

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

**Course Number:** MOC-SC-5001
**Duration:** 1 day

**Overview**

This official Microsoft Applied Skill course SC-5001, Configure SIEM security operations using Microsoft Sentinel, teaches attendees how to configure the Microsoft Sentinel workspace, connect Microsoft services and Windows security events to Microsoft Sentinel, configure Microsoft Sentinel analytics rules, and respond to threats with automated responses.

**Prerequisites**

All attendees must have:

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

**Materials**

All Microsoft training students receive Microsoft official courseware.

For all Microsoft Official Courses taught in their entirety that have a corresponding certification exam, an exam voucher is included for each participant.

**Software Needed on Each Student PC**

Attendees will not need to install any software on their computers for this class. The class will be conducted in a remote environment that Accelebrate will provide; students will only need a local computer with a web browser and a stable Internet connection. Any recent version of Microsoft Edge, Mozilla Firefox, or Google Chrome will work well.

**Objectives**

* Configure your system to meet your organization's security operations requirements
* Connect Microsoft 365 and Azure service logs to Microsoft Sentinel
* Use the Security Events connector
* Understand how Microsoft Sentinel Analytics can help the SecOps team identify and stop cyber attacks
* Use automation rules in Microsoft Sentinel to automate incident management
* Configure SIEM security operations using Microsoft Sentinel

**Outline**

* Create and manage Microsoft Sentinel workspaces
* Connect Microsoft services to Microsoft Sentinel
* Connect Windows hosts to Microsoft Sentinel
* Threat detection with Microsoft Sentinel analytics
* Automation in Microsoft Sentinel
* Configure SIEM security operations using Microsoft Sentinel