Devenir Expert·e en Cybersécurité

En partenariat avec :

Document mis à jour le 19/04/2025

Dispositif de formation :	**Programme Régional de Formation (PRF)**
Date de formation :	**Du 28 mai au 25 juillet 2025**
Lieu(x) de formation :	**Lille**
Réunion d'Information :	**Le 6 mai 2025**
Date limite d'envoi de candidature :	**Le 5 mai 2025**

La région Hauts-de-France tremplin de votre parcours professionnel !
Vous cherchez une formation de haut niveau sur les méthodes d'audits et de tests d'intrusion, d'identification et d'analyse avancée de malwares, de protection et de sécurisation du Système d'Information ?
Une formation qui vous formera à assurer la pérennité de la sécurité des systèmes, des flux et des données dans les entreprises ?
Vous êtes issu d'un parcours diplômant en informatique de niveau 5 (Bac +2) et êtes passionné par la sécurité informatique ?
M2i Formation s'associe à l'ESGI et à l'Efficom Lille, écoles incontournables des métiers de l'informatique, et vous propose une opportunité de formation préparatoire qui précédera l'intégration en Bachelor ou Mastère Cybersécurité en alternance !
Dimension indispensable de toute organisation, la sécurité informatique est riche en opportunités professionnelles et recherche ses experts.
D'une durée de 40 jours en présentiel et animée par des formateurs experts métier/terrain, vous approfondirez vos compétences et notamment :

- La mise en œuvre et l'administration d'une infrastructure systèmes et réseaux Linux/Windows
- Le développement des scripts en Python pour administrer les serveurs
- L'implémentation des solutions techniques pour sécuriser une infrastructure
- L'identification des fondamentaux de la cybersécurité

Vous bénéficierez également d'un accompagnement dans votre retour à l'emploi grâce à nos modules dédiés aux techniques de recherche d'emploi.

Les dates de formation seront du 28 mai au 25 juillet 2025, dans le campus ESGI Lille situé au 65 Rue Philippe-Laurent Roland, 59000 Lille.

Compléter le formulaire et recevez votre invitation pour participer à notre réunion d'information qui aura lieu le 06 mai 2025 dans les locaux de l'ESGI et épanouissez-vous dans la voie qui est la vôtre !

OBJECTIFS DE FORMATION

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

– Etablir un diagnostic pou repérer les failles systèmes et réseaux
– Définir des scénarii d'intrusion
– Tester la vulnérabilité des installations
– Evaluer le niveau de sécurité existant en adéquation avec les besoins
– Proposer et mettre en œuvre des solutions technologiques pour sécuriser un SI
– Collaborer avec les décisionnaires de la politique sécurité de l'entreprise

PRÉREQUIS

• Bac + 2 Informatique option systèmes, réseaux et infrastructure globale
• Avoir une appétence pour les différents systèmes d'exploitation et une compréhension globale de la sécurité informatique et les infrastructures SI
• Parcours et/ou expérience en en systèmes et réseaux recommandé
• Capacité d'analyse et de synthèse
• Rigueur et sens de la méthode
• Vous avez un bon sens de la communication et faites preuve d'aisance relationnelle
• Bonne maitrise de la langue française à l'oral et à l'écrit
• Anglais B2 minimum
• Des notions de programmation sont un plus

PUBLIC CONCERNÉ ET FINANCEMENT

Résident·e·s des Hauts-de-France, souhaitant intégrer le Bachelor ou Mastère Cybersécurité en alternance à l'ESGI ou à l'Efficom Lille.

