# SC-200T00: Microsoft Security Operations Analyst

**Course Duration: 32 Hours** **Course code: SC-200T00**

## 1. Course Overview

The **Microsoft Security Operations Analyst (SC-200T00)** course equips learners with the knowledge and skills required to investigate, respond, and hunt for threats using Microsoft security solutions. Participants will gain expertise in reducing organizational risk by rapidly remediating active attacks in the environment, advising on threat protection practices, and referring policy violations to appropriate stakeholders. The course emphasizes practical, hands-on experience with **Microsoft 365 Defender, Microsoft Sentinel, and Microsoft Defender for Cloud**.

## 2. What You'll Learn?

By the end of this course, you will be able to:

- Mitigate threats using **Microsoft 365 Defender**.
- Utilize **Microsoft Sentinel** for threat detection and response.
- Leverage **Microsoft Defender for Cloud** to protect cloud resources.
- Configure security solutions and automate incident response.
- Investigate, analyze, and respond to cyber threats in real-time.
- Perform advanced threat hunting using Kusto Query Language (KQL).

## 3. Target Audience

This course is designed for:

- **Security Operations Analysts (SOC Analysts)**.
- IT professionals responsible for monitoring and responding to threats.

- Cybersecurity professionals working with Microsoft security tools.
- Individuals preparing for the **Microsoft SC-200 certification exam**.

## 4. Pre-Requisites

Before attending this course, learners should have:

- Basic understanding of **Microsoft security, compliance, and identity concepts**.
- Familiarity with **Microsoft 365 services and Azure fundamentals**.
- Experience with **common cybersecurity practices and principles**.
- Completion of **SC-900: Microsoft Security, Compliance, and Identity Fundamentals** (recommended, but not mandatory).

## 5. Course Content

**Module 1: Mitigate threats using Microsoft 365 Defender**

- Introduction to Microsoft 365 Defender
- Threat investigation and response
- Remediation actions in Microsoft 365 environments

**Module 2: Mitigate threats using Microsoft Sentinel**

- Introduction to Microsoft Sentinel
- Connect data sources and configure workbooks
- Detect, investigate, and respond to threats
- Automating responses with playbooks

**Module 3: Mitigate threats using Microsoft Defender for Cloud**

- Introduction to Microsoft Defender for Cloud
- Protecting Azure workloads and hybrid environments

- Implementing security recommendations
- Managing compliance policies and regulatory requirements

**Module 4: Create queries for advanced hunting**

- Introduction to Kusto Query Language (KQL)
- Building queries for security event analysis
- Hunting for threats across Microsoft security solutions