

Microsoft Security Operations Analyst

Duration: 4 Days **Course Code: M-SC200** **Delivery Method: Virtual Learning**

Overview:

Learn how to investigate, respond to, and hunt for threats using Microsoft Sentinel, Microsoft Defender XDR and Microsoft Defender for Cloud. 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.

Virtual Learning

This interactive training can be taken from any location, your office or home and is delivered by a trainer. This training does not have any delegates in the class with the instructor, since all delegates are virtually connected. Virtual delegates do not travel to this course, Global Knowledge will send you all the information needed before the start of the course and you can test the logins.

Target Audience:

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 XDR, Microsoft Defender for Cloud, 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.

Objectives:

- SC-200: Mitigate threats using Microsoft Defender XDR
- SC-200: Mitigate threats using Microsoft Copilot for Security
- SC-200: Mitigate threats using Microsoft Purview
- SC-200: Mitigate threats using Microsoft Defender for Endpoint
- SC-200: Mitigate threats using Microsoft Defender for Cloud
- SC-200: Create queries for Microsoft Sentinel using Kusto Query Language (KQL)
- SC-200: Configure your Microsoft Sentinel environment
- SC-200: Connect logs to Microsoft Sentinel
- SC-200: Create detections and perform investigations using Microsoft Sentinel
- SC-200: Perform threat hunting in Microsoft Sentinel

Testing and Certification

Microsoft Certified: Security Operations Analyst Associate

Content:

SC-200: Mitigate threats using Microsoft Defender XDR

- Introduction to Microsoft Defender XDR threat protection
- Mitigate incidents using Microsoft 365 Defender
- Protect your identities with Microsoft Entra ID 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

SC-200: Mitigate threats using Microsoft Copilot for Security

- Fundamentals of Generative AI
- Describe Microsoft Copilot for Security
- Describe the core features of Microsoft Copilot for Security
- Describe the embedded experiences of Microsoft Copilot for Security

SC-200: Mitigate threats using Microsoft Purview

- Respond to data loss prevention alerts using Microsoft 365
- Manage insider risk in Microsoft Purview
- Search and investigate with Microsoft Purview Audit
- Investigate threats with Content search in Microsoft Purview

SC-200: 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 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

SC-200: 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 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

SC-200: 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 data in Microsoft Sentinel using Kusto Query Language

SC-200: 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

SC-200: Connect logs to 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

SC-200: 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
- Identify threats with Behavioral Analytics
- Data normalization in Microsoft Sentinel
- Query, visualize, and monitor data in Microsoft Sentinel
- Manage content in Microsoft Sentinel

SC-200: Perform threat hunting in Microsoft Sentinel

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

Further Information:

For More information, or to book your course, please call us on 00 20 (0) 2 2269 1982 or 16142

training@globalknowledge.com.eg

www.globalknowledge.com/en-eg/

Global Knowledge, 16 Moustafa Refaat St. Block 1137, Sheraton Buildings, Heliopolis, Cairo