

Certifiante Sessions garanties disponibles

Formation Analyste des opérations de sécurité Microsoft (SC-200)

Réf. SF33997

4 jours de formation pour maîtriser les outils de sécurité Microsoft !

4 j Durée	3 000 € HT Inter / participant	9 800 € HT Intra (≤12 pers.)	2 Sessions à venir
--------------	-----------------------------------	---------------------------------	-----------------------

Objectifs pédagogiques

- ✓ Gérer un environnement d'opérations de sécurité
- ✓ Configurer des protections et des détections
- ✓ Gérer les réponses aux incidents
- ✓ Effectuer un repérage des menaces

Public visé & prérequis

Public visé Administrateurs systèmes et réseaux

Prérequis Compréhension de base de Microsoft 365. Compréhension fondamentale des produits de sécurité, de conformité et d'identité de Microsoft. Compréhension intermédiaire de Windows 10. Familiarité avec les services Azure, en particulier Azure SQL Database et Azure Storage. Familiarité avec les machines virtuelles Azure et les réseaux virtuels. Compréhension de base des concepts de script.

Programme détaillé

Configurer des paramètres dans Microsoft Defender XDR

Configurer une connexion à partir de Defender XDR à un espace de travail Sentinel
Configurer une règle et des règles de notification des vulnérabilités
Configurer des fonctionnalités avancées de Microsoft Defender for Endpoint
Configurer des paramètres de règles de point de terminaison, notamment les indicateurs et le filtrage de contenu web
Gérer les fonctionnalités d'enquête et de réponse automatisées dans Microsoft Defender XDR
Configurer l'interruption automatique des attaques dans Microsoft Defender XDR

Gérer des ressources et des environnements

Configurer et gérer des groupes d'appareils, des autorisations et des niveaux d'automatisation dans Microsoft Defender for Endpoint
Identifier et corriger les appareils non gérés dans Microsoft Defender for Endpoint
Gérer des ressources en utilisant Azure Arc
Connecter des environnements à Microsoft Defender pour le cloud (en utilisant la gestion de comptes multiclouds)
Découvrir et corriger des ressources non protégées en tirant parti de Defender pour le cloud
Identifier et corriger des appareils en utilisant la Gestion des vulnérabilités Microsoft Defender

Concevoir et configurer un espace de travail Microsoft Sentinel

Planifier un espace de travail Microsoft Sentinel
Configurer des rôles Microsoft Sentinel
Spécifier des rôles RBAC Azure pour la configuration de Microsoft Sentinel
Concevoir et configurer le stockage de données Microsoft Sentinel, notamment les types de journaux et la conservation des journaux
Gérer plusieurs espaces de travail en tirant parti du gestionnaire d'espaces de travail et d'Azure Lighthouse

Ingérer des sources de données dans Microsoft Sentinel

Identifier les sources de données à ingérer pour Microsoft Sentinel
Implémenter et utiliser des solutions de hub de contenu

Configurer et utiliser des connecteurs Microsoft pour les ressources Azure, notamment Azure Policy et les paramètres de diagnostic
Configurer une synchronisation bidirectionnelle entre Microsoft Sentinel et Microsoft Defender XDR
Planifier et configurer des collections d'événements Syslog et CEF (Common Event Format)
Planifier et configurer une collecte d'événements Sécurité Windows en tirant parti de règles de collecte de données, notamment le transfert d'événements Windows (WEF)
Configurer des connecteurs de veille des menaces, notamment la plateforme, TAXII, l'API de chargement des indicateurs et MISP
Créer des tables de journaux personnalisées dans l'espace de travail pour stocker les données ingérées

Configurer des protections dans les technologies de sécurité Microsoft Defender

Configurer des stratégies dans Microsoft Defender pour les applications cloud
Configurer des stratégies dans Microsoft Defender pour Office
Configurer des stratégies de sécurité pour Microsoft Defender for Endpoint, notamment les règles de réduction de la surface d'attaque (ASR)
Configurer des protections de charge de travail cloud dans Microsoft Defender pour le cloud

Configurer la détection dans Microsoft Defender XDR

Configurer et gérer des détections personnalisées
Configurer le réglage d'alertes
Configurer des règles d'imposture dans Microsoft Defender XDR

Configurer des détections dans Microsoft Sentinel

Classifier et analyser des données à l'aide d'entités
Configurer des règles de requête planifiées, notamment KQL
Configurer des règles de requêtes en quasi-temps réel (NRT), notamment KQL
Gérer les règles d'analytique à partir du hub de contenu
Configurer des règles d'analytique de détection d'anomalie
Configurer la règle Fusion
Interroger des données Microsoft Sentinel en utilisant des analyseurs ASIM
Gérer et utiliser des indicateurs de menace

