Devenir Analyste en Cybersécurité

MaCarrière

m2i Formation

En partenariat avec :

La Région Auvergne-Rhône-Alpes

Document mis à jour le 25/11/2026

Dispositif de formation :	**Programme Régional de Formation (PRF)**
Durée de la formation :	**205 jours (1435h)**
Date de formation :	**Du 28 mars 2024 au 14 février 2025**
Période de stage :	**Du 10 septembre 2024 au 11 février 2025**
Lieu(x) de formation :	**Lyon**
Date limite d'envoi de candidature :	**Le 20 mars 2024**

Cette certification est sanctionnée par le Pentesting (réaliser des tests d'intrusion), M2i, RS6092, par l'Inforensic (réaliser des investigations numériques), M2i, RS6093 et par le TOEIC (Test of English for International Communication), Educational Testing Service Global B V, RS6151.

Pour vous inscrire au webinar d'information, sélectionnez la date de votre choix parmi celles proposées : https://app.livestorm.co/m2i-formation/formez-vous-aux-metiers-du-numerique-en-auvergne-rhone-alpes-avec-m2i-formation?s=7412e4b4-2353-4406-87a6-0492a861d2e6

OBJECTIFS DE FORMATION

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

« **Réaliser une investigation numérique (Sécurité Inforensic)** » s'adresse à des professionnels de la sécurité informatique et permet d'acquérir les compétences pour identifier et évaluer l'ensemble des méthodes de rétrospection faisant suite à une menace de sécurité, afin de préconiser les mesures d'urgence pour en limiter la propagation. Le stagiaire pourra ainsi collecter et analyser l'information se trouvant dans un programme informatique pour retrouver les traces des activités d'utilisateurs et prouver un délit numérique.

« **Réaliser des tests d'intrusion (Sécurité Pentesting)** » s'adresse aux professionnels de la sécurité informatique et permet d'acquérir toutes les compétences indispensables pour effectuer des tests qui consistent à examiner tous les réseaux et les systèmes informatiques en simulant les actions d'un intrus potentiel à l'intérieur de leur environnement de travail : analyse des flux, analyse des espaces de stockages, analyse de sécurité spécifique au terminal utilisé.

PRÉREQUIS

- Bac +2 en informatique orienté Systèmes & Réseaux obligatoire
- Avoir une expérience professionnelle dans le domaine

PUBLIC CONCERNÉ ET FINANCEMENT

Cette formation financée à 100%* est à destination des demandeur·se·s d'emploi inscrit·e·s à France Travail en région Auvergne-Rhône-Alpes.
Cette formation est prise en charge en totalité par la région et le FSE.

COMPÉTENCES ET TECHNOLOGIES ABORDÉES

Nom	Contenu et objectifs de la séquence / modules	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 & Compétences de base	Améliorer sa communication au quotidien et prendre la parole en public - Améliorer sa communication écrite - Prendre des notes - Rédiger des écrits professionnels efficaces - Animer une réunion	35	5
Visites d'entreprises partenaires pour parler de leur métier		7	1
Ecoute et relation clients	Mettre en oeuvre le sens de l'écoute et l'esprit de service - Etre réactif face à la diversité des demandes - Vous adapter au profil de vos interlocuteurs - Enrichir la qualité de vos relations clients - Consolider vos pratiques professionnelles	14	2
Devenir un professionnel de l'IT	Assimiler et maîtriser les différentes normes et standardisations liées à la sécurité de l'information. Collaborer et s'entraider en milieu professionnel. Comprendre les principaux biais cognitifs et l'impact sur l'ingénierie sociale. Connaître les périmètres légaux et juridiques (RGPD) de l'activité d'analyste cybersécurité. Détecter et faire la corrélation d'événements et d'indices. Mener un audit auprès d'un client. Synthétiser et vulgariser ses connaissances pour s'adapter à son public. Travailler dans un environnement et au sein d'une équipe agile	35	5
Laïcité, citoyenneté et valeurs de la république	Qu'est-ce que la laïcité ? Les obligations de chacun en matière de laïcité. La conciliation entre l'exercice de la liberté de culte et le principe de laïcité. Mise en oeuvre en situation de travail	4	0,5
Anglais technique	Lire et comprendre des articles techniques - Exposer ses idées - Rédiger une synthèse sur un sujet technique - Suivre un tuto en anglais e-learning individuel - CERTIFICATION TOEIC	28	4
Techniques de Recherche d'entreprise (TRE)	Créer un CV professionnel. Développer sa présence en ligne. Définir et s'approprier son projet professionnel. Rédiger et mettre en forme son CV et sa lettre de motivation. Simuler un entretien d'embauche - Optimiser son réseau professionnel. Optimiser ses réseaux sociaux. Atelier de technique de recherche d'entreprise. Sensibilisation et Inscription sur la plateforme Nos Talents Nos Emplois	21	3
RGPD	Comprendre les fondamentaux du règlement et vérifier son application dans son environnement numérique	7	1

