SC-200: MICROSOFT SECURITY OPERATIONS ANALYST

LEVEL	INTERMEDIATE	ROLE	SECURITY ENGINEER, SECURITY OPERATIONSANALYST
DURATION	4 DAY	PRODUCT	MICROSOFT DEFENDER FOR ENDPOINT

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.

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 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.

In this course, you will learn how to:

- In tDevelop expertise in leveraging Microsoft Sentinel to design, implement, and manage security monitoring and analytics.
- Gain proficiency in crafting Kusto Query Language (KQL) queries to perform efficient threat detection and data analysis.
- Identify and automate repetitive security tasks to enhance operational efficiency using Microsoft Defender automation capabilities.
- Conduct in-depth investigations into multi-domain threats using integrated Microsoft Defender XDR tools.
- Understand and configure advanced security features for endpoint protection using Defender for Endpoint.
- Ensure compliance by identifying, protecting, and auditing sensitive information in organizational data using Microsoft Purview solutions.
- Design and enforce access policies for secure identity management through Microsoft Entra Identity Protection.
- Utilize Microsoft Security Copilot to improve decision-making in handling complex security incidents.
- Enhance incident response effectiveness by using data-driven insights and analytics from Defender for Cloud to improve an organization's security posture.
- Manage and mitigate insider threats by leveraging detection capabilities in Microsoft Purview Insider Risk Management.
- Build a strong foundation in hybrid cloud security, protecting both on-premises and Azure-hosted resources.

- Reduce exposure to vulnerabilities using proactive threat management features in security products like Defender for Endpoint.
- Ensure effective collaboration between all security stakeholders and technologies for holistic protection of the organization's IT ecosystem.

Course Prerequisites:

Before attempting SC-200, attendees should have a:

- Fundamental understanding of Microsoft security, compliance, and identity products.
- Basic experience with Microsoft Defender XDR and Azure services.
- Familiarity with computer networking concepts and practices.

Security Operations Analyst Training Outline

Learning Objectives

Module 1: Mitigate Threats Using Microsoft 365 Defender

- Discover how Microsoft Defender XDR integrates across domains for holistic threat protection.
- Configure and utilize Microsoft 365 Defender for incidents and alerts.
- Conduct investigations with tools like Microsoft Defender for Office 365 and Microsoft Defender for Identity.
- Manage identities and user activities with Microsoft Entra Identity Protection.

Module 2: Mitigate Threats Using Microsoft Security Copilot

- Learn the fundamentals of Generative AI with Microsoft Security Copilot.
- Explore how Microsoft Security Copilot processes natural language input for threat mitigation.

- Integrate Microsoft Security Copilot into security workflows and tools.
- Use practical scenarios to enhance security operations with AI-powered solutions.

Module 3: Mitigate Threats Using Microsoft Purview

- Understand compliance and information protection using Microsoft Purview.
- Respond to data loss prevention alerts and manage insider risk.
- Use Purview Audit for searching, investigating, and monitoring security compliance.
- Investigate threats through content searches in Microsoft Purview.

Module 4: Mitigate Threats Using Microsoft Defender for Endpoint

- Implement and manage Microsoft Defender for Endpoint to protect devices.
- Investigate and remediate advanced threats across endpoints using built-in tools.
- Perform actions like device isolation and forensic data collection.
- Automate security actions to proactively reduce vulnerabilities.

Module 5: Mitigate Threats Using Azure Defender (Microsoft Defender for Cloud)

- Plan and enable cloud workload protections in hybrid and multicloud environments.
- Connect Azure and non-Azure resources to Microsoft Defender for Cloud.
- Remediate security alerts and improve cloud security posture through guidance and tools.
- Monitor and respond to threats targeting cloud assets and workloads.

Further Information:

For More information, or to book your course

Course SC-200: Microsoft Security Operations Analyst

https://smartteklearning.com/Course/sc-200-microsoft-security-operations-analyst/

https://smartteklearning.com
info@smartteklearning.com