Devenir Analyste / Consultant·e Cybersécurité

Document mis à jour le 20/10/2025

Dispositif de formation :	**Programme Régional de Formation (PRF)**
Date de formation :	**Du 20 février au 24 juillet 2024**
Période de stage :	**Du 29 mai au 23 juillet 2024**
Lieu(x) de formation :	**Orléans**
Réunion d'Information :	**Le 9 janvier 2024 ou le 16 janvier 2024**
Date limite d'envoi de candidature :	**Le 12 février 2024**

M2i Formation en partenariat avec la **région Centre Val de Loire** et **France Travail** dans le cadre du Plan Régional de Formation, recherche pour février 2024, des demandeurs d'emploi souhaitant se former **au métier de Analyste / Consultant en Cyber sécurité.**

OBJECTIFS DE FORMATION

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

- acquérir les compétences nécessaires pour surveiller le système d'information d'une entreprise
- détecter toutes activités suspectes ou malveillantes
- proposer un plan d'actions en cas d'incidents de sécurité

PRÉREQUIS

- Bac +4 / +5 en informatique (filière Systèmes et Réseaux de préférence)
- Avoir exercé des missions dans le secteur du développement et/ou de l'administration d'infrastructures informatiques, serait un plus
- Connaissance d'au moins un langage de scripting ou programmation : Java, JavaScript, PowerShell, Bash
- Pratique de l'anglais technique souhaitable
- Aptitudes relationnelles, rédactionnelles et techniques

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

Nom	Contenu	Durée (heures)	Durée (jours)
Accueil des stagiaires - Présentation du cursus - Apprendre à apprendre	Prendre connaissance des différentes parties du cursus, du détail de chaque module - Faire connaissance avec les autres participants via un jeu "brise-glace" - Comprendre comment fonctionne le cerveau pour mémoriser plus efficacement.	7	1
Les Soft Skills & TRE (Techniques de recherche d'emploi / d'entreprise)	Construire son employabilité. Identifier sa situation par rapport à l'emploi visé : compétences, priorités, contraintes. Organiser sa recherche d'emploi. S'approprier les techniques et outils : lettre, CV, réseaux sociaux. Réussir ses entretiens. Coaching sur les compétences transversales.	28	4
Remise à Niveau	Remise à Niveau bureautique – Réseaux – TCP/IP - Python	56	8
Contribuer à une informatique éco-responsable	Valoriser le matériel informatique voué au rebut – Contribuer à réduire l'impact des déchets des équipements bureautiques et informatiques sur l'environnement – Respecter la directive européenne sur les déchets des équipements électriques et électroniques – Sensibiliser un large public à « comment limiter l'empreinte écologique sur le web » lors de conférences organisées par les apprenants ».	10,5	1,5
Vie professionnelle Egalité Femme/Homme	Adopter une posture non-discriminante dans sa vie professionnelles et personnelles – Sortir des stéréotypes – Se former et travailler dans un environnement genré. Se défendre face à la discrimination, au sexisme, au harcèlement.	3,5	0,5
Linux et Services réseaux	Rappels réseaux, TCP/IP, Routage Statique & Dynamique - Switching - Routage Inter VLAN. Superviser et sécuriser l'infrastructure des systèmes et - Implémenter une solution de supervision - Les forces et les faiblesses de TCP/IP - VPN – Intégrer et gérer un Firewall - Proxy, DS et IPS - Sécurité du routage - Virtualisation et durcissement - Connaître les principales menaces de l'environnement Linux et les différentes solutions qui s'y rapportent.	35	5
Techniques de Hacking	Détecter les fragilités d'un système par la connaissance des différentes cibles d'un piratage - Appliquer des mesures et des règles basiques pour lutter contre le hacking - Comprendre le mécanisme des principales attaques	35	5
Investigation Numérique	Réaliser une investigation numérique sur des systèmes Windows et Linux - Acquérir les compétences et la méthodologie pour une investigation numérique sur du réseau TCP/IP - Mettre en pratique les compétences générales sur l'investigation numérique – **Examen de validation des acquis Inforensic**	56	8
Pentest avec Python	Pentest avec Python	35	5
Durcissement d'un système Linux	Guide des bonnes pratiques de déploiement – identification et authentification - Protection des fichiers - La sécurité du noyau - Les malwares sous Linux - La sécurité du réseau – Surveillance du système - Le patch management - Usage des sondes de détection - Durcissements complémentaires	35	5
Détection et prévention des intrusions, SIEM et Centres opérationnel de Sécurité – Architecture de sécurité – Gestion de crises & PCA/PRA	Intégration d'un SOC (Security Operation Center) et mise en place de SIEM : TD avec les outils, Comprendre, implémenter et manipuler un SOC (Security Operation Center) dans un environnement complet - Mettre en place le Prelude SIEM	35	5

