SC-5001: Configure SIEM security operations using Microsoft Sentinel

Course ID #: 7000-897-ZZ-Z
Hours: 7

Course Content

Course Description:

Get started with Microsoft Sentinel security operations by configuring the Microsoft Sentinel workspace, connecting Microsoft services and Windows security events to Microsoft Sentinel, configuring Microsoft Sentinel analytics rules, and responding to threats with automated responses.

Prerequisites:

Fundamental understanding of Microsoft Azure
Basic understanding of Microsoft Sentinel
Experience using Kusto Query Language (KQL) in Microsoft Sentinel

Target Audience:

Security Operations Specialists

Topics:

Lesson:
Create and manage Microsoft Sentinel workspaces

- Introduction
- Plan for the Microsoft Sentinel workspace
- Create a Microsoft Sentinel workspace
- Manage workspaces across tenants using Azure Lighthouse
- Understand Microsoft Sentinel permissions and roles
- Manage Microsoft Sentinel settings
- Configure logs
- Knowledge check
- Summary and resources

Connect Microsoft services to Microsoft Sentinel

- Introduction
- 3 min
- Plan for Microsoft services connectors
- 4 min
- Connect the Microsoft Office 365 connector
- 4 min
- Connect the Microsoft Entra connector
- 3 min
- Connect the Microsoft Entra ID Protection connector
- 3 min
- Connect the Azure Activity connector
- 3 min
- Knowledge check
- 3 min
- Summary and resources

SC-5001: Configure SIEM security operations using Microsoft Sentinel

Course ID #: 7000-897-ZZ-Z
Hours: 7

Connect Windows hosts to Microsoft Sentinel

- Introduction
- Plan for Windows hosts security events connector
- Connect using the Windows Security Events via AMA Connector
- Connect using the Security Events via Legacy Agent Connector
- Collect Sysmon event logs
- Knowledge check
- Summary and resources

Threat detection with Microsoft Sentinel analytics

- Introduction
- Exercise - Detect threats with Microsoft Sentinel analytics
- What is Microsoft Sentinel Analytics?
- Types of analytics rules
- Create an analytics rule from templates
- Create an analytics rule from wizard
- Manage analytics rules
- Exercise - Detect threats with Microsoft Sentinel analytics
- Summary

Automation in Microsoft Sentinel

- Introduction
- Understand automation options
- Create automation rules
- Knowledge check
- Summary and resources

Configure SIEM security operations using Microsoft Sentinel

- Introduction
- Exercise - Configure SIEM operations using Microsoft Sentinel
- Exercise - Install Microsoft Sentinel Content Hub solutions and data connectors
- Exercise - Configure a data connector Data Collection Rule
- Exercise - Perform a simulated attack to validate the Analytic and Automation rules
- Summary

SC-5001: Configure SIEM security operations using Microsoft Sentinel

Course ID #: 7000-897-ZZ-Z
Hours: 7

NASBA Information

Level: Intermediate
Attendance Requirement: To be awarded the full credit hours, you must sign in and attend the entire course.
Fields: Computer Software & Applications
CPEs: 14

Policies: Course Registration, Cancellation, Refund and Complaint Resolution
For more information regarding administrative policies such as complaint and refund, please contact our offices at 800-639-3535 or visit us at: **www.tcworkshop.com**

Official National Registry Statement:
The Computer Workshop is registered with the National Association of State Boards of Accountancy (NASBA) as a sponsor of continuing professional education on the National Registry of CPE Sponsors. State boards of accountancy have final authority on the acceptance of individual courses for CPE credits. Complaints regarding registered sponsors may be submitted to the National Registry of CPE Sponsors through its website: www.nasbaregistry.org

NOTE: Since our information is in multiple places on our web site or in PDF format that is sent to clients, we have provided our normal course content with the NASBA Information added along with links to our policy page on the web. We will add our name to the Official National Registry Statement after we are approved.