploiements cloud - Appliquer les principes DevOps pour optimiser les performances et la disponibilité des applications dans le cloud	3	21
Validation des acquis finale	Travaux pratiques : Développement et déploiement d'une application web sécurisée (Python - flask ou django) dans un cloud	3	21
Validation des acquis finale	**Préparer et passer la certification TOSA Python**	**1**	**7**

CERTIFICATION

La certification Tosa Python détermine et valide le niveau de compétence et d'aptitude d'un candidat dans les principales fonctionnalités de Python (écriture d'algorithmes, gestion des entrées/sorties, importation et exportation de données, structuration de données, emploi de liaisons dynamiques...).

Elle permet de renforcer l'employabilité et d'atteindre les objectifs professionnels.
La certification Tosa Python est composée de 35 questions et dure 90 minutes.
Elle s'appuie sur une base de données de plus de 170 questions de typologies variées, comme des QCM ou des exercices pratiques qui immergent le candidat dans l'environnement du logiciel et lui permettent de réaliser des cas concrets rencontrés en entreprise.

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).

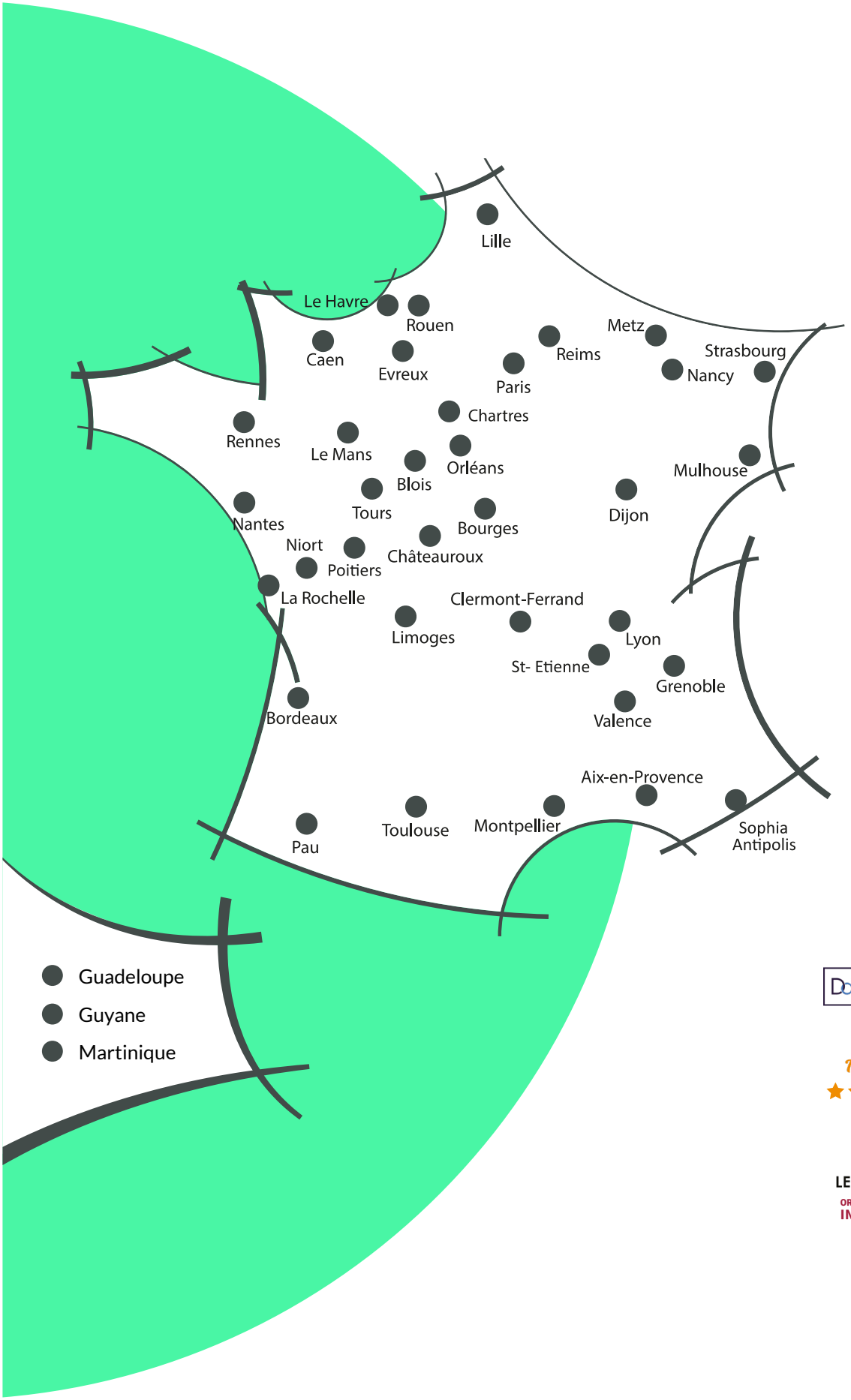
MODALITÉS D'ÉVALUATION

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