Training Course SC-200: Microsoft Security Operations Analyst

Overview: Microsoft Security Operations Analyst certification training focuses on developing skills to mitigate threats using Microsoft's security, compliance, and identity solutions. The course covers a range of topics including threat protection, security management, identity & access configuration and management. Participants learn to protect cloud and hybrid environments, configure Microsoft 365 Defender and Microsoft Defender for Endpoint, and understanding Microsoft's Zero Trust model. The training also involves hands-on labs for practical learning.

Duration: 4 Days.

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.

Certification: This course prepares you for the SC-200: Microsoft Security Operations Analyst.

Course Objectives: After completing this course, students will be able to:

- Explain how Microsoft Defender for Endpoint can remediate risks in your environment.
- Administer a Microsoft Defender for Endpoint environment.
- Configure Attack Surface Reduction rules on Windows 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 365 Defender.
- Conduct 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 Defender for Cloud Apps.
- Explain the types of actions you can take on an insider risk management cases.
- Configure auto-provisioning in Microsoft Defender for Cloud Apps.
- Remediate alerts in Microsoft Defender for Cloud Apps.
- 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 a Microsoft Sentinel workspace.
- Use KQL to access the watchlist in Microsoft Sentinel.
- Manage threat indicators in Microsoft Sentinel.
- Explain the Common Event Format and Syslog connector differences in Microsoft Sentinel.
- Connect Azure Windows Virtual Machines to Microsoft 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.

Course Outline:

1- Introduction to Microsoft 365 threat protection.
   - Understand Microsoft 365 Defender solution by domain.
   - Understand Microsoft 365 Defender role in a Modern SOC.

2- Mitigate incidents using Microsoft 365 Defender.
   - Manage incidents in Microsoft 365 Defender.
   - Investigate incidents in Microsoft 365 Defender.
   - Conduct advanced hunting in Microsoft 365 Defender.

3- Protect your identities with Azure AD Identity Protection.
   - Describe the features of Azure Active Directory Identity Protection.
   - Describe the investigation and remediation features of Azure Active Directory Identity Protection

4- Remediate risks with Microsoft Defender for Office 365.
   - Define the capabilities of Microsoft Defender for Office 365.
   - Understand how to simulate attacks within your network.
   - Explain how Microsoft Defender for Office 365 can remediate risks in your environment.

5- Safeguard your environment with Microsoft Defender for Identity.
   - Define the capabilities of Microsoft Defender for Identity.
   - Understand how to configure Microsoft Defender for Identity sensors.
     - Explain how Microsoft Defender for Identity can remediate risks in your environment.

6- Secure your cloud apps and services with Microsoft Defender for Cloud Apps.
   - Define the Defender for Cloud Apps framework.
   - Explain how Cloud Discovery helps you see what's going on in your organization.
   - Understand how to use Conditional Access App Control policies to control access to the apps in your organization.

7- Respond to data loss prevention alerts using Microsoft 365.
   - Describe data loss prevention (DLP) components in Microsoft 365.
   - Investigate DLP alerts in the Microsoft Purview compliance portal.
   - Investigate DLP alerts in Microsoft Defender for Cloud Apps.

8- Manage insider risk in Microsoft Purview

- Explain how Microsoft Purview Insider Risk Management can help prevent, detect, and contain internal risks in an organization.
- Describe the types of built-in, pre-defined policy templates.
- List the prerequisites that need to be met before creating insider risk policies.
- Explain the types of actions you can take on an insider risk management case.

9- Investigate threats by using audit features in Microsoft 365 Defender and Microsoft Purview Standard
- Describe the differences between Audit (Standard) and Audit (Premium).
- Start recording user and admin activity in the Unified Audit Log (UAL).
- Identify the core features of the Audit (Standard) solution.
- Set up and implement audit log searching using the Audit (Standard) solution.
- Export, configure, and view audit log records.
- Use audit log searching to troubleshoot common support issues.

10- Investigate threats using audit in Microsoft 365 Defender and Microsoft Purview (Premium).
- Describe the differences between Audit (Standard) and Audit (Premium).
- Set up and implement Microsoft Purview Audit (Premium).
- Create audit log retention policies.
- Perform forensic investigations of compromised user accounts.

11- Investigate threats with Content search in Microsoft Purview
- Describe how to use content search in the Microsoft Purview compliance portal.
- Design and create a content search.
- Preview the search results.
- View the search statistics.
- Export the search results and search report.
- Configure search permission filtering.

