APPLIED SKILLS

Configure SIEM security operations using Microsoft Sentinel

Days	SKILL LEVEL	DELIVERY METHOD	Role	TECHNOLOGY
1	Intermediate	VILT/ILT	Security Engineer	Security

Course Overview

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.

Tasks performed.

- Create and configure a Microsoft Sentinel workspace
- Deploy a Microsoft Sentinel content hub solution
- Configure analytics rules in Microsoft Sentinel
- Configure automation in Microsoft Sentinel"

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.

Prepare for the assessment.

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.

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

Module 2: 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

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.

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

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.

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.

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.

Learning objectives

After completing 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.

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

Take the assessment.

This assessment will use an interactive lab to evaluate your performance. It will take a few minutes to load the lab, and you may do other activities while it loads. After you launch the lab, you will need to wait 72 hours to launch it again. Your mouse movements and text entered during the lab will be recorded for quality purposes. Learn more.

Follow on Course

Schedules | Netcampus Group