Configure SIEM security operations using Microsoft Sentinel (SC-5001)

Description

Master the Configuration of Microsoft Sentinel to Secure Your Systems

Cybersecurity is a major concern for all businesses. With the rise in cyberattacks, having an efficient system to monitor, detect, and respond to threats is essential. The SC-5001 training, “Configuring SIEM Security Operations with Microsoft Sentinel,” equips you with the skills needed to implement advanced monitoring using Microsoft Sentinel.

Through this cybersecurity training, you will learn how to configure your workspace in Azure, connect various Microsoft services, and leverage Azure Log Analytics to analyze event logs. You will also discover how to enhance threat detection with analytical rules and automate certain tasks using Azure Logic Apps. The goal is clear: strengthen your security posture and effectively protect your IT infrastructure.

Course Content
Module 1: Create and manage Microsoft Sentinel workspaces

- 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

Module 2: Connect Microsoft services to Microsoft Sentinel

- Plan for Microsoft services connectors
- Connect the Microsoft 365 connector
- Connect the Microsoft Entra connector
- Connect the Microsoft Entra ID Protection connector
- Connect the Azure Activity connector

Module 3: Connect Windows hosts to Microsoft Sentinel

- 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

Module 4: Threat detection 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

Module 5: Automation in Microsoft Sentinel

- Understand automation options
- Create automation rules

Module 6: Configure SIEM security operations using Microsoft Sentinel

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

Lab / Exercises

- This course provides you with exclusive access to the official Microsoft lab, enabling you to practice your skills in a professional environment.

Documentation

- Access to Microsoft Learn, Microsoft's online learning platform, offering interactive resources and educational content to deepen your knowledge and develop your technical skills.

Participant profiles

- Cybersecurity analysts
- System and network administrators
- IT security engineers
- Information security consultants
- Chief Information Security Officers (CISOs)

Prerequisites

- Understand the basics of Microsoft Azure
- Have a basic knowledge of Microsoft Sentinel
- Master the Kusto Query Language (KQL) in Microsoft Sentinel

Objectives

- Configure and manage a Microsoft Sentinel workspace
- Connect Microsoft services and integrate event logs
- Utilize Azure Log Analytics to monitor and analyze data
- Implement analytical rules to detect threats
- Automate incident management with Azure Logic Apps
- Optimize the protection and monitoring of IT infrastructures

Description
Configure SIEM security operations using Microsoft Sentinel (SC-5001)
Niveau
Intermédiaire
Classroom Registration Price (CHF)
900
Virtual Classroom Registration Price (CHF)
850
Duration (in Days)

1

Reference

SC-5001