INFOSECTRAIN

SC-200

Microsoft Security Operations Analyst

CERTIFICATION TRAINING

Microsoft Partner

KEY FEATURES

- Access to the recorded sessions
- Flexible training schedule
- Certified & Experienced Instructors
- Training support

www.infosectrain.com | sales@infosectrain.com

Overview

The Microsoft Security Operations Analyst's task is to provide secure information technology systems to an organization. They have to work with organizational stakeholders to achieve this goal. Their goal is to identify violations of organizational policies and report them, reduce risk by quickly identifying active attacks in the environment and remediating it. They can advise on how to improve threat protection practices.

The SC-200 is an associate-level certification that focuses on operations security. The Microsoft Certified Security Operations Analyst Associate is the designation you will obtain once you've completed this certification. Microsoft Security Operations Analysts collaborate with business partners to safeguard the company's IT infrastructure.

The Microsoft Security Operations Analyst has many other responsibilities that includes threat management, monitoring, and response by using a variety of security solutions. They can perform threat hunting using Microsoft 365 Defender, Azure Security Centre, Azure Defender, Azure Sentinel, and 3rd- party security products.

Target Audience

- IT Professionals
- IT Security Professionals
- Cloud Administrators
- Cloud Architects
- Network Administrators
- Microsoft Security Administrators
- Azure Security Engineers
- Server Administrators
- Cyber Security Analysts

Pre-Requisite

- Good understanding of Windows 10
- Basic knowledge of Microsoft 365
- Fundamental understanding of Microsoft security, compliance, and identity products
- Fundamentals of Azure Cloud
- Basic Knowledge of Azure virtual machines and virtual networking
- Familiarity with Azure SQL Database and Azure Storage
- Basic understanding of scripting concepts

Why Infosec Train?

Certified & Experienced Instructor

Flexible Schedule

Access to the recorded sessions

Post Training Support

Tailor Made Training

4 hrs/day in Weekend/ Weekday

INFOSECTRAIN

Exam Information

Exam Name	Exam SC-200: Microsoft Security Operations Analyst
Number of questions	50-60
Exam Duration	120 Minutes
Languages	English, Japanese, Chinese (Simplified), Korean
Exam Fee	$165 USD

Domain 1: Mitigate threats using Microsoft 365 Defender

- Detect, investigate, respond, and remediate threats to the productivity environment by using Microsoft Defender for Office 365
- Detect, investigate, respond, and remediate endpoint threats by using Microsoft Defender for Endpoint
- Detect, investigate, respond, and remediate identity threats
- Manage cross-domain investigations in Microsoft 365 Defender Portal

Domain 2: Mitigate threats using Azure Defender

- Design and configure an Azure Defender implementation
- Plan and implement the use of data connectors for ingestion of data sources in Azure Defender
- Manage Azure Defender alert rules
- Configure automation and remediation
- Investigate Azure Defender alerts and incidents

Domain 3: Mitigate threats using Azure Sentinel

- Design and configure an Azure Sentinel workspace
- Plan and Implement the use of Data Connectors for Ingestion of Data Sources in Azure Sentinel
- Manage Azure Sentinel analytics rules
- Configure Security Orchestration Automation and Remediation (SOAR) in Azure Sentinel
- Manage Azure Sentinel Incidents
- Use Azure Sentinel workbooks to analyse and interpret data
- Hunt for threats using the Azure Sentinel portal

www.infosectrain.com | sales@infosectrain.com