Présentiel/distanciel | Cours Officiel | Formation certifiante

Se défendre contre les cybermenaces avec la plateforme d'opérations de sécurité Microsoft

Objectifs pédagogiques

- Investiguer et atténuer des menaces avec Microsoft Defender XDR, Microsoft Defender for Endpoint, Microsoft Defender for Cloud et Microsoft Purview
- Utiliser Microsoft Copilot for Security pour accélérer l'analyse et la réponse aux incidents
- Créer des requêtes KQL pour interroger et analyser des données de sécurité dans Microsoft Sentinel
- Configurer un environnement Microsoft Sentinel et connecter différentes sources de journaux
- Créer des détections, automatiser la réponse et conduire des investigations dans Microsoft Sentinel
- Réaliser des activités de threat hunting avec Microsoft Sentinel

Prérequis

- Compréhension de base de Microsoft 365
- Compréhension fondamentale des produits Microsoft de sécurité, conformité et identité
- Compréhension intermédiaire de Microsoft Windows
- Familiarité avec les services Azure, notamment Azure SQL Database et Azure Storage
- Familiarité avec les machines virtuelles Azure et les réseaux virtuels Azure
- Compréhension de base des concepts de scripting

Certification

Cette formation prépare à l'examen**SC-200**, qui permet d'obtenir la certification Microsoft Certified: Security Operations Analyst Associate

Public concerné

Cette formation s'adresse aux analystes des opérations de sécurité, ingénieurs SOC et professionnels de la cybersécurité chargés de détecter, analyser, investiguer et traiter les menaces dans l'environnement de leur organisation.
Elle concerne les personnes qui utilisent Microsoft Sentinel, Microsoft Defender XDR, Microsoft Defender for Endpoint, Microsoft Defender for Cloud, Microsoft Purview et Microsoft Copilot for Security pour réduire les risques, améliorer la détection et accélérer la réponse aux incidents.

Bénéfices pour les participants :

- Développer une approche opérationnelle de détection, d'investigation et de réponse aux menaces avec l'écosystème Microsoft Security
- Renforcer la maîtrise des outils Microsoft de sécurité dans un contexte SOC moderne
- Acquérir des compétences directement applicables sur les scénarios de surveillance, d'investigation et de chasse aux menaces

Programme détaillé

Atténuer les menaces avec Microsoft Defender XDR (3h00)

- Introduction à la protection contre les menaces dans Microsoft 365
- Atténuer les incidents avec Microsoft Defender XDR
- Protéger les identités avec Entra ID Protection
- Corriger les risques avec Microsoft Defender for Office 365
- Sécuriser l'environnement avec Microsoft Defender for Identity
- Sécuriser les applications et services cloud avec Microsoft Defender for Cloud Apps
- Travail pratique :
  - Explorer Microsoft Defender XDR

Prise en main de Microsoft Copilot for Security (2h00)

- Fondamentaux de l'IA générative
- Décrire Microsoft Copilot for Security
- Décrire les fonctionnalités principales de Microsoft Copilot for Security
- Décrire les expériences intégrées de Microsoft Copilot for Security
- Travail pratique :
  - Simulations Microsoft Security Copilot

Atténuer les menaces avec Microsoft Purview (2h00)

- Solutions de conformité Microsoft Purview
- Répondre aux alertes de prévention contre la perte de données avec Microsoft Purview
- Gérer le risque interne dans Microsoft Purview
- Investiguer les menaces avec Content search dans Microsoft Purview
- Investiguer les menaces avec Microsoft Purview Audit
- Travail pratique :
  - Explorer les journaux d'audit Microsoft Purview

Atténuer les menaces avec Microsoft Defender for Endpoint (3h00)

