ENI Service

référence
T126-SC200

28h

Microsoft Sécurité Analyste des opérations

Mise à jour
17 juillet 2023

2690 € HT

(Télé-)présentiel Cours Officiel Formation certifiante

Microsoft Sécurité Analyste des opérations

Objectifs

- Créer un environnement Microsoft Defender pour Endpoint
- Configurer les règles de réduction de la surface d'attaque sur les appareils Windows 10
- Rechercher des domaines et des adresses IP Microsoft Defender pour Endpoint
- Enquêter sur les comptes utilisateurs dans Microsoft Defender pour Endpoint
- Configurer les paramètres d'alerte dans Microsoft Defender pour Endpoint
- Gérer les incidents dans Microsoft 365 Defender
- Examiner les alertes DLP dans Microsoft Cloud App Security
- Configurer l'auto-provisioning dans Azure Defender
- Remédier aux alertes dans Azure Defender
- Construire des instructions KQL
- Gérer un espace de travail Azure Sentinel
- Utiliser KQL pour accéder à la liste de surveillance dans Azure Sentinel
- Gérer les indicateurs de menace dans Azure Sentinel
- Configurer l'agent Log Analytics pour collecter les événements Sysmon
- Créer de nouvelles règles et requêtes d'analyse à l'aide de l'assistant de règles d'analyse
- Utiliser des requêtes pour rechercher des menaces

Pré-requis

- Connaissances de base de l'environnement Microsoft 365
- Connaissances de base sur les produits de sécurité, de conformité et d'identité de Microsoft
- Connaissance de Windows 10
- Être familiarisé avec certains services Azure, notamment Azure SQL Database et Azure Storage
- Connaissances autour des machines virtuelles Azure et les réseaux virtuels.
- Connaissance de bases sur le Scripting

Il est recommandé d'avoir suivi la formation Microsoft Sécurité Notions fondamentales sur l'identité, la conformité et la sécurité ou de posséder les connaissances équivalentes

Certification

Cette formation prépare à l'examen "Microsoft Security Operations Analyst" qui permet d'obtenir la certification Microsoft Certified : Security Operations Analyst Associate

Public

L'analyste des opérations de sécurité de Microsoft collabore avec les parties prenantes de l'organisation pour sécuriser les systèmes de technologie de l'information de l'organisation.
Son objectif est de réduire le risque organisationnel en remédiant rapidement aux attaques actives dans l'environnement, en donnant des conseils sur les améliorations à apporter aux pratiques de protection contre les menaces et en signalant les violations des politiques organisationnelles aux parties prenantes appropriées.
Les responsabilités comprennent la gestion, la surveillance et la réponse aux menaces en utilisant une variété de solutions de sécurité dans leur environnement.
Le rôle consiste principalement à enquêter sur les menaces, à y répondre et à les chasser en utilisant Microsoft Azure Sentinel, Azure Defender, Microsoft 365 Defender et des produits de sécurité tiers.

Programme de la formation

Atténuation des menaces à l'aide de Microsoft Defender pour Endpoint

- Se protéger contre les menaces avec Microsoft Defender pour Endpoint
- Déployer l'environnement Microsoft Defender pour Endpoint
- Mettre en oeuvre les améliorations de sécurité de Windows 10 avec Microsoft Defender pour Endpoint
- Gérer les alertes et les incidents dans Microsoft Defender pour Endpoint
- Effectuer des investigations sur les périphériques dans Microsoft Defender pour Endpoint
- Exécuter des actions sur un périphérique à l'aide de Microsoft Defender pour Endpoint
- Effectuer des enquêtes sur les preuves et les entités à l'aide de Microsoft Defender pour Endpoint
- Configurer et gérer l'automatisation à l'aide de Microsoft Defender pour Endpoint
- Configurer les alertes et les détections dans Microsoft Defender pour Endpoint
- Utiliser la gestion des menaces et des vulnérabilités dans Microsoft Defender pour Endpoint
- Travaux pratiques : Atténuer les menaces à l'aide de Microsoft Defender pour Endpoint
  - Déployer Microsoft Defender pour Endpoint
  - Atténuer les attaques à l'aide de Defender for Endpoint

