



GTech Learn

"Our focus is your Success"



Course Contents

SC-200: Microsoft Security Operations Analyst

Duration: 4 Days	Level: Intermediate	Role: Security Engineer
Certification: Available	Public Schedules: View Dates	Private Delivery: Reach Us

What's included?

- ✓ Learn from Microsoft Certified Trainer (MCT's)
- ✓ 24x7 Lab Access
- ✓ Official Courseware
- ✓ Exam Preps / Practice Tests
- ✓ Badges & Completion Certificate
- ✓ Discounted Exam Vouchers



Email: info@gtechlearn.com

Overview

Learn how to investigate, respond to, and hunt for threats using Microsoft Sentinel, Microsoft Defender for Cloud, and Microsoft 365 Defender. In this course you will learn how to mitigate cyberthreats using these technologies. Specifically, you will configure and use Microsoft 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 Sentinel, Microsoft Defender for Cloud, 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.

Contents

Learning path 1: Mitigate threats using Microsoft Defender XDR

- Introduction to threat protection with Microsoft Defender XDR
- Mitigate incidents using Microsoft Defender XDR
- Remediate risks with Defender for Office 365 in Microsoft Defender XDR
- Microsoft Defender for Identity in Microsoft Defender XDR
- Protect your identities with Entra ID Protection
- Defender for Cloud Apps in Microsoft Defender XDR

Learning Path 2: Mitigate threats using Microsoft Purview

- Microsoft Purview Compliance Solutions
- Investigate and remediate compromised entities identified by Microsoft Purview data loss prevention (DLP) policies
- Investigate and remediate insider risk threats identified by Microsoft Purview policies
- Investigate threats using Content search in Microsoft Purview
- Investigate threats using Microsoft Purview Audit (Standard)
- Investigate threats using Microsoft Purview Audit (Premium)

Learning Path 3: Mitigate threats using Microsoft Defender for Endpoint

- Protect against threats with Microsoft Defender for Endpoint
- Deploy the Microsoft Defender for Endpoint environment
- Implement Windows security enhancements
- Perform device investigations
- Perform actions on a device
- Perform evidence and entities investigations
- Configure and manage automation
- Configure for alerts and detections
- Utilize Threat and Vulnerability Management

Learning Path 4: Mitigate threats using Microsoft Defender for Cloud

- Plan for cloud workload protections using Microsoft Defender for Cloud
- Connect Azure assets to Microsoft Defender for Cloud
- Connect non-Azure assets to Microsoft Defender for Cloud
- Manage your cloud security posture management
- Workload protections in Microsoft Defender for Cloud
- Remediate security alerts using Microsoft Defender for Cloud

Learning Path 5: Create queries for Microsoft Sentinel using Kusto Query Language (KQL)

- Construct KQL statements for Microsoft Sentinel
- Analyze query results using KQL
- Build multi-table statements using KQL
- Work with string data in using KQL statements

Learning Path 6: Configure your Microsoft Sentinel environment

- Introduction to Microsoft Sentinel
- Create and manage Microsoft Sentinel workspaces
- Query logs in Microsoft Sentinel
- Use watchlists in Microsoft Sentinel
- Utilize threat intelligence in Microsoft Sentinel

Learning Path 7: Connect logs to Microsoft Sentinel

- Manage content in Microsoft Sentinel
- Connect data to Microsoft Sentinel using data connectors
- Connect Microsoft services to Microsoft Sentinel

- Connect Microsoft Defender XDR to Microsoft Sentinel
- Connect Windows hosts to Microsoft Sentinel
- Connect Common Event Format logs to Microsoft Sentinel
- Connect syslog data sources to Microsoft Sentinel
- Connect threat indicators to Microsoft Sentinel

Learning Path 8: Create detections and perform investigations using Microsoft Sentinel

- Threat detection with Microsoft Sentinel analytics
- Automation in Microsoft Sentinel
- Threat response with Microsoft Sentinel playbooks
- Security incident management in Microsoft Sentinel
- Entity behavioral analytics in Microsoft Sentinel
- Data normalization in Microsoft Sentinel
- Query, visualize, and monitor data in Microsoft Sentinel

Learning Path 9: Perform threat hunting in Microsoft Sentinel

- Explain threat hunting concepts in Microsoft Sentinel
- Threat hunting with Microsoft Sentinel
- Use Search jobs in Microsoft Sentinel
- Optional – Hunt for threats using notebooks in Microsoft Sentinel

About GTech Learn

Established in 2011 in the USA, GTech Learn is one of the leading IT training organizations in North America & South East Asia. Driven by its unique USPs, GTech Learn is spurring competition, meeting the unmet needs of customers, assisting in skills upgrade, and supplementing talent pools with its presence in the USA, Canada, Singapore and India. This is consistent with our vision to help our Learners with skills upgrade for enhanced career opportunities.

As a Microsoft Learning Partner, we offer a broad range of learning solutions across the full Microsoft technology stack that can be customized.

Since 2011, GTech Learn has been developing custom-fit learning solutions that involve creating and delivering maximum results.

We have successfully helped all types of businesses, government entities, and individuals. For this reason, GTech has chosen by Microsoft to deliver comprehensive learning programs around the globe.

With flexible learning options, state-of-the-art delivery methods, numerous language preferences, experienced instructors, and complete dedication to our students, GTech Learn has the capabilities to help students develop their Microsoft skill sets and achieve increasingly high standards of productivity while organizations of all sizes realize the full potential of their technology investments.

Our Accreditations with Microsoft



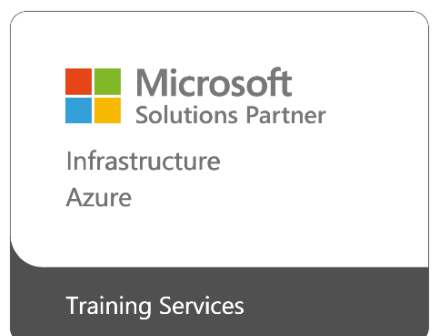
Microsoft Solutions Partner
Security
Training Services



Microsoft Solutions Partner
Modern Work
Training Services



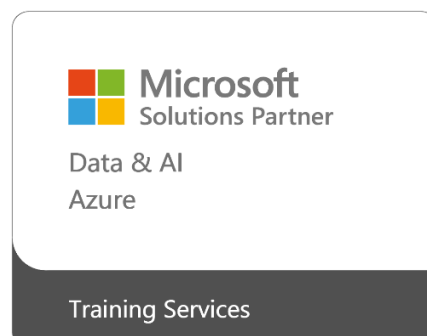
Microsoft Solutions Partner
Business Applications
Training Services



Microsoft Solutions Partner
Infrastructure
Azure
Training Services



Microsoft Solutions Partner
Digital & App Innovation
Azure
Training Services



Microsoft Solutions Partner
Data & AI
Azure
Training Services