Analyste des opérations de sécurité Microsoft

Maitriser les outils de sécurité Microsoft pour parer les risques

Présentiel ou en classe à distance

4 jours (28 h)

Prix inter : 2.850,00 € HT
Forfait intra : 6.990,00 € HT

Réf.: MSSC200

Formation officielle

Microsoft

Idéal en Distanciel

Cette formation offre une montée en compétences essentielle pour les professionnels de la sécurité souhaitant devenir des acteurs opérationnels dans les opérations de **détection d'attaques, d'investigation et de remédiation**. Elle couvre des outils stratégiques dans l'écosystème Microsoft, notamment **Sentinel, Defender XDR et Defender pour le Cloud**.
L'usage de **KQL** pour interroger les logs, ainsi que la maîtrise de l'automatisation des réponses via des playbooks, sont des compétences très recherchées dans les centres d'opérations de sécurité (SOC). En combinant théorie, laboratoires pratiques et cas d'usage, cette formation permet de développer une approche pragmatique et opérationnelle.
Cette formation prépare à la certification Microsoft Certified Security Operations Analyst Associate.
Cette formation prépare à la certification Microsoft Certified Security Operations Analyst Associate.

A qui s'adresse cette formation ?

Pour qui

- Analystes sécurité
- Ingénieurs sécurité

Prérequis

- Compréhension de base de Microsoft 365
- Compréhension fondamentale des produits de sécurité, de conformité et d'identité Microsoft
- Compréhension intermédiaire de Microsoft Windows
- Familiarité avec les services Azure, en particulier les bases de données Azure SQL et le stockage Azure
- Connaissance des machines virtuelles Azure et des réseaux virtuels
- Compréhension de base des concepts de script
- Disposez-vous des connaissances nécessaires pour suivre cette formation ? Testez-vous !

Programme

1 - Atténuer les menaces à l'aide de Microsoft 365 Defender

- Présentation de la protection contre les menaces Microsoft 365
- Atténuer les incidents à l'aide de Microsoft 365 Defender
- Protéger les identités avec Azure AD Identity Protection
- Corriger les risques avec Microsoft Defender pour Office 365
- Protéger un environnement avec Microsoft Defender pour Identity

- Gérer Microsoft Entra Identity Protection
- Protéger votre environnement grâce à Microsoft Defender pour Identity
- Sécuriser vos applications et services cloud avec Microsoft Defender pour applications cloud

2 - Atténuer les menaces à l'aide de Microsoft Defender for Endpoint

- Se protéger contre les menaces avec Microsoft Defender for Endpoint
- Déployer l'environnement Microsoft Defender pour Endpoint
- Implémenter les améliorations de sécurité de Windows
- Effectuer des enquêtes sur les appareils
- Effectuer des actions sur un appareil
- Effectuer des enquêtes sur les preuves et les entités
- Configurer et gérer l'automatisation
- Configurer les alertes et les détections
- Utiliser la gestion des vulnérabilités

3 - Atténuer les menaces à l'aide de Microsoft Security Copilot

- Introduction à l'IA générative
- Découvrir Microsoft Security Copilot et ses fonctionnalités
- Fonctionnalités de base de Copilote de sécurité Microsoft
- Expériences intégrées et usages de Microsoft Security Copilot
- Cas d'usage et bonnes pratiques avec Microsoft Security Copilot

4 - Atténuer les menaces avec Microsoft Purview

- Examiner et gérer les alertes DLP avec Microsoft Purview
- Analyser les alertes de risques internes et surveiller les activités associées
- Rechercher et enquêter sur les activités avec Microsoft Purview Audit
- Rechercher, analyser et gérer le contenu avec Microsoft Purview eDiscovery

5 - Atténuer les menaces avec Microsoft Defender pour point de terminaison

- Protéger les terminaux contre les menaces avec Microsoft Defender for Endpoint
- Déployer et configurer Microsoft Defender for Endpoint
- Renforcer la sécurité Windows avec Microsoft Defender for Endpoint
- Gérer et sécuriser les appareils avec Microsoft Defender for Endpoint
- Configurer et automatiser la sécurité avec Microsoft Defender for Endpoint
- Implémenter et optimiser la gestion des vulnérabilités avec Microsoft Defender for Endpoint

