Web: www.secureninja.com
Phone: 703.535.8600
Email: info@secureninja.com

Microsoft Certified: Security Operations Analyst Associate

Course Description & Overview

SecureNinja’s Microsoft Certified: Security Operations Analyst Associate certification training is a comprehensive program designed to prepare learners for detecting, investigating, responding to, and remediating threats using Microsoft security solutions. This detailed course equips students with the skills to monitor and respond to threats across Microsoft 365 Defender, Microsoft Defender for Cloud, and Microsoft Sentinel.

Participants will explore the principles of threat protection and security incident management in a hybrid enterprise environment. By leveraging Microsoft's integrated security tools, participants will develop the technical expertise necessary for real-time security operations. This course also prepares students for the SC-200 exam, which is required to earn the Microsoft Certified: Security Operations Analyst Associate credential.

Why Choose Microsoft Certified: Security Operations Analyst Associate

- Role-Based Certification: Designed for SOC analysts and security professionals working with Microsoft technologies.
- Integrated Threat Protection: Learn how to use Microsoft 365 Defender, Azure Defender, and Microsoft Sentinel to investigate and mitigate threats.
- Cloud-Focused: Tailored for cloud-first environments with Microsoft security solutions.
- Hands-On Skill Development: Lab exercises and case studies based on real-world threat scenarios.

Topics Covered

- Microsoft 365 Defender: Investigating and responding to threats using Defender for Endpoint, Defender for Office 365, Defender for Identity, and more.
- Microsoft Sentinel: Configure and use a SIEM for data collection, analysis, and incident response.
- Azure Defender: Protect cloud workloads across hybrid environments.
- Threat Hunting: Use Kusto Query Language (KQL) to build custom queries and identify threats.
- Incident Response: Investigate security incidents, escalate threats, and improve detection rules.

Who is it for

- Security Analysts: Working in security operations centers or cloud environments.
- IT Professionals: Looking to enhance their Microsoft security capabilities.
- SOC Engineers: Focused on incident detection, response, and remediation.

Who Would Benefit

- Individuals preparing for the SC-200 certification exam.

Web: www.secureninja.com
Phone: 703.535.8600
Email: info@secureninja.com

- Organizations using Microsoft Defender, Sentinel, or Azure security tools.
- Teams transitioning to a cloud-first security operations model.

Prerequisites

Basic familiarity with Microsoft Azure and Microsoft 365. A foundational understanding of cybersecurity principles is recommended.

Course Outline

1. Mitigate threats using Microsoft 365 Defender

    - Explore Microsoft 365 Defender portal and components
    - Investigate threats using Microsoft Defender for Endpoint, Office 365, Identity, and Cloud Apps

2. Mitigate threats using Microsoft Sentinel

    - Configure Microsoft Sentinel and connect data sources
    - Create and tune analytics rules and use workbooks
    - Investigate incidents and respond with playbooks

3. Mitigate threats using Microsoft Defender for Cloud

    - Assess and strengthen security posture for cloud workloads
    - Use Defender for Cloud to detect and respond to threats across IaaS and PaaS resources

4. Create queries for Microsoft Sentinel using KQL

    - Write KQL queries for log and telemetry data
    - Visualize and interpret query results

5. Configure automation and threat detection

    - Build automation with Logic Apps and playbooks
    - Improve detection accuracy and reduce false positives

Course Length

- 5 Days
- 40 Hours

Exam Details

- Exam Code: SC-200
- Certification: Microsoft Certified: Security Operations Analyst Associate
- Question Types: Multiple-choice, case studies, drag-and-drop, labs
- Duration: 120 minutes
- Passing Score: 700 (on a scale of 100–1000)

Web: www.secureninja.com
Phone: 703.535.8600
Email: info@secureninja.com

The SC-200 certification is ideal for cybersecurity professionals looking to expand their knowledge of Microsoft’s security ecosystem and gain in-demand skills in threat detection and response. With expert-led instruction and immersive labs, SecureNinja’s training provides the foundation needed to confidently secure modern cloud environments and prepare for real-world security operations.