1 formation = 1 job

Préparation Opérationnelle à l'Emploi d'Analyste SOC

Avis Vérifiés 4,6/5

m2iformation.fr

m2i Formation

Choisir M2i Formation, c'est l'assurance d'un recrutement adapté à vos besoins !

Dans un marché en constante évolution, vous avez l'obligation d'être proactif et d'anticiper pour gagner de nouveaux marchés.

M2i vous accompagne afin de recruter celles et ceux qui feront votre force demain !

- Avec plus de 30 ans d'expérience, nous avons développé une expertise de vos problématiques et de vos besoins. M2i s'impose la plus grande rigueur pour recruter et vous proposer des candidats correspondant précisément à vos critères.
- Notre maillage, votre force ! Avec nos 35 centres répartis sur toute la France, nous sommes en mesure d'identifier et sélectionner les meilleurs candidats près de chez vous. De plus, chacun de nos centres est équipé de solutions de formation à distance. Il est désormais possible pour chaque candidat de suivre sa formation où qu'il soit.
- Un accent particulier est mis sur les projets Fil Rouge : il ne s'agit pas de former uniquement aux compétences techniques, mais aussi aux métiers. Grâce aux nombreux travaux pratiques, vos futures recrues seront mises en situation afin d'être opérationnelles dès le premier jour de leur embauche.
- Les solutions de financement évoluent régulièrement et sont parfois méconnues. Notre maîtrise des dispositifs mis en place par France Travail, l'OPCO Atlas et les régions nous permet de vous accompagner pour faciliter le travail de vos DRH.

Tous nos cursus sont réalisables en formation distancielle.

De la sélection à l'embauche, M2i Formation s'occupe de tout !

SÉLECTION

Sourcing
Analyse et pré-sélection des CV éligibles selon vos critères.

Sélection
Conduite de réunions d'information auprès des candidats.
Passage et correction des tests logiques et techniques.
Entretien de motivation et de savoir-être pour chaque candidat en vue de valider son profil.

FORMATION

Animation de la formation via une orientation métier
Travaux et cas pratiques rythmés par un projet Fil Rouge durant toute la période de formation.
Suivi individuel de chaque apprenant (assiduité, assimilation, motivation et comportement) avec reporting mensuel auprès des futurs employeurs.

Tous nos cursus sont réalisables en formation distancielle.

RECRUTEMENT

Encadrement
Organisation de Jobdating par M2i Formation au cours du cursus.

Analyste SOC

Tous nos cursus sont réalisables en formation distancielle.

OBJECTIFS DE FORMATION

Ce cursus permet aux apprenants de comprendre les techniques d'analyse et de détection d'intrusion, de mettre en œuvre des solutions de prévention dans un SOC et de comprendre le métier d'analyste SOC en utilisant des outils d'analyse et de reporting. L'analyste SOC peut travailler au sein d'un SOC interne à une entreprise ou pour le compte d'une société de service.

LES MISSIONS DE DÉVELOPPEUR·SE C++

- Analyser, interpréter et traiter les alertes de sécurité émises par le centre de sécurité (SOC)
- Evaluer les dommages subis et contribue 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 veiller au respect des bonnes pratiques
- Assurer une veille permanente sur les menaces et les vulnérabilités

MÉTIERS CIBLES

Analyste SOC, Analyste Cybersécurité, Consultant Cybersécurité, Spécialiste réponse à incident, Analyste traitement d'incidents.

PRÉREQUIS

Bac +3/+4 informatique ou expérience équivalente - 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 - Connaissance de l'anglais et d'un langage de programmation ou de scripting.

PUBLIC CONCERNÉ

Demandeur d'emploi inscrit à France Travail.

MODALITÉS, MOYENS ET MÉTHODES PÉDAGOGIQUES

Formation dispensée en présentiel et/ou à distance par des formateurs professionnels : apports théoriques, exercices de mise en situation professionnelle.

Les formateurs alternent entre la méthode affirmative (présentations, démonstrations), interrogative (tests, quiz…) et active (jeu de rôles, cas pratique, apprentissage par les pairs …). Ils s'appuient sur les 4 piliers de l'apprentissage issus des dernières découvertes en neurosciences. Les journées sont rythmées par l'alternance entre théorie et pratique via un jeu d'exercices : exercices progressifs, exercices récapitulatifs et de validation des acquis.

ADMISSION

- Dossier de candidature
- Test pour vérifier les prérequis
- Entretien
- Validation et éligibilité France Travail

MODALITÉS D'ACCÈS

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 et Handicap.

VALIDATION DES ACQUIS

- Dans chaque module, environ 50% de travaux pratiques + Quiz pour valider la compréhension
- Tout au long du parcours, 7 jours de travaux pratiques en semi-autonomie pour valider la mémorisation et ancrer les acquis
- En fin de parcours, 2 jours pour préparer et passer la certification Splunk Core Certified User

DÉLAIS D'ACCÈS

La candidature peut être déposée jusqu'à 15 jours avant la date de démarrage de la session.

OBJECTIFS PÉDAGOGIQUES ET TECHNOLOGIES ABORDÉES

57 jours - 399 heures

Dans chaque module, le ratio cours théorique/pratique est d'au moins 50%.

