

MS-SC5001: CONFIGURE SIEM SECURITY OPERATIONS USING MICROSOFT SENTINEL



DURATION	LEVEL	TECHNOLOGY	DELIVERY METHOD	TRAINING CREDITS
1 Day	Intermediate	Security	Instructor-led	NA

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.

AUDIENCE PROFILE

This course is designed for professionals who are actively involved in managing and securing cloud environments. Here's a breakdown of the ideal audience:

- Security Analysts and SOC Operators responsible for threat detection and incident response
- Cloud Security Engineers managing Microsoft Sentinel environments
- IT Security Professionals transitioning to or deploying cloud-native SIEM solutions
- Individuals preparing for the SC-200: Microsoft Security Operations Analyst certification

PREREQUISITES

Before attending this course, delegates must know:

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

COURSE OBJECTIVES

After completion of this course, the key objectives are:

- Create and manage Microsoft Sentinel workspaces
- Learn to architect and configure Sentinel environments tailored to organizational needs.
- Connect Microsoft services to Microsoft Sentinel
- Integrate Microsoft 365 and Azure service logs for centralized monitoring.
- Connect Windows hosts to Microsoft Sentinel
- Use connectors to ingest Windows security events from both Azure and non-Azure machines.
- Threat detection with Microsoft Sentinel analytics
- Develop and manage analytics rules to identify and respond to cyber threats.
- Automation in Microsoft Sentinel
- Implement automation rules to streamline incident response and reduce manual effort.
- Configure SIEM security operations using Microsoft Sentinel
- Apply all learned skills to build a cohesive, responsive SIEM strategy

COURSE CONTENT

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.

Lessons

- 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.
- By the end of this module, you'll be able to:
- Describe Microsoft Sentinel workspace architecture.
 - Install Microsoft Sentinel workspace.
 - Manage a Microsoft Sentinel workspace.

Module 2: Connect Microsoft services to Microsoft Sentinel

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

Lessons

- 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.
- By the end of this module, you'll be able to:
- Connect Microsoft service connectors.

- Explain how connectors auto-create incidents in Microsoft Sentinel.

Module 3: 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.

Lessons

- 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.

By the end of this module, you'll 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.

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.

Lessons

- 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.
- Knowledge check.

By the end of this module, you'll be able to:

- 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.

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.

Lessons

- Introduction.
- Understand automation options.
- Create automation rules.
- Knowledge check.

By the end of this module, you'll be able to:

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

Module 6: Configure SIEM security operations using Microsoft Sentinel

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

Lessons

- 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.
- Knowledge check.

By the end of this module, you'll be 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.

ASSOCIATED CERTIFICATIONS & EXAM

There is no Associated Certification or Exam for this course.