ADVANCIA TRAINING

Analyse des opérations de sécurité Microsoft

Réf. SC-200 · Microsoft · Cybersécurité · **Formation certifiante**

DURÉE	NIVEAU	MODALITÉS	VOUCHER EXAMEN
4 jours	**Intermédiaire**	**Présentiel · Live · Intra**	**Inclus**

Présentation

Formation dédiée aux analystes des opérations de sécurité qui exploitent l'écosystème Microsoft de détection et de réponse. Elle couvre Microsoft Sentinel, Defender XDR et Defender for Cloud, ainsi que la chasse aux menaces avec le langage KQL. Elle prépare à l'examen SC-200 et rend opérationnel dès la fin du cursus sur un SOC réel.

Objectifs pédagogiques

- Configurer et exploiter Microsoft Defender XDR pour la détection et la remédiation des menaces
- Déployer et administrer Microsoft Sentinel (connecteurs, règles analytiques, classeurs)
- Investiguer et répondre aux incidents à l'échelle des identités, endpoints, e-mails et applications
- Écrire des requêtes de détection et de chasse aux menaces en KQL (Kusto Query Language)
- Sécuriser les charges cloud avec Microsoft Defender for Cloud
- Automatiser la réponse aux incidents avec les playbooks SOAR et Logic Apps

Programme détaillé

1. Module 1 — Atténuer les menaces avec Microsoft Defender XDR

- Defender for Endpoint, Identity, Office 365 et Cloud Apps
- Investigation et remédiation des incidents dans le portail Defender
- Gestion des alertes et des incidents multi-domaines
- Gestion des vulnérabilités et réduction de la surface d'attaque

2. Module 2 — Atténuer les menaces avec Microsoft Defender for Cloud

- Posture de sécurité des ressources Azure, hybrides et multicloud
- Plans de protection des charges de travail (serveurs, conteneurs, bases de données)
- Alertes de sécurité et recommandations
- Intégration avec Microsoft Sentinel

3. Module 3 — Chasse aux menaces avec KQL

- Fondamentaux du langage Kusto (KQL)
- Construction de requêtes de détection et d'analyse
- Techniques de threat hunting proactif
- Optimisation et réutilisation des requêtes

4. Module 4 — Opérations avec Microsoft Sentinel

- Architecture, espaces de travail et connecteurs de données
- Règles analytiques, incidents et entités
- Classeurs (workbooks), notebooks et threat intelligence
- Automatisation SOAR : playbooks et règles d'automatisation

Prérequis

Connaissances fondamentales des services Microsoft 365 et Azure, notions de sécurité, de conformité et d'identité (niveau SC-900 recommandé), ainsi qu'une familiarité avec les systèmes Windows et Linux.

Public visé

Analystes SOC, analystes des opérations de sécurité, ingénieurs sécurité, administrateurs sécurité et intervenants en réponse aux incidents.

Ce qui est inclus

- Support de cours officiel Microsoft (MOC SC-200)
- Labs pratiques sur Microsoft Sentinel et Defender XDR
- Attestation de réussite Advancia Training
- Voucher d'examen SC-200 et passage sur notre centre Pearson VUE
- Pauses café et déjeuner inclus + accompagnement d'un formateur expert du SOC

Certification

Prépare à l'examen Microsoft SC-200 : Microsoft Security Operations Analyst (niveau associé). Épreuve d'environ 40 à 60 questions (QCM et mises en situation), durée approximative de 120 minutes. Advancia Training est centre d'examen agréé Pearson VUE : passage de l'examen possible dans nos locaux.

1 500 DT HT / participant — tarif inter-entreprise · financement CNFCPP possible