Analyse des Opérations de Sécurité dans Microsoft 365 et Azure Sentinel

DURÉE
5 jours (35h)

RÉFÉRENCE
SEC318

CATÉGORIE
Sécurité des Systèmes, Sécurité des Serveurs

OBJECTIFS DE LA FORMATION

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

- Comprendre en profondeur les principes et outils de détection, d’analyse et de réponse aux menaces dans les environnements Microsoft 365 et Azure
- Configurer, corréler et automatiser les opérations de sécurité à l’aide de Microsoft Defender, Azure Defender et Azure Sentinel
- Développer des compétences avancées en requêtage KQL et en création de playbooks d’automatisation de la réponse aux incidents
- Améliorer la posture de sécurité organisationnelle à travers la surveillance proactive, la chasse aux menaces et la remédiation automatisée

POUR QUI ?

- Administrateurs systèmes et réseaux responsables de la sécurité dans les environnements Microsoft
- Analystes SOC souhaitant renforcer leurs compétences sur les solutions de sécurité Microsoft 365 et Azure
- Responsables sécurité IT et ingénieurs cybersécurité cherchant à automatiser et industrialiser les opérations de sécurité

Programme détaillé

1/ COMPRÉHENSION DES PRINCIPES DE LA SÉCURITÉ MICROSOFT

- Cadre de sécurité Microsoft 365 et Azure
- Concepts clés : XDR, SIEM, SOAR, Zero Trust
- Rôle des différents outils de la suite Microsoft Security

2/ DÉCOUVERTE DE MICROSOFT DEFENDER POUR ENDPOINT

- Architecture et composants
- Déploiement initial et intégration à Microsoft 365
- Configuration des paramètres d’alerte et de détection

3/ EXPLORATION DES MENACES ET DES INCIDENTS

- Navigation dans le portail de sécurité
- Analyse des alertes, incidents et entités
- Corrélation et priorisation des alertes

4/ GESTION DES RISQUES ET DE LA PROTECTION IDENTITAIRE

- Sécurisation des identités avec Microsoft Entra ID Protection
- Détection des comportements suspects et gestion des accès à risque
- Bonnes pratiques de durcissement de la sécurité des identités

5/ DÉTECTION ET RÉPONSE DANS MICROSOFT 365 DEFENDER

- Analyse et réponse aux incidents multi-services
- Exploitation des tableaux de bord et rapports de sécurité
- Gestion proactive des menaces et des vulnérabilités

6/ AUTOMATISATION DE LA RÉPONSE AUX INCIDENTS

- Présentation des capacités SOAR de Microsoft
- Création et test de flux automatisés simples
- Exemples d’automatisation pour les alertes répétitives

7/ INTRODUCTION À LA SÉCURITÉ DES RESSOURCES CLOUD

- Panorama des menaces dans les environnements Azure
- Protection des ressources IaaS, PaaS et hybrides
- Rôles et intégration d’Azure Defender

8/ CONFIGURATION ET SUPERVISION D’AZURE DEFENDER

- Connexion des ressources Azure et non-Azure
- Suivi et correction des alertes de sécurité
- Tableau de bord et recommandations de sécurité

9/ OPTIMISATION DE LA POSTURE DE SÉCURITÉ

- Évaluation continue de la conformité
- Bonnes pratiques pour la remédiation automatisée
- Intégration avec les services Microsoft 365 Defender

10/ FONDAMENTAUX DU LANGAGE KUSTO (KQL)

- Syntaxe et opérateurs de base
- Requêtes mono-table et multi-table
- Filtres avancés : gravité, domaine, utilisateur, IP

11/ ANALYSE ET INTERPRÉTATION DES DONNÉES

- Visualisation et tableaux interactifs
- Corrélation d’événements et recherche de modèles

- Construction de tableaux de bord personnalisés

12/ INTÉGRATION ET CONNECTEURS DE DONNÉES

- Connexion des journaux de sécurité (Syslog, CEF)
- Liaison avec Microsoft 365 Defender et Azure Defender
- Bonnes pratiques pour la collecte et la normalisation des logs

13/ GESTION DES INCIDENTS ET DES PLAYBOOKS

- Création et déploiement de playbooks dans Azure Sentinel
- Réponse automatisée aux incidents : scénarios pratiques
- Suivi et amélioration continue des automatisations

14/ CHASSE AUX MENACES DANS AZURE SENTINEL

- Principes et méthodologie de la threat hunting
- Utilisation des blocs-notes et notebooks pour l'investigation
- Recherche proactive de compromissions (IOC, TTP)

15/ SIMULATION D'INCIDENTS ET BONNES PRATIQUES

- Cas pratique : de la détection à la remédiation
- Coordination avec les équipes IT et SOC
- Évaluation de la maturité et pistes d'amélioration

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

08 au 12 Juin 2026	Casablanca - Maroc
03 au 07 Août 2026	Casablanca - Maroc
28 Sep. au 02 Oct. 2026	Casablanca - Maroc
23 au 27 Nov. 2026	Casablanca - Maroc

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

Scannez pour accéder à la fiche en ligne