12- Protect against threats with Microsoft Defender for Endpoint
- Define the capabilities of Microsoft Defender for Endpoint.
- Understand how to hunt threats within your network.
- Explain how Microsoft Defender for Endpoint can remediate risks in your environment.

13- Deploy the Microsoft Defender for Endpoint environment.
- Create a Microsoft Defender for Endpoint environment.
- Onboard devices to be monitored by Microsoft Defender for Endpoint.
- Configure Microsoft Defender for Endpoint environment settings.

14- Implement Windows security enhancements with Microsoft Defender for Endpoint
- Explain Attack Surface Reduction in Windows.
- Enable Attack Surface Reduction rules on Windows 10 devices.
- Configure Attack Surface Reduction rules on Windows 10 devices.

15- Perform device investigations in Microsoft Defender for Endpoint.
- Use the device page in Microsoft Defender for Endpoint.
- Describe device forensics information collected by Microsoft Defender for Endpoint.
- Describe behavioral blocking by Microsoft Defender for Endpoint.

16- Perform actions on a device using Microsoft Defender for Endpoint.
- Perform actions on a device using Microsoft Defender for Endpoint.
- Conduct forensics data collection using Microsoft Defender for Endpoint.

- Access devices remotely using Microsoft Defender for Endpoint.

17- Perform evidence and entities investigations using Microsoft Defender for Endpoint.
  - Investigate files in Microsoft Defender for Endpoint
  - Investigate domains and IP addresses in Microsoft Defender for Endpoint
  - Investigate user accounts in Microsoft Defender for Endpoint

18- Configure and manage automation using Microsoft Defender for Endpoint
  - Configure advanced features of Microsoft Defender for Endpoint.
  - Manage automation settings in Microsoft Defender for Endpoint.

19- Configure for alerts and detections in Microsoft Defender for Endpoint
  - Configure alert settings in Microsoft Defender for Endpoint.
  - Manage indicators in Microsoft Defender for Endpoint.

20- Utilize Vulnerability Management in Microsoft Defender for Endpoint.
  - Describe Vulnerability Management in Microsoft Defender for Endpoint.
  - Identify vulnerabilities on your devices with Microsoft Defender for Endpoint.
  - Track emerging threats in Microsoft Defender for Endpoint.

21- Plan for cloud workload protections using Microsoft Defender for Cloud
  - Describe Microsoft Defender for Cloud features.
  - Microsoft Defender for Cloud workload protections.
  - Enable Microsoft Defender for Cloud.

22- Connect Azure assets to Microsoft Defender for Cloud
  - Explore Azure assets.
  - Configure auto-provisioning in Microsoft Defender for Cloud.
  - Describe manual provisioning in Microsoft Defender for Cloud.

23- Connect non-Azure resources to Microsoft Defender for Cloud
  - Connect non-Azure machines to Microsoft Defender for Cloud.
  - Connect AWS accounts to Microsoft Defender for Cloud.
  - Connect GCP accounts to Microsoft Defender for Cloud.

24- Manage your cloud security posture management.
  - Describe Microsoft Defender for Cloud features.
  - Explain the Microsoft Defender for Cloud security posture management protections for your resources.

25- Explain cloud workload protections in Microsoft Defender for Cloud.
  - Explain which workloads are protected by Microsoft Defender for Cloud.
  - Describe the benefits of the protections offered by Microsoft Defender for Cloud.
  - Explain how Microsoft Defender for Cloud protections function.

26- Remediate security alerts using Microsoft Defender for Cloud.
  - Describe alerts in Microsoft Defender for Cloud.
  - Remediate alerts in Microsoft Defender for Cloud.
  - Automate responses in Microsoft Defender for Cloud.

27- Construct KQL statements for Microsoft Sentinel.
  - Construct KQL statements.
  - Search log files for security events using KQL.
  - Filter searches based on event time, severity, domain, and other relevant data using KQL.

28- Analyze query results using KQL.

- Summarize data using KQL statements.
- Render visualizations using KQL statements.

29- Build multi-table statements using KQL.
- Create queries using unions to view results across multiple tables using KQL.
- Merge two tables with the join operator using KQL.

30- Work with data in Microsoft Sentinel using Kusto Query Language.
- Extract data from unstructured string fields using KQL.
- Extract data from structured string data using KQL.
- Create Functions using KQL.

31- Introduction to Microsoft Sentinel.
- Identify the various components and functionality of Microsoft Sentinel.
- Identify use cases where Microsoft Sentinel would be a good solution.