- Se protéger contre les menaces avec Microsoft Defender for Endpoint
- Déployer l'environnement Microsoft Defender for Endpoint
- Mettre en oeuvre les améliorations de sécurité Windows avec Microsoft Defender for Endpoint
- Effectuer des investigations sur les appareils dans Microsoft Defender for Endpoint
- Effectuer des actions sur un appareil avec Microsoft Defender for Endpoint
- Effectuer des investigations sur les preuves et entités avec Microsoft Defender for Endpoint
- Configurer et gérer l'automatisation avec Microsoft Defender for Endpoint
- Configurer les alertes et détections dans Microsoft Defender for Endpoint
- Utiliser la gestion des vulnérabilités dans Microsoft Defender for Endpoint
- Travail pratique :
  - Déployer Microsoft Defender for Endpoint
  - Atténuer des attaques avec Microsoft Defender for Endpoint

Atténuer les menaces avec Microsoft Defender for Cloud (2h00)

- Planifier la protection des charges de travail cloud avec Microsoft Defender for Cloud
- Connecter des ressources Azure à Microsoft Defender for Cloud
- Connecter des ressources non Azure à Microsoft Defender for Cloud
- Gérer la posture de sécurité cloud
- Expliquer les protections des charges de travail cloud dans Microsoft Defender for Cloud
- Corriger les alertes de sécurité avec Microsoft Defender for Cloud
- Travail pratique :
  - Activer Microsoft Defender for Cloud

Créer des requêtes pour Microsoft Sentinel avec Kusto Query Language (KQL) (3h00)

- Construire des instructions KQL pour Microsoft Sentinel
- Analyser les résultats de requête avec KQL
- Créer des instructions multi-tables avec KQL
- Travailler avec les données dans Microsoft Sentinel avec Kusto Query Language
- Travail pratique :
  - Créer des requêtes KQL Microsoft Sentinel

Configurer votre environnement Microsoft Sentinel (2h00)

- Introduction à Microsoft Sentinel
- Créer et gérer des espaces de travail Microsoft Sentinel
- Interroger les journaux dans Microsoft Sentinel
- Utiliser les watchlists dans Microsoft Sentinel
- Utiliser le renseignement sur les menaces dans Microsoft Sentinel
- Intégrer Microsoft Defender XDR à Microsoft Sentinel
- Travail pratique :
  - Déployer Microsoft Sentinel

Connecter les journaux à Microsoft Sentinel (3h00)

- Connecter les données à Microsoft Sentinel avec les connecteurs de données
- Connecter les services Microsoft à Microsoft Sentinel
- Connecter Microsoft Defender XDR à Microsoft Sentinel
- Connecter des hôtes Windows à Microsoft Sentinel
- Connecter les journaux Common Event Format à Microsoft Sentinel
- Connecter les sources de données Syslog à Microsoft Sentinel
- Connecter les indicateurs de menace à Microsoft Sentinel
- Travail pratique :
  - Connecter des services à Microsoft Sentinel
  - Connecter des hôtes Windows à Microsoft Sentinel

Créer des détections et effectuer des investigations avec

Microsoft Sentinel (4h00)

- Détection des menaces avec les règles analytiques Microsoft Sentinel
- Automatisation dans Microsoft Sentinel
- Réponse aux menaces avec les playbooks Microsoft Sentinel
- Gestion des incidents de sécurité dans Microsoft Sentinel
- Identifier les menaces avec Entity behavioral analytics dans Microsoft Sentinel
- Normalisation des données dans Microsoft Sentinel
- Interroger, visualiser et superviser les données dans Microsoft Sentinel
- Gérer le contenu dans Microsoft Sentinel
- Travail pratique :
  - Créer une règle de sécurité
  - Créer un playbook
  - Créer une requête planifiée à partir d'un modèle
  - Créer une requête planifiée
  - Créer une règle Near Real Time
  - Effectuer des attaques simulées
  - Créer des détections

Effectuer de la chasse aux menaces avec Microsoft Sentinel (4h00)

- Expliquer les concepts de threat hunting dans Microsoft Sentinel
- Effectuer du threat hunting avec Microsoft Sentinel
- Utiliser les Search jobs dans Microsoft Sentinel
- Rechercher des menaces avec les notebooks dans Microsoft Sentinel
- Travail pratique :
  - Threat hunting dans Microsoft Sentinel

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, 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