SC-5001: Configure SIEM security operations using Microsoft Sentinel

Duration: 8 Hours (1 Day)

Overview

The SC-5001 certification pertains to configuring SIEM (Security Information and Event Management) operations using Microsoft Sentinel. This certification represents expertise in using Microsoft's cloud-native SIEM solution to collect, detect, investigate, and respond to security threats across an organization's IT environment. It is valuable for security operations professionals who need to implement and manage Sentinel to safeguard enterprise systems. By obtaining this certification, individuals demonstrate their skills in leveraging Sentinel for Real-time analysis, maintaining security data, Creating alerts, and orchestrating threat responses. Industries use it to ensure their security teams are proficient in using advanced tools to protect their infrastructure from cyber threats.

Audience Profile

IT professionals managing security operations - Security analysts and engineers

- Security architects
- System administrators focused on security
- Technical personnel implementing Microsoft Sentinel
- Professionals seeking to understand SIEM with Microsoft Sentinel

Course Syllabus

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

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