Formation Sentinel : Configurer les opérations de sécurité SIEM avec Microsoft

Introduction à Microsoft Sentinel

- Présentation de Microsoft Sentinel comme solution SIEM
- Architecture et intégration dans Azure

Création et gestion des espaces de travail Sentinel

- Création d'un espace de travail Log Analytics
- Activation de Microsoft Sentinel
- Gestion des autorisations et des ressources

Connexion des services Microsoft

- Connecteurs de données intégrés (Microsoft 365, Azure AD, etc.)
- Configuration des permissions et intégration fluide

Connexion des hôtes Windows

- Collecte des journaux d'événements de sécurité
- Installation et configuration des agents sur les hôtes

Détection des menaces avec Microsoft Sentinel

- Utilisation des règles d'analyse programmées
- Création de requêtes KQL personnalisées
- Gestion des incidents et alertes

Automatisation de la réponse aux incidents

- Création de playbooks avec Logic Apps
- Déclencheurs et actions automatisées
- Cas pratiques de réponses automatisées

Bonnes pratiques et supervision continue

- Surveillance proactive et tableaux de bord
- Optimisation de la détection et réduction des faux positifs
- Intégration avec d'autres outils de sécurité