Répondre aux alertes et aux incidents dans Microsoft Defender XDR

Enquêter et corriger des menaces visant Microsoft Teams, SharePoint Online et OneDrive
Enquêter et corriger des menaces dans les e-mails en utilisant Microsoft Defender pour Office
Enquêter et corriger des incidents de compromission d'e-mails professionnels et de rançongiciel identifiés par une interruption automatique d'attaque
Examiner et corriger les entités compromises identifiées par les stratégies de protection contre la perte de données (DLP) Microsoft Purview
Enquêter et corriger des menaces identifiées par des stratégies de risque interne Microsoft Purview
Enquêter et corriger des alertes et des incidents identifiés par Microsoft Defender pour le cloud
Enquêter et corriger des risques de sécurité identifiés par Microsoft Defender pour les applications cloud
Enquêter et corriger des identités compromises dans Microsoft Entra ID
Enquêter et corriger des alertes de sécurité de Microsoft Defender pour Identity
Gérer des actions et des soumissions dans le portail Microsoft Defender

Répondre aux alertes et aux incidents identifiés par Microsoft Defender for Endpoint

Enquêter une chronologie des appareils compromis
Effectuer des actions sur l'appareil, y compris la réponse dynamique et la collecte de packages d'investigation
Effectuer des enquêtes d'entités et de preuves

Enrichir des enquêtes en utilisant d'autres outils Microsoft

Enquêter sur des menaces en utilisant un journal d'audit unifié
Enquêter sur des menaces en tirant parti de Recherche de contenu
Effectuer un repérage des menaces en utilisant des journaux d'activité Microsoft Graph

Gérer les incidents dans Microsoft Sentinel

Trier les incidents dans Microsoft Sentinel
Investiguer les incidents dans Microsoft Sentinel

Configurer l'orchestration, automatisation et réponse dans le domaine de la sécurité (SOAR, Security Orchestration, Automation, and Response) dans Microsoft Sentinel

- Créer et configurer des règles d'automatisation
- Créer et configurer des playbooks Microsoft Sentinel
- Configurer des règles analytiques pour déclencher l'automatisation
- Déclencher manuellement des playbooks à partir d'alertes et d'incidents
- Exécuter des playbooks sur des ressources locales

Repérer des menaces en utilisant KQL

- Identifier les menaces à l'aide de Langage de requête Kusto (KQL)
- Interpréter les analyses de menaces dans le portail Microsoft Defender
- Créer des requêtes de repérage personnalisées en tirant parti de KQL

Effectuer un repérage des menaces avec Microsoft Sentinel

- Analyser la couverture de vecteurs d'attaque en utilisant MITRE ATT&CK dans Microsoft Sentinel
- Personnaliser les requêtes de repérage de la galerie de contenu
- Utiliser des signets de repérage pour les investigations de données
- Superviser des requêtes de repérage à l'aide de Livestream
- Récupérer et gérer les données de journaux archivées
- Créer et gérer des travaux de recherche

Analyser et interpréter des données en utilisant des classeurs

- Activer et personnaliser des modèles de classeur Microsoft Sentinel
- Créer des classeurs personnalisés qui incluent KQL
- Configurer des visualisations

Prochaines sessions

DATE	LIEU	STATUT
07/12/2026	à distance	Sur confirmation
15/03/2027	à distance	Sur confirmation

Pourquoi choisir Sparks Formation ?

20 ans d'expertise IT, des formateurs experts et des sessions garanties contre l'annulation.

20 ans
d'expertise

1 068+
formations

11 178
apprenants formés/an

+67
Net Promoter Score

Avis des participants

Note moyenne des participants de l'ensemble de nos formations : 4,9/5 — 735 avis

Berenice P. — formatrice agréable à l'écoute bonne pédagogie j'ai beaucoup apprécié nos échanges

Anne-Lise C. — Très bonne adaptation du formateur au public et au niveau d'attente.

Votre formateur

Loic D. — Formateur Microsoft Azure & Windows

Loic intervient sur des formations portant sur Microsoft Azure. Les sujets abordés incluent notamment Windows. Son activité de formation remonte à 2018.

Ils nous font confiance

Cette année notre filière Microsoft Azure a accompagné plus de 28 entreprises dont :

SILAE EPSILON FRANCE GERFLOR SAS LEMONWAY MALAKOFF HUMANIS AMAP ACENSI SANA ALIAPUR ALTECA APSIDE TOP AREAS
ASSURANCES +18 autres

Financement & certifications

Cette formation est éligible aux financements OPCO et FNE-Formation. Nos équipes vous accompagnent dans le montage de votre dossier.



Réservez votre place dès maintenant

20 ans d'expertise · 1 000+ formations · NPS +67 · réponse sous 24h ouvrées

0 805 950 800

demande@sparks-formation.com