Microsoft SC-200 : devenez analyste SOC expert en détection et réponse aux cybermenaces

Lien : https://innov-maroc.com/formation/microsoft-sc-200-devenez-analyste-soc-expert-en-detection-et-reponse-aux-cybermenaces

DURÉE	RÉFÉRENCE	CATÉGORIE
5 jours (35h)	**SI43**	**SIEM, SOC et LogPoint**

OBJECTIFS DE LA FORMATION

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

- Comprendre le rôle d’un analyste SOC
- Maîtriser les outils Microsoft de cybersécurité (Defender, Sentinel)
- Détecter et analyser les menaces informatiques
- Mener des investigations sur incidents de sécurité
- Répondre efficacement aux cyberattaques
- Utiliser les requêtes KQL dans Microsoft Sentinel
- Mettre en place des mécanismes d’automatisation des réponses
- Améliorer la surveillance et la détection des menaces
- Renforcer la posture de cybersécurité de l’organisation
- Se préparer à la certification Microsoft SC-200

POUR QUI ?

- Analystes SOC (Security Operations Center)
- Ingénieurs cybersécurité
- Administrateurs systèmes et réseaux
- Techniciens support sécurité
- Responsables IT sécurité
- Professionnels en reconversion vers la cybersécurité
- Toute personne souhaitant devenir analyste des opérations de sécurité Microsoft

Programme détaillé

1 / Introduction à la cybersécurité et au rôle du SOC

- Fonctionnement d’un Security Operations Center (SOC)
- Missions de l’analyste SOC
- Chaîne de gestion des incidents

2 / Présentation de Microsoft Security Stack

- Microsoft Defender XDR
- Microsoft Sentinel
- Microsoft 365 Defender

3 / Collecte et analyse des données de sécurité

- Sources de logs
- Ingestion des données
- Corrélation des événements

4 / Détection des menaces

- Règles de détection
- Alertes de sécurité
- Analyse comportementale

5 / Investigation des incidents

- Analyse des alertes
- Investigation guidée
- Identification des attaques

6 / Réponse aux incidents de sécurité

- Containment et mitigation
- Playbooks de réponse
- Gestion des priorités

7 / Gestion des menaces avancées (APT)

- Techniques d’attaque avancées
- Indicateurs de compromission (IOC)
- Threat intelligence

8 / Utilisation de Microsoft Sentinel

- Création de requêtes KQL
- Workbooks et dashboards
- Automatisation des réponses

9 / Automatisation et orchestration des réponses

- SOAR (Security Orchestration)
- Playbooks automatisés
- Optimisation des temps de réponse

10 / Amélioration continue et reporting SOC

- KPI de sécurité
- Rapport d’incidents

- Optimisation du dispositif SOC

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

09 au 13 Nov. 2026	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-maroc.com
Web : https//www.innov-maroc.com