Devenir Analyste SOC / Technicien en Cybersécurité

Document mis à jour le 16/09/2025

Dispositif de formation :	**Préparation Opérationnelle à l'Emploi (POE)**
Date de formation :	**Du 17 juin au 17 septembre 2024**
Lieu(x) de formation :	**Villeneuve d'Ascq**
Réunion d'Information :	**Le 18 avril 2024 ou le 22 mai 2024**
Date limite d'envoi de candidature :	**Le 21 mai 2024**

M2i Formation et l'OPCO Atlas vous proposent d'intégrer une formation de 57 jours qui vous permettra d'acquérir des compétences clés dans le domaine de la cybersécurité.

L'analyste SOC que l'on pourrait aussi appeler "Technicien en Cybersécurité" est en effet en charge de la sécurité d'un système informatique.

Vous aborderez au fil de ce cursus notamment :

les techniques d'analyse et de détection d'intrusion
la mise en œuvre des solutions de prévention
les outils d'analyse et de reporting

La formation aura lieu du **17 Juin au 17 Septembre 2024** *(période de congé du 03 au 18 Août 2024)* **en présentiel à Villeneuve d 'Ascq.**

En amont de la formation, vous bénéficierez d'un job dating organisé par M2i en présence d'entreprises de référence dans le domaine de la Cyber !

Nous vous invitons à postuler à ce projet dès maintenant ! *Votre candidature sera étudiée à partir du 18 Mars et selon les prérequis du poste, les profils retenus seront obligatoirement ceux en adéquation avec le(s) projet(s).*

OBJECTIFS DE FORMATION

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

- Analyser, interpréter et traiter les alertes de sécurité émises par le centre de sécurité (SOC)
- Evaluer les dommages subis et contribuer à concevoir une solution technique pour une reprise d'activité et une sécurisation du SI
- Assurer le maintien à jour des dispositifs de supervision de la sécurité comme le SIEM (Software Information Event Management)
- Jouer un rôle essentiel auprès des utilisateurs en termes de prévention et veille au respect des bonnes pratiques
- Assurer une veille permanente sur les menaces et les vulnérabilités

PRÉREQUIS

– Bac +2 informatique (branche infrastructure) minimum
– Bonne connaissance des systèmes et réseaux
– Avoir déjà eu une approche de la cybersécurité
– Capacité d'analyse et de synthèse
– Curiosité et goût pour les défis
– Rigueur et sens de la méthode
– La connaissance de l'anglais est un atout
– La connaissance d'un langage de programmation et/ou de scripting

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

Contenu non contractuel pouvant être soumis à modifications :

Catégorie	Module	Durée (Jours)	Durée (heures)
Méthode	Présentation du cursus, des plateformes et du projet fil rouge - présentation du métier	0,5	3h30
Fondamentaux	**Connaitre l'état de la cybersécurité :** Comprendre le monde la cybersécurité, ses disciplines, ses métiers	1,5	10h30
Fondamentaux	**Concevoir des scripts Python :** Acquérir les fondamentaux de la programmation structurée et objets avec Python	5	35
Compétence transverse	**Technique de recherche d'emploi : Concevoir un CV :** Aborder de manière sereine les outils de candidatures - Savoir rédiger et construire de manière personnalisée et impactante des outils de candidature (CV et lettre de motivation) - Avoir une posture d'offreur de services et non de demandeur d'emploi.	1	7
Fondamentaux	**Consolider ses connaissances en sécurité Systèmes et réseaux :** Réviser des notions de sécurité de base en réseau, sur les principaux protocoles de communication, et en virtualisation	5	35
Métier -Cybersécurité	**Connaitre les techniques d'Hacking et les contre-mesures :** 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	7	49
Métier -Cybersécurité	**Concevoir des tests d'intrusion avec des scripts Python** Mettre en pratique les compétences nécessaires en scripting pour créer des outils en Python pour un test d'intrusion.	2	14
Validation des acquis intermédiaire	Travaux pratiques : Création d'un RAT en Python – Développer des scripts d'intrusion	2	14
Compétence transverse	**Technique de recherche d'emploi : simulation entretien d'embauche :** Se préparer et réussir un entretien d'embauche - Vous positionner et avoir l'état d'esprit de réussite d'un entretien ou d'un job dating - Préparer les étapes d'un entretien (avant, pendant et après) - Savoir anticiper et pouvoir répondre à tous types de questions - Connaitre un cadrage de réponses pour des questions d'entretiens.	1	7
Métier -Cybersécurité	**Mettre en œuvre les méthodes d'investigation numérique (Forensic) :** Techniques d'investigation numérique Réseau, Windows et Linux – Faire une analyse de malware simple – Investiguer les sites Web et les mobiles.	5	35
Validation des acquis intermédiaire	**Travaux pratiques** : investigation numérique : détecter des attaques de différents types	2	14
Métier -Cybersécurité	**Mettre en place une stratégie de durcissement (Hardening) :** Implémenter des composant de cyber sécurité – Durcir les infrastructure Linux et Windows – Durcir les protocoles - Sécuriser les applications Web	10	70
Validation des acquis intermédiaire	**Travaux pratiques** : Implémenter une infra IPSEC et des VPN – Durcir l'infra de l'entreprise « fil rouge »	2	14
Compétence transverse	**Développer ses compétences comportementales :** Compléter vos savoir-faire métiers par la maîtrise des savoir-être aujourd'hui incontournables pour être un professionnel efficace - Identifier vos besoins, vos limites, vos croyances négatives, en termes de comportements au travail - Identifier les principales dimensions des compétences comportementales et développer les éléments fondamentaux de ces attitudes : la relation positive, la maîtrise temporelle, l'attitude résiliente Améliorer votre rapport au travail et au collectif de travail Retrouver de la stabilité et des certitudes à travers une meilleure vision de vos forces et de vos faiblesses.	2	14