32- Create and manage Microsoft Sentinel workspaces.
- Describe Microsoft Sentinel workspace architecture.
- Install Microsoft Sentinel workspace.
- Manage a Microsoft Sentinel workspace.

33- Query logs in Microsoft Sentinel.
- Use the Logs page to view data tables in Microsoft Sentinel.
- Query the most used tables using Microsoft Sentinel.

34- Use watchlists in Microsoft Sentinel.
- Create a watchlist in Microsoft Sentinel.
- Use KQL to access the watchlist in Microsoft Sentinel.

35- Utilize threat intelligence in Microsoft Sentinel.
- Manage threat indicators in Microsoft Sentinel.
- Use KQL to access threat indicators in Microsoft Sentinel.

36- Connect data to Microsoft Sentinel using data connectors.
- Explain the use of data connectors in Microsoft Sentinel.
- Describe the Microsoft Sentinel data connector providers.
- Explain the Common Event Format and Syslog connector differences in Microsoft Sentinel.

37- Connect Microsoft services to Microsoft Sentinel.
- Connect Microsoft service connectors.
- Explain how connectors auto-create incidents in Microsoft Sentinel.

38- Connect Microsoft 365 Defender to Microsoft Sentinel.
- Activate the Microsoft 365 Defender connector in Microsoft Sentinel.
- Activate the Microsoft Defender for Cloud connector in Microsoft Sentinel.
- Activate the Microsoft Defender for IoT connector in Microsoft Sentinel.

39- Connect Windows hosts to Microsoft Sentinel.
- Connect Azure Windows Virtual Machines to Microsoft Sentinel.
- Connect non-Azure Windows hosts to Microsoft Sentinel.
- Configure Log Analytics agent to collect Sysmon events.

40- Connect Common Event Format logs to Microsoft Sentinel.
- Explain the Common Event Format connector deployment options in Microsoft Sentinel.
- Run the deployment script for the Common Event Format connector.

41- Connect syslog data sources to Microsoft Sentinel.

- Describe the Syslog connector deployment options in Microsoft Sentinel.
- Run the connector deployment script to send data to Microsoft Sentinel.
- Configure the Log Analytics agent integration for Microsoft Sentinel.
- Create a parse using KQL in Microsoft Sentinel.

42- Connect threat indicators to Microsoft Sentinel.
- Configure the TAXII connector in Microsoft Sentinel.
- Configure the Threat Intelligence Platform connector in Microsoft Sentinel.
- View threat indicators in Microsoft Sentinel.

43- Threat detection with Microsoft Sentinel analytics.
- Explain the importance of Microsoft Sentinel Analytics.
- Explain different types of analytics rules.
- Create rules from templates.
- Create new analytics rules and queries using the analytics rule wizard.
- Manage rules with modifications.

44- Automation in Microsoft Sentinel.
- Explain automation options in Microsoft Sentinel.
- Create automation rules in Microsoft Sentinel.

45- Security incident management in Microsoft Sentinel.
- Understand Microsoft Sentinel incident management.
- Explore Microsoft Sentinel evidence and entity management.
- Investigate and manage incident resolution.

46- Identify threats with Behavioral Analytics.
- Explain User and Entity Behavior Analytics in Azure Sentinel.
- Explore entities in Microsoft Sentinel.

47- Data normalization in Microsoft Sentinel.
- Use ASIM Parsers.
- Create ASIM Parser.
- Create parameterized KQL functions.

48- Query, visualize, and monitor data in Microsoft Sentinel.
- Visualize security data using Microsoft Sentinel Workbooks.
- Understand how queries work.
- Explore workbook capabilities.
- Create a Microsoft Sentinel Workbook.

49- Manage content in Microsoft Sentinel.
- Install a content hub solution in Microsoft Sentinel.
- Connect a GitHub repository to Microsoft Sentinel.

50- Explain threat hunting concepts in Microsoft Sentinel.
- Describe threat hunting concepts for use with Microsoft Sentinel.
- Define a threat hunting hypothesis for use in Microsoft Sentinel.

51- Threat hunting with Microsoft Sentinel.
- Use queries to hunt for threats.
- Save key findings with bookmarks.
- Observe threats over time with livestream.

52- Use Search jobs in Microsoft Sentinel.
    - Use Search Jobs in Microsoft Sentinel.
    - Restore archive logs in Microsoft Sentinel.
53- Hunt for threats using notebooks in Microsoft Sentinel.
    - Explore API libraries for advanced threat hunting in Microsoft Sentinel.
    - Describe notebooks in Microsoft Sentinel.
    - Create and use notebooks in Microsoft Sentinel.