COMPÉTENCES ET TECHNOLOGIES ABORDÉES

catégorie	module	durée en jours	durée en heures
Méthode	**Présentation :** Identifier les plateformes pédagogiques et le projet fil rouge - Présenter le cursus - Se connaitre avec une activité "brise-glace"	0,5	3,5
Méthode	**Apprendre à apprendre :** Comprendre comment fonctionne notre cerveau en phase d'apprentissage - Utiliser une technique de prise de notes efficace - Mettre en pratique des stratégies d'apprentissage qui favorise la mémorisation	0,5	3,5
Réseaux	**Révisions sur les réseaux et TCP/IP :** Rappels sur le modèle OSI et TCP/IP - Fonctionnement des protocoles réseaux courants - Introduction à l'interception et l'analyse réseau	3	21
Systèmes	**Windows server - La sécurité :** Révision sur l'administration d'un serveur Windows - Concevoir et configurer une infrastructure sécurisée sous Windows Server 2022 ou Windows Server 2025 - Identifier et analyser les risques - Lister les principales méthodes de sécurisation d'un parc Windows Server - Respecter les bonnes pratiques.	5	35
Programmation	**Algorithmique :** Reconnaître les structures de base de la programmation (boucles, conditions) - Identifier les grands paradigmes de programmation (procédural, objet) - Distinguer la notion d'objet et les concepts associés - Identifier les variables et le typage des données - Utiliser les algorithmes de tri face à des problématiques identifiées.	2	14
Programmation	**Python par la pratique :** Identifier les usages courants du langage - Mettre en pratique le scripting en Python - Structurer le code en fonctions, classes et modules - Utiliser des modules existants - Décrire la programmation réseau avec Python - Expérimenter la programmation objet en Python.	4,5	31,5
Validation des acquis	Utiliser un système d'IA générative pour écrire des scripts Python	0,5	3,5
Systèmes	**Linux - des fondamentaux à l'administration :** Identifier les principes fondamentaux du système d'exploitation - Utiliser le shell et connaître les commandes essentielles - Gérer les fichiers et les dossiers - Installer les grands types de distributions Linux et effectuer les tâches post-installation - Administrer les comptes et les groupes utilisateurs - Gérer les disques et le système de fichiers - Gérer le processus de démarrage et d'arrêt - Gérer les applications et les packages Analyser l'activité du système - Configurer le client réseau - Intégration d'un environnement Linux avec un environnement Windows AD - Maintenir et monitorer un serveur Linux - Introduction au déploiement et l'administration d'une base de données PostGreSQL	7	49
Systèmes	**Les bases de la sécurité des systèmes et services réseaux :** Proposer des solutions pour pouvoir faire transiter et stocker des données sur un réseau d'entreprise de façon sécurisée - Installer et paramétrer un pare-feu approprié au réseau d'une entreprise - Installer et configurer un proxy - Mettre en place un filtrage - Utiliser différents outils permettant de prévenir et détecter une intrusion sur un réseau.	5	35
Validation des acquis	**Travaux pratiques** : Travaux pratiques : Mise en œuvre d'une infrastructure sécurisée sous Linux et Windows	2	14

Cybersécurité	**Les fondamentaux de la cybersécurité :** Identifier les principales tendances de la cybercriminalité et leurs impacts économiques - Expliquer les principes fondamentaux de la SSI, y compris la sécurité en profondeur et la "security by design" - Décrire les méthodes de gestion des cyberattaques, y compris les SOC et la gestion des incidents - Analyser le rôle des acteurs publics et privés impliqués dans la cybersécurité - Interpréter les principales lois, normes et référentiels en matière de cybersécurité (RGPD, ISO 27001, ANSSI...) - Décrire les différentes phases d'un test d'intrusion et les cadres légaux associés - Mettre en œuvre un test d'intrusion en utilisant des frameworks et outils adaptés (ex : Metasploit, OSINT, OpenVAS) - Réaliser une collecte d'informations sur une cible en s'appuyant sur l'ingénierie des sources publiques - Identifier et exploiter des vulnérabilités sur une infrastructure - Appliquer des techniques de post-exploitation (élévation de privilèges, mouvements latéraux, nettoyage des traces...) - Présenter les missions d'une Blue Team et le fonctionnement d'un SOC - Mettre en œuvre un plan de renforcement de la sécurité sur des postes et serveurs Windows - Auditer l'architecture d'un système d'information et élaborer un plan de contre-mesure - Collecter des données à des fins d'investigation numérique - Analyser des artéfacts numériques pour produire un rapport d'enquête - Définir un risque et contextualiser les scénarios de risque (actifs, menaces, vulnérabilités...) - Appliquer des méthodes qualitatives et quantitatives pour estimer le niveau de risque - Comparer les différentes méthodes de gestion des risques (EBIOS, MEHARI, OCTAVE, Bow-Tie) - Élaborer des barrières de prévention et de protection à partir d'une analyse Bow-Tie - Expliquer les missions du RSSI et le rôle de l'assistant RSSI dans la gouvernance de la SSI - Analyser les référentiels ISO 27001/27002 pour les appliquer à un contexte organisationnel - Rédiger une politique de sécurité des systèmes d'information (PSSI) - Appliquer les activités du NIST Cybersecurity Framework - Évaluer la maturité de sécurité d'une organisation à l'aide du modèle CMMI - Construire un tableau de bord de pilotage SSI avec des indicateurs pertinents - Identifier les enjeux de la sécurité des environnements industriels et les recommandations de l'ANSSI.	10	70

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).