Atténuation des menaces à l'aide de Microsoft 365 Defender

- Introduction à la protection contre les menaces avec Microsoft 365
- Atténuer les incidents à l'aide de Microsoft 365 Defender
- Protéger vos identités avec Azure AD Identity Protection
- Remédier aux risques avec Microsoft Defender pour Office 365
- Protection de votre environnement avec Microsoft Defender for Identity
- Sécurisez vos applications et services en nuage avec Microsoft Cloud App Security
- Répondre aux alertes de prévention des pertes de données avec Microsoft 365
- Gérez les risques liés aux initiés dans Microsoft 365
- Travaux pratiques : Atténuer les menaces avec Microsoft 365 Defender
  - Atténuer les attaques avec Microsoft 365 Defender

Atténuer les menaces à l'aide de Azure Defender

- Planifier les protections des charges de travail en nuage à l'aide de Azure Defender
- Expliquer les protections des charges de travail en nuage dans Azure Defender.
- Connecter les ressources Azure à Azure Defender
- Connecter les ressources non-Azure à Azure Defender
- Corriger les alertes de sécurité à l'aide de Azure Defender
- Travaux pratiques : Atténuer les menaces à l'aide de Azure Defender
  - Déployer Azure Defender
  - Atténuer les attaques avec Azure Defender

Configuration de votre environnement Azure Sentinel

- Introduction à Azure Sentinel
- Créer et gérer les espaces de travail Azure Sentinel
- Interroger les journaux dans Azure Sentinel
- Utiliser les listes de surveillance dans Azure Sentinel
- Utiliser les renseignements sur les menaces dans Azure Sentinel
- Travaux pratiques : Configurer votre environnement Azure Sentinel
  - Créer un espace de travail Azure Sentinel
  - Créer une liste de surveillance
  - Créer un indicateur de menace

Connecter les journaux à Azure Sentinel

- Connecter des données à Azure Sentinel à l'aide de connecteurs de données
- Connecter les services Microsoft à Azure Sentinel
- Connecter Microsoft 365 Defender à Azure Sentinel
- Connecter les hôtes Windows à Azure Sentinel
- Connecter les journaux Common Event Format à Azure Sentinel
- Connecter des sources de données syslog à Azure Sentinel
- Connecter les indicateurs de menace à Azure Sentinel
- Travaux pratiques : Connecter les journaux à Azure Sentinel
  - Connecter les services Microsoft à Azure Sentinel
  - Connecter les hôtes Windows à Azure Sentinel
  - Connecter les hôtes Linux à Azure Sentinel
  - Connecter les renseignements sur les menaces à Azure Sentinel

Créer des détections et effectuer des investigations à l'aide de Azure Sentinel

- Détection des menaces avec les analyses de Azure Sentinel
- Réponse aux menaces avec les manuels Azure Sentinel
- Gestion des incidents de sécurité dans Azure Sentinel
- Utiliser l'analyse du comportement des entités dans Azure Sentinel
- Interroger, visualiser et surveiller les données dans Azure Sentinel
- Travaux pratiques : Créer des détections et effectuer des enquêtes en utilisant Azure Sentinel
  - Créer des règles analytiques
  - Modéliser les attaques pour définir la logique des règles
  - Atténuer les attaques à l'aide de Azure Sentinel
  - Créer des classeurs dans Azure Sentinel

Effectuer la chasse aux menaces dans Azure Sentinel

- Chasse aux menaces avec Azure Sentinel

- Chasse aux menaces à l'aide de notebooks dans Azure Sentinel
- Travaux pratiques : Chasse aux menaces dans Azure Sentinel
  - Chasse aux menaces dans Azure Sentinel
  - Chasse aux menaces à l'aide de notebooks

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, 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.