6 - Atténuer les menaces avec Microsoft Defender pour le cloud

- Planifier la protection des charges de travail Cloud avec Microsoft Defender for Cloud
- Connecter des ressources Azure à Microsoft Defender pour le Cloud
- Comprendre et expliquer les protections de charge de travail cloud dans Microsoft Defender pour le Cloud
- Corriger les alertes de sécurité avec Microsoft Defender pour le Cloud

Les objectifs de la formation

- Être capable d'expliquer comment Microsoft Defender pour Endpoint peut remédier aux risques dans votre environnement
- Configurer et utiliser Microsoft Sentinel pour détecter et répondre aux menaces
- Construire des requêtes avec Kusto Query Language (KQL) pour analyser les données de sécurité
- Intégrer les données via des connecteurs vers Microsoft Sentinel
- Créer des règles analytiques, des playbooks et automatiser des réponses aux incidents
- Chasser les menaces (threat hunting) dans Microsoft Sentinel à l'aide de notebooks et jobs de recherche
- Mitiger les risques via Microsoft Defender XDR, Defender pour Endpoint et Defender pour le cloud

Evaluation

- Pendant la formation, le formateur évalue la progression pédagogique des participants via des QCM, des mises en situation et des travaux pratiques. Les participants passent un test de positionnement avant et après la formation pour valider leurs compétences acquises.

Les points forts de la formation

- Une formation complète qui permet aux participants d'acquérir les connaissances nécessaires pour détecter et contrer les menaces de sécurité avec Microsoft Sentinel, Microsoft Defender pour le Cloud et Microsoft 365 Defender.
- Une formation rythmée durant laquelle s'alternent les phases d'apports théoriques, d'échanges, de partage d'expériences et de mises en situation.
- 82% des participants à cette formation se sont déclarés satisfaits ou très satisfaits au cours des 12 derniers mois.

Dates et villes 2026 - Référence MSSC200

Dernières places disponibles Session garantie

A distance

du 19 janv. au 22 janv.	du 18 mai au 21 mai	du 19 oct. au 22 oct.
du 23 mars au 26 mars	du 27 juil. au 30 juil.	du 7 déc. au 10 déc.

Toulouse

du 19 janv. au 22 janv.	du 18 mai au 21 mai	du 19 oct. au 22 oct.

Aix-en-Provence

du 19 janv. au 22 janv.	du 18 mai au 21 mai	du 19 oct. au 22 oct.

Rennes

du 19 janv. au 22 janv.	du 23 mars au 26 mars	du 7 déc. au 10 déc.

Paris

du 19 janv. au 22 janv.	du 18 mai au 21 mai	du 19 oct. au 22 oct.
du 23 mars au 26 mars	du 27 juil. au 30 juil.	du 7 déc. au 10 déc.

Lille

du 19 janv. au 22 janv.	du 18 mai au 21 mai	du 19 oct. au 22 oct.

Nantes

du 19 janv. au 22 janv.	du 23 mars au 26 mars	du 7 déc. au 10 déc.

Marseille

du 19 janv. au 22 janv.	du 18 mai au 21 mai	du 19 oct. au 22 oct.

Strasbourg

du 23 mars au 26 mars	du 27 juil. au 30 juil.	du 7 déc. au 10 déc.

Sophia Antipolis

du 23 mars au 26 mars	du 27 juil. au 30 juil.	du 7 déc. au 10 déc.

Rouen

du 23 mars au 26 mars	du 27 juil. au 30 juil.	du 7 déc. au 10 déc.

Lyon

du 23 mars au 26 mars	du 27 juil. au 30 juil.	du 7 déc. au 10 déc.

Bordeaux

du 23 mars au 26 mars	du 27 juil. au 30 juil.	du 7 déc. au 10 déc.