Atelier - architecture et déploiement FireWall et VPN	Décrire les concepts de base et les fonctionnalités des firewalls Reconnaître l'architecture de réseau et de sécurité, et le rôle des firewalls dans la protection des réseaux Configurer et gérer les firewalls de manière efficace Déployer et utiliser pfSense pour la sécurité des réseaux.	28	4
RGPD	Comprendre les fondamentaux du règlement et vérifier son application dans son environnement numérique	7	1
Tour d'horizon de l'analyse des risques – ISO 27001 – ISO 27005	Analyse et gestion des risques – ISO 27001/2 – ISO 27005	21	3
CERTIFICATION PENTESTER	Etude de cas – Soutenance devant Jury (Mise en situation professionnelle) Compétences attestées : • 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 clair et reproductible afin de pouvoir restituer des éléments comparables dans leurs approches. • Concevoir et réaligner des outils d'intrusions 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'intrusions évoqués dans les enjeux initiaux dans le but de découvrir les points de faiblesses de l'organisation. • Remonter et restituer les différentes vulnérabilités identifiées ainsi qu'un plan d'action contenant les mesures de sécurité permettant à l'organisation de corriger ses failles.	21	3
Période pratique	Stage en entreprise	280	40
Période de bilan		7	1

CERTIFICATION

Certification PENTESTER RS6092

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

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 Politique Handicap.

POURQUOI CHOISIR M2I ?

- 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).

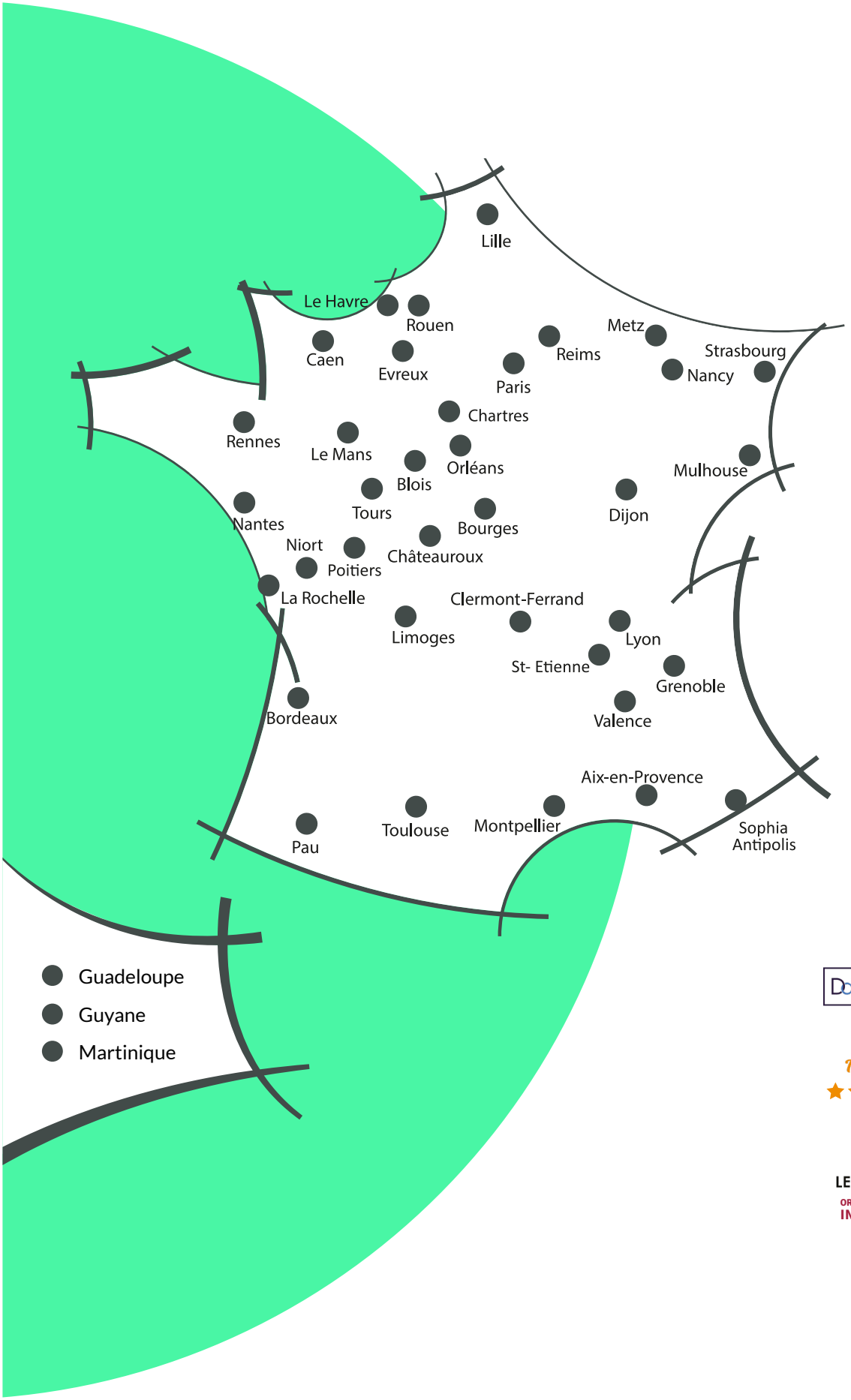
MODALITÉS D'ÉVALUATION

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