

**Microsoft Security Operations Analyst (SC-200)**

**Course Number:** MOC-SC-200
**Duration:** 4 days

**Overview**

This live online or in-person Microsoft Security Operations Analyst training course (SC-200) teaches teams how to find and mitigate threats using Microsoft Azure Sentinel, Azure Defender, and Microsoft 365 Defender. Attendees learn how to use Kusto Query Language (KQL) to perform threat detection, analysis, and reporting. This course prepares students for the [SC-200 exam](https://docs.microsoft.com/en-us/learn/certifications/exams/SC-200) for which every attendee receives a voucher.

**Prerequisites**

All students must have:

* Basic understanding of Microsoft 365
* Fundamental understanding of Microsoft security, compliance, and identity products
* Intermediate understanding of Windows 10
* Familiarity with Azure services, specifically Azure SQL Database and Azure Storage
* Familiarity with Azure virtual machines and virtual networking
* Basic understanding of scripting

**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 computer 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 be fine.

**Objectives**

All students will learn how to:

* Investigate, respond to, and hunt for threats using Microsoft Sentinel, Microsoft Defender for Cloud, and Microsoft 365 Defender
* Utilize Kusto Query Language (KQL) to perform detection, analysis, and reporting
* Perform actions on a device using Microsoft Defender for Endpoint
* Conduct advanced hunting in Microsoft 365 Defender
* Configure auto-provisioning in Azure Defender
* Filter searches based on event time, severity, domain, and other relevant data using KQL
* Manage an Azure Sentinel workspace
* Manage threat indicators in Azure Sentinel
* Connect Azure Windows Virtual Machines to Azure Sentinel
* Use queries to hunt for threats
* Observe threats over time with livestream

**Outline**

* Introduction to Microsoft 365 threat protection
* Mitigate incidents using Microsoft 365 Defender
* Protect your identities with Azure AD Identity Protection
* Remediate risks with Microsoft Defender for Office 365
* Safeguard your environment with Microsoft Defender for Identity
* Secure your cloud apps and services with Microsoft Defender for Cloud Apps
* Respond to data loss prevention alerts using Microsoft 365
* Manage insider risk in Microsoft Purview
* Investigate threats by using audit features in Microsoft 365 Defender and Microsoft Purview Standard
* Investigate threats using audit in Microsoft 365 Defender and Microsoft Purview (Premium)
* Investigate threats with Content search in Microsoft Purview
* Protect against threats with Microsoft Defender for Endpoint
* Deploy the Microsoft Defender for Endpoint environment
* Implement Windows security enhancements with Microsoft Defender for Endpoint
* Perform device investigations in Microsoft Defender for Endpoint
* Perform actions on a device using Microsoft Defender for Endpoint
* Perform evidence and entities investigations using Microsoft Defender for Endpoint
* Configure and manage automation using Microsoft Defender for Endpoint
* Configure for alerts and detections in Microsoft Defender for Endpoint
* Utilize Vulnerability Management in Microsoft Defender for Endpoint
* Plan for cloud workload protections using Microsoft Defender for Cloud
* Connect Azure assets to Microsoft Defender for Cloud
* Connect non-Azure resources to Microsoft Defender for Cloud
* Manage your cloud security posture management​
* Explain cloud workload protections in Microsoft Defender for Cloud
* Remediate security alerts using Microsoft Defender for Cloud
* Construct KQL statements for Microsoft Sentinel
* Analyze query results using KQL
* Build multi-table statements using KQL
* Work with data in Microsoft Sentinel using Kusto Query Language
* Security Operations Analyst
* Microsoft Sentinel
* Introduction to Microsoft Sentinel
* Create and manage Microsoft Sentinel workspaces
* Query logs in Microsoft Sentinel
* Use watchlists in Microsoft Sentinel
* Conclusion