Bilan intermédiaire de formation		3	0,5
Remise des certifications - attestations de compétences générales et professionnelles + bilan final de la formation avec tous les partenaires		7	1
Stage en entreprise PAMP		700	100
Administrer et sécuriser les composants constituant l'infrastructure	Rappels réseaux : 21h - Ratio théorie/TP, TD avec les outils : 50/ 50 - TCP/IP - Routage Statique & Dynamique - Switching - Routage Inter VLAN	21	3
	Superviser et sécuriser l'infrastructure des systèmes et réseaux : 119h - Ratio théorie/ TP, TD avec les outils : 40/60 - 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 - Pouvoir optimiser la sécurisation du système - Considérer les menaces courantes pesant sur les systèmes d'information, en vue de l'implémentation de mesures de sécurité adaptées (organisationnelles et techniques) : domaines, protocoles, Serveurs, postes client - Sécuriser un réseau WIFI	112	16
Intégrer, administrer et sécuriser une infrastructure distribuée	Implémenter et administrer des serveurs et services Windows : 35h - Ratio théorie/ TP, TD avec les outils : 50/50 - Révision sur l'administration de base - Virtualisation - Mettre en oeuvre Active Directory mono-domaine et multi-domaines - Mettre en oeuvre les services réseaux DNS et DHCP - Mettre en place de la haute disponibilité	35	5
	Administrer des systèmes et services Linux : 49h - Ratio théorie/ TP, TD avec les outils : 40/60 Révisions des commandes de base - Gestion de utilisateurs - Démarrage et arrêt du système (GRUB / GRUB2) - Gestion des processus - Gestion de disques et partitionnement - LVM - Gestionnaires de paquets - Journaux systèmes - Interfaces réseau - Gestion du service de temps - Gestion à distance (SSH, etc...) - Fichiers resolv.conf - hosts - Services DHCP, DNS (Bind) - Routage NAT - iptables - Mise en place de Docker	35	5
	Automatiser l'administration de Linux avec des scripts : 21h - Ratio théorie/ TP, TD avec les outils : 20/80 - Rappels des commandes de base - Les variables d'environnements - Les différents types de shell - Variables, boucles et conditions	21	3
	Implémenter et administrer des infrastructures hybrides (35h) : Ratio théorie/ TP, TD avec les outils : 40/60 - Infrastructures DNS mixte Windows/Linux - Infrastructures DHCP & DHCP-Relay - Infrastructure Active Directory avec SaMBa / Redondance ADDS sous SaMBa - Serveur de fichiers SaMBa et interopérabilité avec Windows - PowerShell Core sous Linux	42	6
	Mise en oeuvre de PKI : 14h - Ratio théorie/ TP, TD avec les outils : 40/60 - Introduction au chiffrement et aux systèmes d'infrastructures à clefs publiques - PKI dans un environnement d'entreprise - Les fondamentaux du Cloud Azure et la gestion de la sécurité : 21h - Ratio théorie/ TP, TD avec les outils : 50/50	14	2
	Concepts et services de base - Outils de gestion - Définir les normes et standards pour sécuriser le Cloud Microsoft - Reconnaître les moyens offerts pour la sécurisation du Cloud Microsoft - Sécuriser votre approche Cloud - Eviter la mise en place d'une sécurité coûteuse et laborieuse - Effectuer des attaques et des tests de pénétration sur le tenant - Mettre en place des architectures sécurisées - Sécuriser l'infrastructure du tenant - Utiliser les bonnes pratiques	21	3