Métier -Cybersécurité	**Intégrer un SOC et mettre en place d'un SIEM :** Décrire l'état de l'art du SOC (Security Operation Center) - Répondre aux besoins des enjeux liés à la cybersécurité et des menaces par le métier d'analyste SOC.	5	35
Métier -Cybersécurité	**Gérer les risques avec la méthode EBIOS RM - Risk manager :** Cadrage et socle de sécurité – Sources de risques – Scénarii stratégiques et opérationnels – Traitement du risque	3	21
Métier -Cybersécurité	**Connaitre les normes de la gestion de la sécurité - ISO 27001/27002 :** Présenter la norme ISO 27001 (2013, les processus de sécurité qui lui sont associés et la démarche de certification) - Reconnaître les mesures de sécurité de la norme ISO 27002 (2013) - Expliquer les contextes d'implémentation des mesures de sécurité et leur intégration dans l'organisation générale de la sécurité - Vous exercer à la sélection et l'approfondissement de mesures de sécurité depuis l'appréciation des risques, les pièges à éviter et l'audit de ces mesures - Proposer une vue globale des référentiels existants, des guides d'implémentation ou de bonnes pratiques des mesures de sécurité.	2	14
Validation des acquis finale	Travaux pratiques : Jeu "Catch the flag"	3	21

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 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 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).

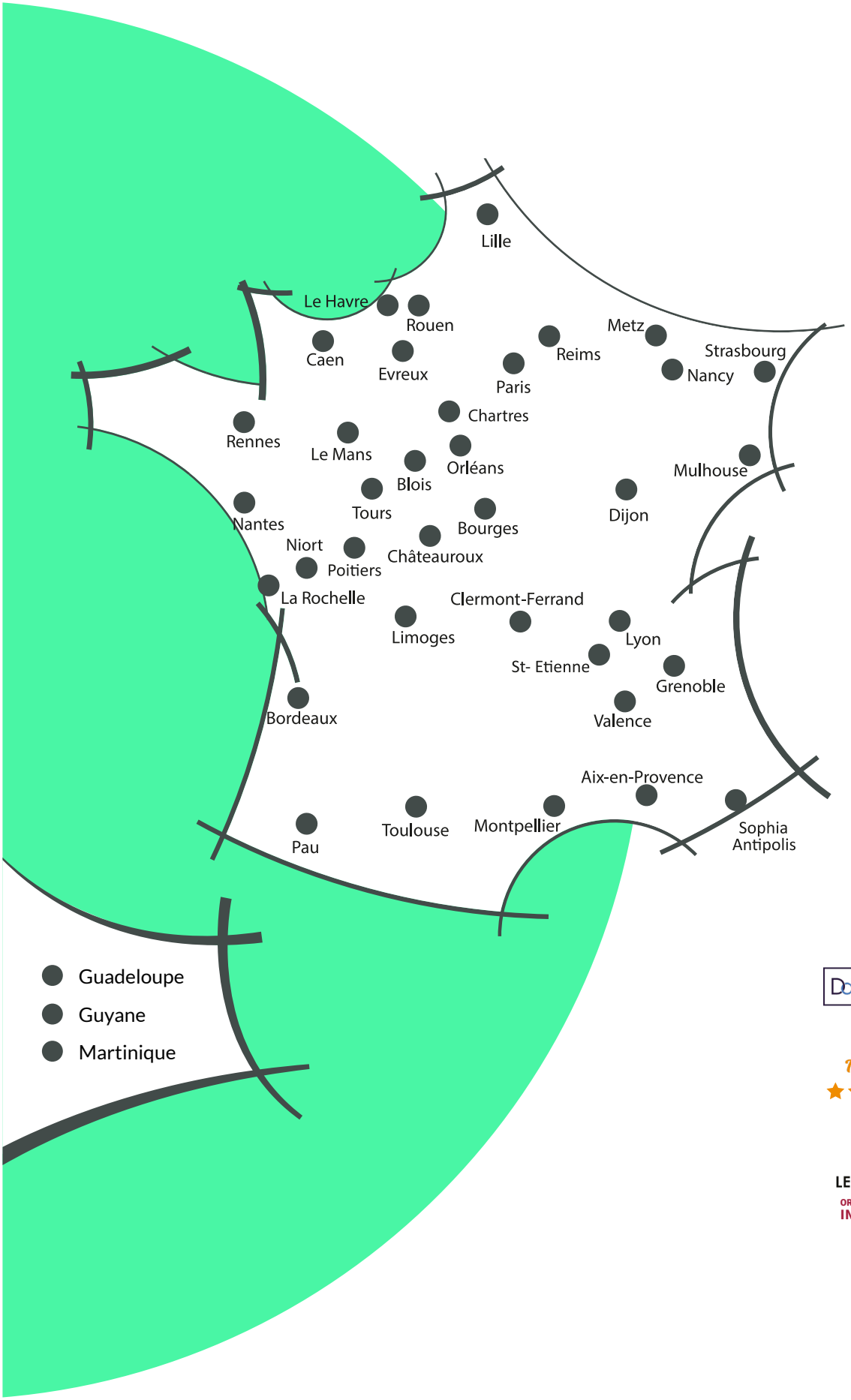
MODALITÉS D'ÉVALUATION

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