Learn

Configure SIEM security operations using Microsoft Sentinel

Course SC-5001: 1 day; Instructor-Led; Level: Intermediate

Introduction

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.

Note: You need to have your own Azure subscription.
You need an Azure subscription to complete the exercises. If you don't have an Azure subscription, create a free account and add a subscription before you begin. If you're a student, you can take advantage of the Azure for students offer.

Prerequisites

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

Course Outline

Module 1: Create and manage Microsoft Sentinel workspaces
Learn about the architecture of Microsoft Sentinel workspaces to ensure you configure your system to meet your organization's security operations requirements.
Upon completion of this module, the learner will be able to:

- Describe Microsoft Sentinel workspace architecture
- Install Microsoft Sentinel workspace
- Manage a Microsoft Sentinel workspace

Prerequisites

- Basic experience with Azure services

Lessons

- 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
Learn how to connect Microsoft 365 and Azure service logs to Microsoft Sentinel.

Upon completion of this module, the learner will be able to:

- Connect Microsoft service connectors
- Explain how connectors auto-create incidents in Microsoft Sentinel

Prerequisites
Basic experience with Azure services

Lessons

- 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

Module 3: Connect Windows hosts to Microsoft Sentinel
In this module, you'll learn about forms, grids, views, charts, and dashboards that can be used in model-driven apps. One of the most common logs to collect is Windows security events. Learn how Microsoft Sentinel makes this easy with the Security Events connector.

Upon completion of this module, the learner will be able to:
- Connect Azure Windows Virtual Machines to Microsoft Sentinel
- Connect non-Azure Windows hosts to Microsoft Sentinel
- Configure Log Analytics agent to collect Sysmon events

Prerequisites
Basic knowledge of operational concepts such as monitoring, logging, and alerting.

Lessons
- 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
In this module, you learned how Microsoft Sentinel Analytics can help the SecOps team identify and stop cyber attacks.

In this module, you will:
- Explain the importance of Microsoft Sentinel Analytics.
- Explain different types of analytics rules.
- Create rules from templates.
- Create new analytics rules and queries using the analytics rule wizard.
- Manage rules with modifications.

Prerequisites
- Basic knowledge of Azure services
- Basic knowledge of operational concepts, such as monitoring, logging, and alerting
- Azure subscription
- Microsoft Sentinel instance in your Azure subscription

Lessons
- 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

Module 5: Automation in Microsoft Sentinel
By the end of this module, you'll be able to use automation rules in Microsoft Sentinel to automated incident management.

After completing this module, you'll be able to:
- Explain automation options in Microsoft Sentinel
- Create automation rules in Microsoft Sentinel

Prerequisites
- None

Lessons

- Understand automation options
- Create automation rules

Module 6: Configure SIEM security operations using Microsoft Sentinel

In this module, you learned how to configure SIEM security operations using Microsoft Sentinel.

Upon completion of this module, the learner is able to:

- Create and configure a Microsoft Sentinel workspace
- Deploy Microsoft Sentinel Content Hub solutions and data connectors
- Configure Microsoft Sentinel Data Collection rules, NRT Analytic rule and Automation
- Perform a simulated attack to validate Analytic and Automation rules

Prerequisites

- Basic experience with Azure services
- Basic knowledge of operational concepts, such as monitoring, logging, and alerting
- An Azure subscription

Lessons

- 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