Faire évoluer et optimiser l'infrastructure et son niveau de sécurité	Etat de l'art de la Cyber : 7h - Ratio théorie/ TP, TD avec les outils : 80/20 - Connaître les tendances de la cybercriminalité - Gérer des cyberattaques - Maîtriser les incidents et riposter face à une cyberattaque - Identifier les acteurs de la utte contre la cybercriminalité - Aborder les bonnes pratiques types OIV / OSE - Appréhender les meilleures pratiques pour maîtriser la sécurité d'un SI	7	1
	Python : 56h - Ratio théorie/ TP, TD avec les outils : 40/60 Connaître les usages courants du langage - Structurer son code en fonction, classes et modules - Utiliser des modules existants - s'initier à la programmation réseau avec Python - Maîtrise la programmation objet en Python - Acquérir les compétences nécessaires en scripting pour créer des outils en Python pour un test d'intrusion	56	7
	Technique de hacking : 35h - Ratio théorie/ TP, TD avec les outils : 50/50 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 (Forensic) : 49h - Ratio théorie/ TP, TD avec les outils : 40/60 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	42	6
	Durcissement Linux : 28h - Ratio théorie/ TP, TD avec les outils : 20/80 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	28	4
	Durcissement AD Windows : 14h - Ratio théorie/ TP, TD avec les outils : 20/80 Introduction au durcissement Active Directory - Principales attaques et sécurisation Active Directory - Mesures défensives Active Directory - Stratégie de sécurisation AD	14	2
	Intégration d'un SOC (Security Operation Center) et mise en place de SIEM : 21h - Ratio théorie/ TP, TD avec les outils : 60/40 Comprendre, implémenter et manipuler un SOC (Security Operation Center) dans un environnement complet - Mettre en place le Prelude SIEM	21	3
	Analyse et gestion des risques avec EBIOS et ISO 27005 : 21h - Ratio théorie/ TP, TD avec les outils : 80/20 - Analyse et compréhension d'une stratégie d'entreprise - Compréhension de la gouvernance SSI - Mise en oeuvre d'une analyse de risques basée sur l'ISO 27005 au travers de la méthode EBIOS - Les différentes étapes de l'analyse de risques - Comprendre les concepts, approches, méthodes et techniques permettant une gestion efficace de risque selon ISO 27005 - Mettre en oeuvre l'ensemble des critères et des seuils indispensables à la mise en place d'une analyse de risque - Extrapolation et méthode d'implémentation d'une politique de SI	21	3
Phase de positionnement pédagogique	Phase de positionnement pédagogique via la plateforme JOBREADY et tests de connaissances techniques Débriefing individuel	7	1
Projet "Catch the flag"	Jeu "Catch the flag" : Jeu consistant à exploiter des vulnérabilités affectant des logiciels de manière à s'introduire sur des ordinateurs pour récupérer les drapeaux preuves d'intrusion.	21	3

Mise en place de l'environnement de formation et de travail et la prise en main de la formation à distance avec notamment les tests des ordinateurs, la vérification des connexions internet ainsi que l'installation des logiciels		7	1
Passage des examens M2i : Sécurité Pentesting - Sécurité Inforensic		7	1

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).

