SC-200T00 Microsoft Security Operations Analyst

Price: 2495

Duration: 4 days

Delivery Methods: Virtual

Overview

Learn how to investigate, respond to, and hunt for threats using Microsoft Azure Sentinel, Azure Defender, and Microsoft 365 Defender. In this course students will learn how to mitigate cyberthreats using these technologies. Specifically, students will configure and use Azure Sentinel as well as utilize Kusto Query Language (KQL) to perform detection, analysis, and reporting. The course was designed for people who work in a Security Operations job role and helps learners prepare for the exam SC-200: Microsoft Security Operations Analyst.

Audience Profile

The Microsoft Security Operations Analyst collaborates with organizational stakeholders to secure information technology systems for the organization. Their goal is to reduce organizational risk by rapidly remediating active attacks in the environment, advising on improvements to threat protection practices, and referring violations of organizational policies to appropriate stakeholders. Responsibilities include threat management, monitoring, and response by using a variety of security solutions across their environment. The role primarily investigates, responds to, and hunts for threats using Microsoft Azure Sentinel, Azure Defender, Microsoft 365 Defender, and third-party security products. Since the Security Operations Analyst consumes the operational output of these tools, they are also a critical stakeholder in the configuration and deployment of these technologies.

At Course Completion

After completing this course, students will be able to:

- Explain how Microsoft Defender for Endpoint can remediate risks in your environment.
- Create a Microsoft Defender for Endpoint environment.
- Configure Attack Surface Reduction rules on Windows 10 devices.
- Perform actions on a device using Microsoft Defender for Endpoint.
- Investigate domains and IP addresses in Microsoft Defender for Endpoint.
- Investigate user accounts in Microsoft Defender for Endpoint.
- Configure alert settings in Microsoft Defender for Endpoint.
- Explain how the threat landscape is evolving.
- Conduct advanced hunting in Microsoft 365 Defender.
- Manage incidents in Microsoft 365 Defender.
- Explain how Microsoft Defender for Identity can remediate risks in your environment.
- Investigate DLP alerts in Microsoft Cloud App Security.
- Explain the types of actions you can take on an insider risk management case.
- Configure auto-provisioning in Azure Defender.
- Remediate alerts in Azure Defender.
- Construct KQL statements.
- Filter searches based on event time, severity, domain, and other relevant data using KQL.
- Extract data from unstructured string fields using KQL.
- Manage an Azure Sentinel workspace.
- Use KQL to access the watchlist in Azure Sentinel.
- Manage threat indicators in Azure Sentinel.
- Explain the Common Event Format and Syslog connector differences in Azure Sentinel.
- Connect Azure Windows Virtual Machines to Azure Sentinel.
- Configure Log Analytics agent to collect Sysmon events.
- Create new analytics rules and queries using the analytics rule wizard.
- Create a playbook to automate an incident response.
- Use queries to hunt for threats.
- Observe threats over time with livestream.

Prerequisites

- 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 Concepts

Course Schedule

Date	Time	Price	Options
07/28/2026	**09:00 AM - 05:00 PM CT**	**2,495.00**	**Buy Now Enroll**

Why Professional Choose TOPTALENT?

Dedicated Texas-Based Support

Get assistance every step of the way from our **Texas-based team**, ensuring your training experience is hassle-free and aligned with your goals.

3000+ Curated Professional Courses

Access an extensive portfolio of over 3000 courses across IT, Business Application and Leadership – Designed to meet evolving Industry demands

95% Client Approval Rating

Trusted by professionals nationwide our 95% approval rating reflects consistent quality, measurable impact and exceptional service.

Certified Industry Instructor

Learn from professionaly certified experts with real world experience and a proven commitment to learner success.

For questions

call:

(469) 721-6100

Email:

info@toptalentlearning.com

Find More Training

FAQ

What if I have to reschedule my class due to conflict?

Ten (10) business days' notice is required to reschedule a class with no additional fees. Notify TOPTALENT LEARNING as soon as possible at 469-721-6100 or by written notification to info@toptalentlearning.com to avoid rescheduling penalties.

How do I enroll for this class?

Please contact our team at 469-721-6100; we will gladly guide you through the online purchasing process.

What happens once I purchase a class?

You will receive a receipt and an enrollment confirmation sent to the email you submitted at purchase. Your enrollment email will have instructions on how to access the class. Any additional questions our team is here to support you. Please call us at 469-721-6100.

What is your late policy?

If a student is 15 minutes late, they risk losing their seat to a standby student. If a student is 30 minutes late or more, they will need to reschedule. A no-show fee will apply. Retakes are enrolled on a stand-by basis. The student must supply previously issued courseware. Additional fees may apply.

What happens when I finish my class?

You will receive a ‘Certificate of Completion’ once you complete the class. If you purchased an exam voucher for the class, a team member from TOPTALENT LEARNING will reach out to discuss your readiness for the voucher and make arrangements to send it.