

SC-200T00A – Security Operations Analyst

This course is designed for students who are planning to take the corresponding certification exam, or students who are performing security operations analyst tasks in their daily job.

Both the certification exam and the courseware are based on the security operations analyst role.

The Microsoft security operations analyst collaborates with organizational stakeholders to secure information technology systems for the organization. Their goal is to reduce organizational risk by rapidly remediating active attacks in the environment, advising on improvements to threat protection practices, and referring violations of organizational policies to appropriate stakeholders.

Responsibilities include threat management, monitoring, and response by using a variety of security solutions across their environment.

The role primarily investigates, responds to, and hunts for threats using Microsoft Sentinel, Microsoft Defender for Cloud, Microsoft 365 Defender, and third-party security products. Since the security operations analyst consumes the operational output of these tools, they are also a critical stakeholder in the configuration and deployment of these technologies.

Détails

- Code : SC-200T00A
- Durée : 4 jours (28 heures)

Public

- Analystes système
- Application Developers
- Consultants
- Consultants en Sécurité
- Database Administrators
- Développeurs
- Directeurs des Systèmes d'information
- Experts Techniques
- Ingénieurs Sécurité
- IT Professionals

Pré-requis

- Understanding of Microsoft 365, of Microsoft security, of Microsoft Windows, Familiarity with Azure services, Azure SQL Database and Azure Storage, with Azure virtual machines and virtual networking.

Objectifs

- Mitigate threats using Microsoft 365 Defender
- Mitigate threats using Microsoft Defender for Endpoint
- Mitigate threats using Microsoft Defender for Cloud
- Create queries for Microsoft Sentinel using Kusto Query Language (KQL)
- Configure your Microsoft Sentinel environment

Programme

1. Mitigate threats using Microsoft 365 Defender

- Introduction to Microsoft 365 threat protection
- Mitigate incidents using Microsoft 365 Defender
- Protect your identities with Azure AD Identity Protection
- Remediate risks with Microsoft Defender for Office 365
- Safeguard your environment with Microsoft Defender for Identity
- Secure your cloud apps and services with Microsoft Defender for Cloud Apps
- Respond to data loss prevention alerts using Microsoft 365
- Manage insider risk in Microsoft Purview

2. Mitigate threats using Microsoft Defender for Endpoint

- Protect against threats with Microsoft Defender for Endpoint
- Deploy the Microsoft Defender for Endpoint environment

- Implement Windows security enhancements with Microsoft Defender for Endpoint
- Perform device investigations in Microsoft Defender for Endpoint
- Perform actions on a device using Microsoft Defender for Endpoint
- Perform evidence and entities investigations using Microsoft Defender for Endpoint
- Configure and manage automation using Microsoft Defender for Endpoint
- Configure for alerts and detections in Microsoft Defender for Endpoint
- Utilize Vulnerability Management in Microsoft Defender for Endpoint

3. Mitigate threats using Microsoft Defender for Cloud

- Plan for cloud workload protections using Microsoft

Defender for Cloud

- Connect Azure assets to Microsoft Defender for Cloud
- Connect non-Azure resources to Microsoft Defender for Cloud
- Manage your cloud security posture management
- Explain cloud workload protections in Microsoft Defender for Cloud
- Remediate security alerts using Microsoft Defender for Cloud

4. Create queries for Microsoft Sentinel using Kusto Query Language (KQL)

- Construct KQL statements for Microsoft Sentinel
- Analyze query results using KQL
- Build multi-table statements using KQL
- Work with data in Microsoft Sentinel using Kusto Query Language

5. SC-200: Configure your Microsoft Sentinel environment

- Introduction to Microsoft Sentinel
- Create and manage Microsoft Sentinel workspaces
- Query logs in Microsoft Sentinel
- Use watchlists in Microsoft Sentinel
- Utilize threat intelligence in Microsoft Sentinel

6. Connect logs to Microsoft Sentinel

- Connect data to Microsoft Sentinel using data connectors
- Connect Microsoft services to Microsoft Sentinel
- Connect Microsoft 365 Defender to Microsoft Sentinel
- Connect Windows hosts to Microsoft Sentinel
- Connect Common Event Format logs to Microsoft Sentinel
- Connect syslog data sources to Microsoft Sentinel
- Connect threat indicators to Microsoft Sentinel

7. Create detections and perform investigations using Microsoft Sentinel

- Threat detection with Microsoft Sentinel analytics
- Automation in Microsoft Sentinel
- Threat response with Microsoft Sentinel playbooks
- Security incident management in Microsoft Sentinel
- Identify threats with Entity behavioral analytics in Microsoft Sentinel
- Data normalization in Microsoft Sentinel
- Query, visualize, and monitor data in Microsoft Sentinel
- Manage content in Microsoft Sentinel

8. Perform threat hunting in Microsoft Sentinel

- Explain threat hunting concepts in Microsoft Sentinel
- Threat hunting with Microsoft Sentinel
- Use Search jobs in Microsoft Sentinel
- Threat hunting with Microsoft Sentinel
- Optional – Play Who Hacked? Cloud Game

Modalités

- **Type d'action** :Acquisition des connaissances
- **Moyens de la formation** :Formation présentielle – 1 poste par stagiaire – 1 vidéo projecteur – Support de cours fourni à chaque stagiaire
- **Modalités pédagogiques** :Exposés – Cas pratiques – Synthèse
- **Validation** :Exercices de validation – Attestation de stages