Analyse et Opérations de Sécurité avec Microsoft Defender et Sentinel

Lien : https://innov-systems.com/formation/analyse-et-operations-de-securite-avec-microsoft-defender-et-sentinel

DURÉE
5 jours (35h)

RÉFÉRENCE
SEC316

CATÉGORIE
Sécurité des Systèmes et Serveurs

Innov Systems

OBJECTIFS DE LA FORMATION

À l'issue de cette formation, vous serez capable de :

- Comprendre le rôle et les responsabilités de l’analyste des opérations de sécurité dans l’écosystème Microsoft
- Déployer et configurer Microsoft Defender pour protéger les terminaux, identités et applications cloud
- Maîtriser les techniques d’investigation, de corrélation et de réponse aux incidents à l’aide de Microsoft 365 Defender
- Utiliser Azure Sentinel pour collecter, analyser et corréler les événements de sécurité à grande échelle
- Concevoir et automatiser des scénarios de détection et de réponse à l’aide du langage KQL et des playbooks Sentinel
- Développer des stratégies de chasse proactive aux menaces et d’amélioration continue des défenses

POUR QUI ?

- Analystes SOC
- Administrateurs Sécurité
- Responsables de la supervision des menaces et incidents
- Professionnels IT en charge de la sécurité Microsoft 365 ou Azure

Innov Systems

Programme détaillé

1 / INTRODUCTION AUX OPÉRATIONS DE SÉCURITÉ MICROSOFT

- Rôle et responsabilités de l’analyste de sécurité
- Écosystème Microsoft Security et intégration entre les solutions Defender et Sentinel
- Cycle de vie d’un incident : détection, analyse, réponse, amélioration

2 / PRISE EN MAIN DE MICROSOFT DEFENDER POUR ENDPOINT

- Déploiement et configuration initiale de Microsoft Defender for Endpoint
- Gestion des capteurs et intégration des machines
- Analyse des alertes et incidents de sécurité

3 / SÉCURISATION DES TERMINAUX WINDOWS

- Configuration des règles de réduction de la surface d’attaque (ASR)
- Protection contre les vulnérabilités et gestion corrective
- Analyse et remédiation des menaces sur les endpoints

4 / ARCHITECTURE ET COMPOSANTS DE MICROSOFT 365 DEFENDER

- Intégration de Defender for Identity, Defender for Office 365 et Cloud App Security
- Gestion des identités à risques avec Azure AD Identity Protection
- Détection et remédiation des attaques basées sur les identités

5 / INVESTIGATION ET RÉPONSE AUX INCIDENTS

- Gestion et priorisation des incidents dans Microsoft 365 Defender
- Analyse des entités, preuves et corrélations entre les services
- Automatisation des réponses via des actions manuelles et guidées

Innov Systems

6 / GESTION DU RISQUE ET DE LA CONFORMITÉ

- Supervision des alertes DLP et risques d’initiés
- Mise en œuvre de stratégies de protection des données dans Microsoft 365
- Corrélation des événements de conformité et de sécurité

7 / INTRODUCTION À AZURE DEFENDER

- Positionnement d’Azure Defender dans la défense cloud
- Connecter et protéger les ressources Azure et non-Azure
- Planification des protections de charge de travail (VM, App Services, SQL, etc.)

8 / INVESTIGATION ET CORRÉLATION DANS AZURE DEFENDER

- Lecture et interprétation des alertes de sécurité
- Analyse des menaces et recommandations de correction
- Intégration avec Microsoft 365 Defender et Azure Sentinel

9 / AUTOMATISATION DES RÉPONSES DANS AZURE DEFENDER

- Création de politiques automatiques de correction
- Configuration du provisionnement automatique
- Centralisation de la visibilité et du reporting

10 / INTRODUCTION AU LANGAGE DE REQUÊTE KUSTO (KQL)

- Syntaxe, opérateurs et structure d’une requête KQL
- Filtres, agrégations et fonctions de base
- Analyse des événements et création de rapports dynamiques

11 / ANALYSE AVANCÉE AVEC KQL DANS AZURE SENTINEL

- Requêtes multi-tables et corrélations complexes
- Extraction de chaînes non structurées et enrichissement des données

Inov Systems

- Utilisation de KQL pour la chasse aux menaces

12 / CRÉATION DE RÈGLES D’ANALYSE ET DÉTECTIONS PERSONNALISÉES

- Utilisation de l’assistant de création de règle
- Définition des seuils, fréquences et filtres contextuels
- Test et validation des détections avant déploiement

13 / CONFIGURATION ET ADMINISTRATION D’AZURE SENTINEL

- Création et gestion d’espaces de travail
- Connexion des sources de données (Microsoft 365, Syslog, CEF)
- Gestion des connecteurs et des indicateurs de menace

14 / AUTOMATISATION ET RÉPONSE AUX INCIDENTS

- Création de playbooks automatisés avec Logic Apps
- Intégration de workflows de réponse adaptative
- Orchestration des alertes et notifications

15 / CHASSE AUX MENACES ET ANALYSE CONTINUE

- Méthodologie de chasse proactive dans Sentinel
- Utilisation des blocs-notes et visualisations interactives
- Analyse comportementale et amélioration continue des détections

Inov Systems

Approche pédagogique

- Support Ecrit et Projection
- Exposés Interactifs, Podcasts et Vidéos
- Brainstorming et Jeux de Rôle
- Cas Pratiques et Labs inclus pour leur impact opérationnel
- Test de Validation des Acquis des Connaissances

Prochaines dates programmées

16 au 20 Nov. 2026	Distanciel
01 au 05 Fév. 2027	Présentiel - Casablanca
29 Mars au 02 Avr. 2027	Présentiel - Casablanca
24 au 28 Mai 2027	Présentiel - Casablanca
19 au 23 Juil. 2027	Présentiel - Casablanca

Autres dates possibles sur demande. Contactez-nous pour organiser une session intra-entreprise.

Réservation & Renseignements

Téléphone : +212 522 247 210
Email : contact@innov-systems.com
Web : https//www.innov-systems.com

Innov Systems — Tous droits réservés