REAL WORLD
TECHNOLOGY TRAINING & SOLUTIONS
"Training You Can Really Use"

SC-200T00: Microsoft Security Operations Analyst

Duration: 4 Days

Method: Instructor-Led Training (ILT) | Live Online Training

Certification: *Microsoft Certified: Security Operations Analyst Associate —* ***Exam:*** *SC-200 Microsoft Security Operations Analyst*

Course Description

In this course, participants will learn how to investigate, respond to, and hunt for threats using Microsoft Azure Sentinel, Azure Defender, and Microsoft 365 Defender. They will learn how to mitigate cyber threats using these technologies. Specifically, participants will configure and use Azure Sentinel as well as utilize Kusto Query Language (KQL) to perform detection, analysis, and reporting.

Target Audience

This course is intended for:

- Security Engineers
- Security Operations Analysts
- Professionals who wish to prepare for the certification exam.

Prerequisites

To attend this course, candidates must have:

- Basic understanding of Microsoft 365.
- Fundamental understanding of Microsoft security, compliance, and identity products.
- Intermediate understanding of Windows 10.
- Familiarity with Azure services, specifically Azure SQL Database and Azure Storage.
- Familiarity with Azure virtual machines and virtual networking.
- Basic understanding of scripting concepts.

REAL WORLD
TECHNOLOGY TRAINING & SOLUTIONS
"Training You Can Really Use"

Course Objectives

Upon successful completion of this course, attendees will be able to:

- Explain how Microsoft Defender for Endpoint can remediate risks in your environment.
- Create a Microsoft Defender for the Endpoint environment.
- Configure Attack Surface Reduction rules on Windows 10 devices.
- Perform actions on a device using Microsoft Defender for Endpoint.
- Investigate domains and IP addresses in Microsoft Defender for Endpoint.
- Investigate user accounts in Microsoft Defender for Endpoint.
- Configure alert settings in Microsoft Defender for Endpoint.
- Explain how the threat landscape is evolving.
- Conduct advanced hunting in Microsoft 365 Defender.
- Manage incidents in Microsoft 365 Defender.
- Explain how Microsoft Defender for Identity can remediate risks in your environment.
- Investigate DLP alerts in Microsoft Cloud App Security.
- Explain the types of actions you can take on an insider risk management case.
- Configure auto-provisioning in Azure Defender.
- Remediate alerts in Azure Defender.
- Construct KQL statements.
- Filter searches based on event time, severity, domain, and other relevant data using KQL.
- Extract data from unstructured string fields using KQL.
- Manage an Azure Sentinel workspace.
- Use KQL to access the watchlist in Azure Sentinel.
- Manage threat indicators in Azure Sentinel.
- Explain the Common Event Format and Syslog connector differences in Azure Sentinel.
- Connect Azure Windows Virtual Machines to Azure Sentinel.
- Configure Log Analytics agent to collect Sysmon events.
- Create new analytics rules and queries using the analytics rule wizard.
- Create a playbook to automate incident response.
- Use queries to hunt for threats.
- Observe threats over time with Livestream.

REAL WORLD
TECHNOLOGY TRAINING & SOLUTIONS
"Training You Can Really Use"

Course Topics

Module 1: Mitigate Threats Using Microsoft Defender for Endpoint

- Protect Against Threats with Microsoft Defender for Endpoint
- Deploy the Microsoft Defender for Endpoint Environment
- Implement Windows 10 Security Enhancements with Microsoft Defender for Endpoint
- Manage Alerts and Incidents in 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 Threat and Vulnerability Management in Microsoft Defender for Endpoint

Module 2: Mitigate Threats Using Microsoft 365 Defender

- Introduction to Threat Protection with Microsoft 365
- 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 Cloud App Security
- Respond to Data Loss Prevention Alerts Using Microsoft 365
- Manage Insider Risk in Microsoft 365

Module 3: Mitigate Threats Using Azure Defender

- Plan for Cloud Workload Protections Using Azure Defender
- Explain Cloud Workload Protections in Azure Defender
- Connect Azure Assets to Azure Defender
- Connect Non-Azure Resources to Azure Defender
- Remediate Security Alerts Using Azure Defender

Module 4: Create Queries for Azure Sentinel Using Kusto Query Language (KQL)

- Construct KQL Statements for Azure Sentinel
- Analyse Query Results Using KQL
- Build Multi-Table Statements Using KQL
- Work with Data in Azure Sentinel Using Kusto Query Language

Course Topics *Continued*

Module 5: Configure Your Azure Sentinel Environment

- Introduction to Azure Sentinel
- Create and Manage Azure Sentinel Workspaces
- Query Logs in Azure Sentinel
- Use Watchlists in Azure Sentinel
- Utilize Threat Intelligence in Azure Sentinel

Module 6: Connect Logs to Azure Sentinel

- Connect Data to Azure Sentinel Using Data Connectors
- Connect Microsoft services to Azure Sentinel
- Connect Microsoft 365 Defender to Azure Sentinel
- Connect Windows Hosts to Azure Sentinel
- Connect Common Event Format Logs to Azure Sentinel
- Connect Syslog Data Sources to Azure Sentinel
- Connect Threat Indicators to Azure Sentinel

Module 7: Create Detections and Perform Investigations Using Azure Sentinel

- Threat Detection with Azure Sentinel Analytics
- Threat Response with Azure Sentinel Playbooks
- Security Incident Management in Azure Sentinel
- Use entity Behaviour Analytics in Azure Sentinel
- Query, Visualize, and Monitor Data in Azure Sentinel

Module 8: Perform Threat Hunting in Azure Sentinel

- Threat Hunting with Azure Sentinel
- Hunt for Threats Using Notebooks in Azure Sentinel

LABS INCLUDED