Catégories	Modules	Durée (Jours)	Durée (Heures)
Fondamentaux	**Présentation :** Présentation du cursus, des plateformes pédagogiques et de la certification - Brise-glace - Présentation du métier.	0,5	3,5
	Apprendre à apprendre : Comprendre comment fonctionne notre mémoire pour mieux apprendre - Mettre en pratique des stratégies d'apprentissage - Apprendre à prendre des notes efficacement - Favoriser l'ancrage mémoriel.	0,5	3,5
Technique de recherche d'emploi	**CV & 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
Système	**Rappels systèmes & réseaux :** Rappels sur les couches OSI et TCP/IP - Installation et configuration de serveurs Windows et Linux - Paramétrage des services réseaux - Administration en PowerShell et Bash - Mode commande.	5	35
Sécurité du SI	**Les métiers de l'analyste SOC :** Bonne pratique et installation, configuration des firewalls et des sondes de type Intrusion Prenvention System, Intrusion Detection System, Network Intrusion Detection System.	1	7
	Cyber Threat Intelligence CTI : Identification et analyse des cybermenaces à l'aide de frameworks de chasse à la menace (Open CTI...) - Analyse proactive des attaques et détection - Mise en application de la nomenclature.	3	21
Validation des acquis	**Travaux pratiques :** Suivi et recherche de pattern d'attaques via Cyber Threat Intelligence.	1	7
Sécurité du SI	**Sécurité réseaux :** Bonne pratique et installation, configuration des firewalls et des sondes de type Intrusion Prevention System, Intrusion Detection System, Network Intrusion Detection System.	2	14
	SOC réseaux : Analyse de log réseaux, enrichissement des logs, outils complémentaires d'analyse de logs (Wireshark...).	5	35
	Sécurité systèmes : Bonne pratique et installation, configuration et hardening des systèmes Linux et Windows : Hosts Intrusion Detection System, Antivirus, End Point Detection and Response.	2	14
	SOC systèmes Linux et Windows : Analyse de log systèmes, enrichissement des logs, outils complémentaires d'analyse de logs : Sysmon & Sysmon Simulator, Journaux evtx, Logs Linux.	5	35
Validation des acquis	**Travaux pratiques :** Analyse de logs et recommandations.	1	7
Sécurité du SI	**Introduction au SIEM :** Généralité, comparatif, fonctionnement : ELK, Splunk, Grey Log, Qradar.	1	7
	Elasticsearch : Installation, Configuration, prise en main, Beats, Elastic Agent, Fleet, Rapports, KQL.	5	35

Catégories	Modules	Durée (Jours)	Durée (Heures)
Validation des acquis	**Travaux pratiques :** Capture The Flag Elasticsearch.	1	7
Sécurité du SI	**Splunk :** Utiliser Splunk pour collecter, analyser et générer des rapports sur les données - Enrichir les données opérationnelles à l'aide de recherches et de flux - Créer des alertes en temps réel - Réaliser du scripting sur Splunk - Intégrer des graphiques avancés - Utiliser l'API de Splunk - Mettre en place les bons réflexes d'exploitation de Splunk - Améliorer l'exploitation de données avec Splunk - Reconnaître les obligations légales en matière de conservation des données - Définir la démarche d'une analyse de log - Interpréter la corrélation et l'analyse avec Splunk - Déployer Splunk de manière avancée - Administrer Splunk.	6	42
Validation des acquis	**Travaux pratiques :** Capture The Flag Splunk	2	14
Sécurité du SI	**Règles de détection :** Apprendre à écrire des règles de détection selon les standards Sigma, Yara, Snort.	2	14
	Adversary émulation (Détection d'attaques) : Installer et utiliser des outils de simulation d'attaques tel que Caldera, Atomic Red team, Honeypot.	3	21
	Forensic : Fondamentaux de l'investigation numérique : capture de données volatiles et non volatiles, préservation juridique de preuves, fondamentaux de l'analyse système & mémoire.	5	35
Technique de recherche d'emploi	**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
Validation des acquis	**Travaux pratiques :** Déploiement d'un SOC & Adversary emulation & reporting.	2	14
	Préparation et passage de la certification Splunk Core Certified User : Entraînement en ligne Splunk : QCM, vidéos… Certification : 60 min, 60 questions.	2	14
		57 jours	399 heures

Programme et planning sur demande

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
- Espace dédié aux formateurs pour les fiches de suivi des apprenants qui permettent d'indiquer le niveau d'acquisition des connaissances de chaque apprenant
- Outil de gestion des TPs pour suivre le niveau de progression
- Intégration de la plateforme WooClap pour proposer des activités d'apprentissage interactives
- Fonctionnalités pour gérer des sessions à distance

La playlist e-Learning*

En option, en cas de décrochage, de remédiation pédagogique ou la nécessité de se mettre à niveau pour intégrer le parcours, nous pouvons mettre à disposition avant, pendant et après le cursus, des modules e-learning depuis notre plateforme ACADEMIIC.

* pour ce cursus, certains modules e-learning peuvent être en anglais

→ **Je souhaite recruter des Analystes SOC**

Datadock

Avis Vérifiés 4,6/5

LEADERS LEAGUE
ORGANISME DE FORMATION INCONTOURNABLE

m2iformation.fr

© Mars 2024 - 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