[TECH12]

- **Objectifs**
  - **Atténuer les menaces avec Microsoft Defender XDR, Microsoft Purview, Microsoft Copilot, Microsoft Defender pour point de terminaison et pour le cloud**
  - **Créer des requêtes pour Microsoft Sentinel avec le langage de requête Kusto** (KQL)
  - **Configurer un environnement Microsoft Sentinel et connecter les journaux**
  - **Créer investigations avec des détections et effectuer des Microsoft Sentinel**
  - **Effectuer la chasse aux menaces dans Microsoft Sentinel**

- **Public visé :** Analyste des opérations de sécurité
- **Prérequis**
  - Connaissances de base en sécurité informatique, notamment en détection des menaces et en réponse aux incidents
  - Expérience pratique des environnements Microsoft et des services de sécurité cloud

- **Accessibilité aux personnes en situation de handicap**
  - Si l'un des participants est en situation de handicap et souhaite nous en faire part, n'hésitez pas à prendre contact avec notre Référente Handicap clients par mail à l'adresse trainingcenter.ocd@orange.com

Cyberdefense

Microsoft Certified :
Security Operations Analyst Associate

Programme de formation

- **Introduction à Microsoft Sentinel pour la détection des menaces**
  - Configuration de Microsoft Sentinel et création de workspaces dédiés
  - Intégration des connecteurs de données
  - Création de requêtes KQL (Kusto Query Language)
  - Construction de playbooks automatisés

Lab : Configuration de Sentinel, connexion de sources de données et détection de menaces avec KQL

- **Gestion des incidents et investigation avec Microsoft 365 Defender**
  - Introduction aux fonctionnalités de Microsoft 365 Defender
  - Gestion des alertes de sécurité et investigation des incidents dans le centre de sécurité
  - Analyse des menaces et corrélation des signaux
  - Implémentation des stratégies de réponse et des automatisations

Lab : Investigation d'incidents, configuration d'alertes et automatisation des réponses avec Microsoft 365 Defender

- **Protection avancée avec Azure Defender**
  - Présentation d'Azure Defender et de ses fonctionnalités de protection pour les environnements cloud et hybrides
  - Configuration des alertes de sécurité et détection des vulnérabilités sur les ressources Azure
  - Détection des menaces sur les réseaux, bases de données et conteneurs avec Azure Defender

Lab : Protection d'un environnement hybride avec Azure Defender et gestion des alertes de sécurité

- **Optimisation et automatisation de la réponse aux incidents**
  - Introduction aux workflows d'automatisation Création de playbooks avancés avec Logic Apps
  - Optimisation des stratégies de sécurité et gestion centralisée des incidents avec Microsoft Sentinel
  - Exploitation des données de surveillance

Lab : Création de playbooks automatisés et optimisation de la gestion des incidents

[TECH12] Microsoft Certified :
Security Operations Analyst Associate

Sécurité applicative

Méthodes pédagogiques

- Alternance de théorie et de pratique, études de cas
- Retour d'expérience, échange de bonnes pratiques et écueils à éviter au quotidien
- Rédaction d'un plan d'action individuel
- Remise d'un support pédagogique favorisant la transférabilité des acquis

Méthodes d'évaluation de l'atteinte des objectifs

- Évaluation continue lors des exercices et des mises en situation pratique
- Exercices de mise en pratique des acquis de la formation, en lien avec les attendus de la certificat Microsoft SC-200.

Durée	4 jours (28 heures)
Groupe de formation	De 3 à 10 participants
Langue	Français / Anglais

Mode de déploiement	Présentiel	Distanciel	E-learning
Modalités	Intra	Inter	Sur-mesure
Tarif	Sur devis	Non concerné	Sur devis

Demande de devis – Modalités et délais d'accès

- **Pour toute demande intra**, contacter le Training Center à l'adresse **trainingcenter.ocd@orange.com** ou **au 06 87 05 79 34.** Le délai moyen de mise en œuvre est d'**environ 2 mois** (hors demande urgente).