Présentiel/distanciel

Cours Officiel

Configurer des opérations de sécurité SIEM avec Microsoft Sentinel

Objectifs pédagogiques

- Configurer et gérer des espaces de travail Microsoft Sentinel
- Détecter les menaces en utilisant des règles analytiques avancées
- Automatiser les opérations de sécurité pour optimiser la réponse aux incidents

Prérequis

- Comprendre les bases de Microsoft Azure
- Connaissance élémentaire de Microsoft Sentinel
- Savoir utiliser le langage de requête Kusto (KQL) dans Microsoft Sentinel

Public concerné

Professionnels de la cybersécurité, analystes SOC, administrateurs IT, responsables sécurité, ingénieurs cloud souhaitant maîtriser Microsoft Sentinel

Certification

Cette formation est associée à la Microsoft Applied Skills « Configurer les opérations de sécurité SIEM à l'aide de Microsoft Sentinel« , validation ciblée pour les scénarios réels.
Maîtrisez les scénarios techniques à la demande pour démontrer votre compétence dans des ensembles de compétences spécifiques basés sur des scénarios afin que vous puissiez avoir un impact plus important sur chaque projet, au sein de votre organisation et dans votre carrière.

Présentiel/distanciel

Cours Officiel

Programme détaillé

Créer et gérer des espaces de travail Microsoft Sentinel (1 heure)

- Organisation de l'espace de travail Microsoft Sentinel
- Créer un espace de travail Microsoft Sentinel
- Gérer les espaces de travail parmi les locataires avec Azure Lighthouse
- Présentation des autorisations et des rôles Microsoft Sentinel
- Gestion des paramètres Microsoft Sentinel
- Configurer les journaux

Connecter des services Microsoft à Microsoft Sentinel (1 heure)

- Planifier les connecteurs de services Microsoft
- Activer le connecteur Microsoft Office 365
- Connecter le connecteur Microsoft Entra
- Connecter le connecteur Microsoft Entra ID Protection
- Se connecter au connecteur Activité Azure

Connecter des hôtes Windows à Microsoft Sentinel (0,5 heure)

- Planifier le connecteur pour les événements de sécurité des hôtes Windows
- Se connecter en utilisant le connecteur Événements de sécurité Windows via AMA
- Se connecter en utilisant le connecteur Événements de sécurité via l'agent hérité
- Collecter des journaux d'événements Sysmon

Détection des menaces avec Analytique Microsoft Sentinel (2 heures)

- Travaux pratiques : Détecter les menaces avec Analytique Microsoft Sentinel
- Qu'est-ce qu'Analytique Microsoft Sentinel ?
- Types de règles analytiques
- Créer une règle analytique à partir de modèles
- Créer une règle analytique à partir de l'Assistant
- Gérer les règles analytiques
- Travaux pratiques : Détecter les menaces avec Analytique Microsoft Sentinel

Automatisation dans Microsoft Sentinel (0,5 heure)

- Comprendre les options d'automatisation
- Créer des règles d'automatisation

Configurer les opérations de sécurité SIEM à l'aide de Microsoft Sentinel (2 heures)

- Travaux pratiques : configurer les opérations SIEM à l'aide de Microsoft Sentinel
- Travaux pratiques : installer des solutions d'hub de contenu Microsoft Sentinel et des connecteurs de données
- Travaux pratiques : configurer un connecteur de données Règle de collecte de données
- Travaux pratiques : effectuer une attaque simulée pour valider les règles d'analytique et d'automatisation

Documentation

Travaux pratiques et/ou Labo en anglais

Délais d'accès à la formation

Les inscriptions sont possibles jusqu'à 48 heures avant le début de la formation.
Dans le cas d'une formation financée par le CPF, ENI Service est tenu de respecter un délai minimum obligatoire de 11 jours ouvrés entre la date d'envoi de sa proposition et la date de début de la formation.

Modalités et moyens pédagogiques, techniques et d'encadrement

Formation avec un formateur, qui peut être suivie selon l'une des 3 modalités ci-dessous :
1 Dans la salle de cours en présence du formateur.
2 Dans l'une de nos salles de cours immersives, avec le formateur présent physiquement à distance. Les salles immersives sont équipées d'un système de visio-conférence HD et complétées par des outils pédagogiques qui garantissent le même niveau de qualité.
3 Depuis votre domicile ou votre entreprise. Vous rejoignez un environnement de formation en ligne, à l'aide de votre ordinateur, tout en étant éloigné physiquement du formateur et des autres participants. Vous êtes en totale immersion avec le groupe et participez à la formation dans les mêmes conditions que le présentiel. Pour plus d'informations : Le téléprésentiel notre solution de formation à distance.

Le nombre de stagiaires peut varier de 1 à 12 personnes (5 à 6 personnes en moyenne), ce qui facilite le suivi permanent et la proximité avec chaque stagiaire.
Chaque stagiaire dispose d'un poste de travail adapté aux besoins de la formation, d'un support de cours et/ou un manuel de référence au format numérique ou papier.
Pour une meilleure assimilation, le formateur alterne tout au long de la journée les exposés théoriques, les démonstrations et la mise en pratique au travers d'exercices et de cas concrets réalisés seul ou en groupe.

Modalités d'évaluation des acquis

En début et en fin de formation, les stagiaires réalisent une auto-évaluation de leurs connaissances et compétences en lien avec les objectifs de la formation. L'écart entre les deux évaluations permet ainsi de mesurer leurs acquis.
En complément, le formateur évalue chaque stagiaire sur l'atteinte des objectifs pédagogiques de la formation selon quatre niveaux (non évalué, non acquis, en cours d'acquisition, acquis). Cette évaluation repose sur une modalité choisie par le formateur en cohérence avec la formation : QCM, exercices pratiques réalisés pendant la formation, évaluation finale de synthèse, quiz interactif de validation, étude de cas, mise en situation, analyse de l'auto-évaluation, autres modalités adaptées.
Pour les stagiaires qui le souhaitent, certaines formations peuvent être validées officiellement par un examen de certification. Les candidats à la certification doivent produire un travail personnel important en vue de se présenter au passage de l'examen, le seul suivi de la formation ne constitue pas un élément suffisant pour garantir un bon résultat et/ou l'obtention de la certification.
Pour certaines formations certifiantes (ex : ITIL, DPO, ...), le passage de l'examen de certification est inclus et réalisé en fin de formation. Les candidats sont alors préparés par le formateur au passage de l'examen tout au long de la formation.

Moyens de suivi d'exécution et appréciation des résultats

Feuille de présence, émargée par demi-journée par chaque stagiaire et le formateur.
Evaluation qualitative de fin de formation, qui est ensuite analysée par l'équipe pédagogique ENI.
Attestation de fin de formation, remise au stagiaire en main propre ou par courrier électronique.

Qualification du formateur

La formation est animée par un professionnel de l'informatique et de la pédagogie, dont les compétences techniques, professionnelles et pédagogiques ont été validées par des certifications et/ou testées et approuvées par les éditeurs et/ou notre équipe pédagogique.
Il est en veille technologique permanente et possède plusieurs années d'expérience sur les produits, technologies et méthodes enseignés.
Il est présent auprès des stagiaires pendant toute la durée de la formation.

Accessibilité de la formation