Analyste SOC (Security Operation Center) Consultant Cybersécurité

57 jours | 399 h

OBJECTIFS DE FORMATION

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

PRÉREQUIS

Diplômés en études supérieures (Bac +4/+5 requis) en informatique/scientifique

Connaissance d'un langage de programmation et des fondamentaux de l'infrastructure Windows et/ou Linux.

Capacité d'analyse et de synthèse.

Rigueur et sens de la méthode.

Connaissance de l'anglais est un plus.

PUBLIC CONCERNÉ

Demandeurs d'emploi inscrits à Pôle Emploi.

COMPÉTENCES ET TECHNOLOGIES ABORDÉES

Compétences	Module	Durée (Jours)	Durée (Heures)
Fondamentaux	**Présentation du cursus**, du projet fil rouge et des certifications.	0,5	4
	Etat de l'art de la Cybersécurité : Connaître les tendances de la cybercriminalité - Gérer des cyberattaques - Maîtriser les incidents et riposter face à une cyberattaque - Identifier les acteurs de la lutte contre la cybercriminalité - Aborder les bonnes pratiques types OIV / OSE - Appréhender les meilleures pratiques pour maîtriser la sécurité d'un SI.	2	14
	Rappels Réseaux - Systèmes Windows et Linux : TCP/IP – routage – Microsoft AD – DHCP – DNS – Systèmes de fichiers - Processus de démarrage…	5	35
	Python par la pratique : Connaître les usages courants du langage - Maîtriser le scripting en Python - Structurer son code en fonction, classes et modules - Utiliser des modules existants - Vous initier à la programmation réseau avec Python - Maîtriser la programmation objet en Python.	5	35
Connaissances métier et techniques	**Technique de Hacking et contre-mesure :** 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.	5	35
	Tests d'intrusion avec Python : Acquérir les compétences nécessaires en scripting pour créer des outils en Python pour un test d'intrusion.	3	21
	Durcissement Linux : Connaître les principales menaces de l'environnement Linux et les différentes solutions qui s'y rapportent - Pouvoir optimiser la sécurisation du système.	5	35
	Durcissement Windows : 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.	5	35
	Intégration d'un SOC et mise en place d'un SIEM : Comprendre, implémenter et manipuler un SOC (Security Operation Center) dans un environnement complet – Mettre en place le Prelude SIEM.	4	28
	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 – Analyser un serveur Web compromis – Introduction à l'investigation de mobiles.	9	63

Technique de recherche d'emploi et savoir-être	**Posture du consultant IT :** Relations avec les autres - Connaître les principes de base de la communication - Comprendre l'interlocuteur et qualifier son besoin - Animer une réunion et s'adresser à un auditoire.	1	7
	Gestion de crises : Mettre en place une organisation adaptée pour répondre efficacement aux situations de crise - Elaborer une communication cohérente en période de crise - Eviter les pièges induits par les situations de crise - Tester votre gestion de crise SSI.	1	7
	Techniques de recherche d'emploi et savoir-être : Vous 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 - Connaître un cadrage de réponses pour des questions d'entretiens. Préparer son CV, sa lettre de motivation et sa visibilité sur les réseaux et les sites d'emploi (LinkedIn, Apec, Pôle Emploi).	2	14
Gouvernance	**Analyse des risques avec la méthode EBIOS :** Etablir une analyse des risques avec les méthodes EBIOS ainsi que les scénarii stratégiques, opérationnels et le traitement du risque.	3	21
	Les fondamentaux 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) - Connaître les mesures de sécurité de la norme ISO 27002 (2013) - Comprendre les contextes d'implémentation des mesures de sécurité et leur intégration dans l'organisation générale de la sécurité - Avoir une vue globale des référentiels existants, des guides d'implémentation ou de bonnes pratiques des mesures de sécurité.	2	14
Savoir Faire	**Jeu « Catch the Flag »**	2	14
Validation des acquis	**Préparation et passage des certifications M2i Inforensic et Pentesting et de la soutenance**	2,5	17

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
+ Intégration de la plateforme WooClap pour proposer des activités d'apprentissage interactives
+ 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

* pour ce cursus SAP, les modules e-learning sont en anglais

→ Je souhaite devenir Analyste SOC

Retrouvez tous les **détails de notre offre en présentiel et à distance** sur **m2iformation.fr**