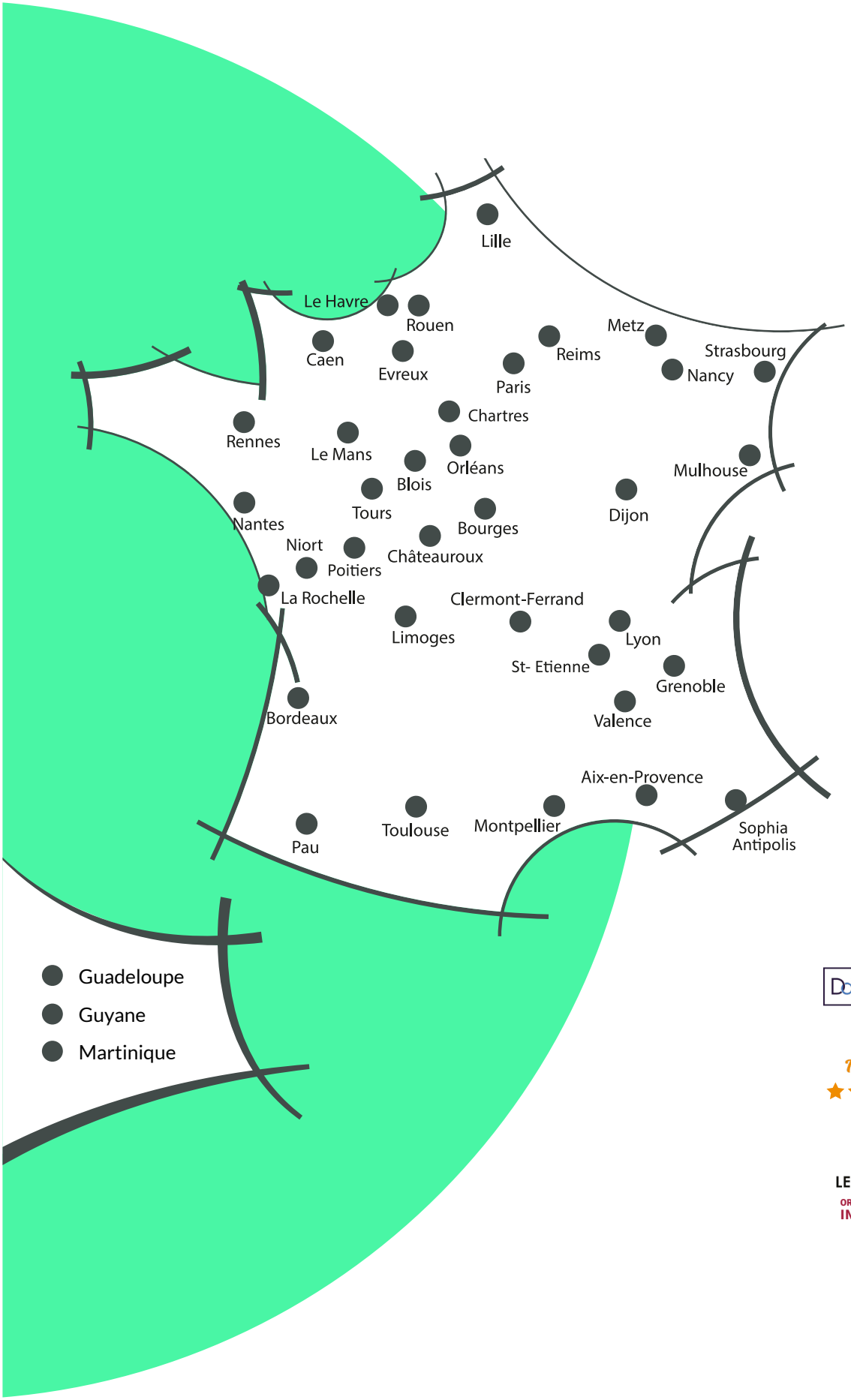
MODALITÉS D'ÉVALUATION

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

© Ma Carrière M2i Formation - Crédits photos : Getty Images - Document non contractuel - Les informations contenues dans ce document peuvent être modifiées sans préavis - NE PAS JETER SUR LA VOIE PUBLIQUE