

SC-5001: Configure SIEM security operations using Microsoft Sentinel

Course Details

Course Code: SC-5001

Duration: 1 day

Notes:

- This course syllabus should be used to determine whether the course is appropriate for the students, based on their current skills and technical training needs.
- Course content, prices, and availability are subject to change without notice.
- Terms and Conditions apply

Elements of this syllabus are subject to change.

About this course

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

Academy IT Pty Ltd

Level 4, 45 Grenfell Street
ADELAIDE 5000

Email: sales@academyit.com.au

Web: www.academyit.com.au

Phone: 08 7324 9800

Brian: 0400 112 083

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.

Learning objectives

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

Connect Microsoft services to Microsoft Sentinel

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

Learning objectives

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

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

Connect Windows hosts to Microsoft Sentinel

One of the most common logs to collect is Windows security events. Learn how Microsoft Sentinel makes this easy with the Security Events connector.

Learning objectives

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

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.

Learning objectives

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.

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.

Learning objectives

After completing this module, you'll be able to:

- Explain automation options in Microsoft Sentinel
- Create automation rules in Microsoft Sentinel

Configure SIEM security operations using Microsoft Sentinel

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

Learning objectives

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