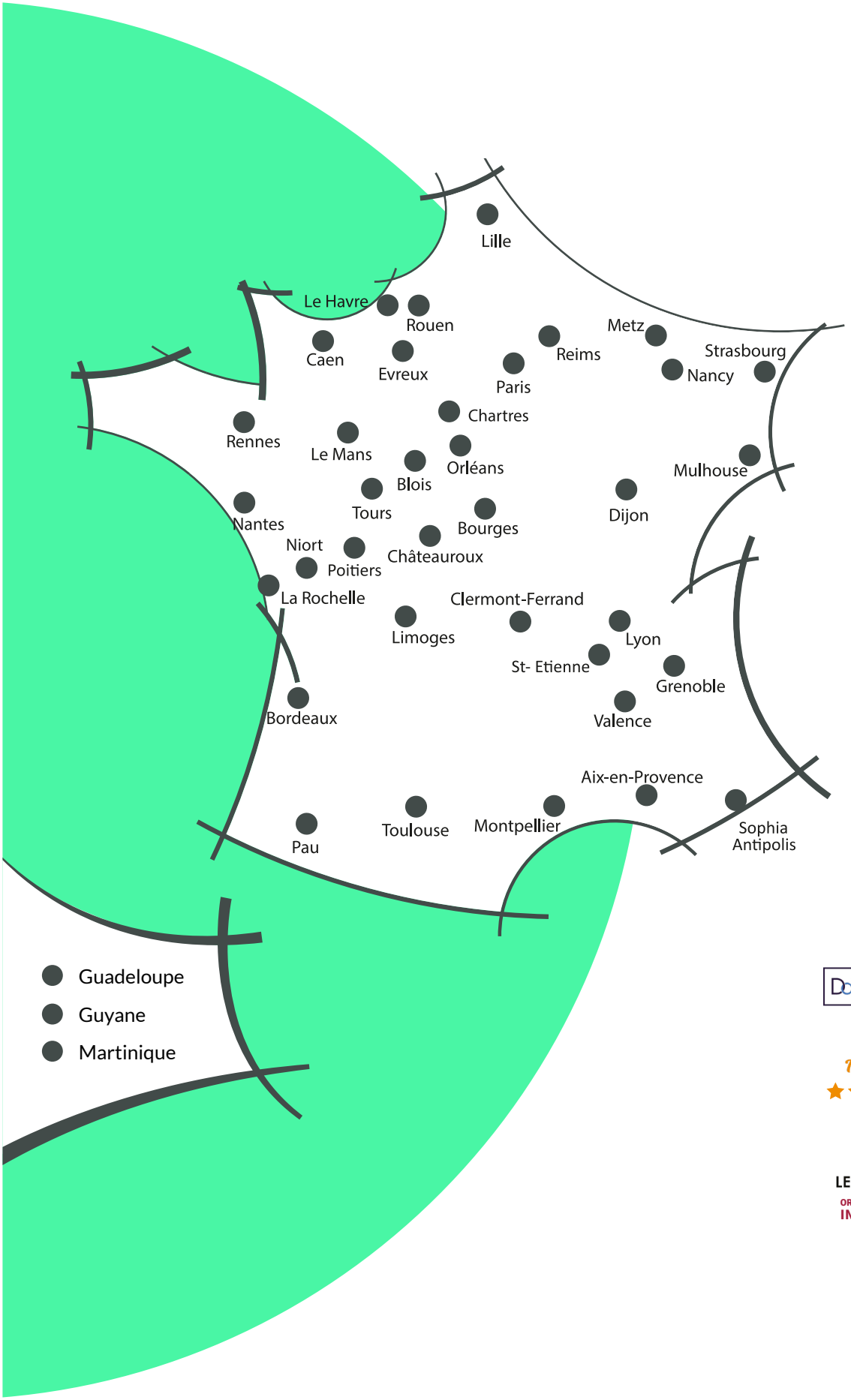
MODALITÉS D'ÉVALUATION

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