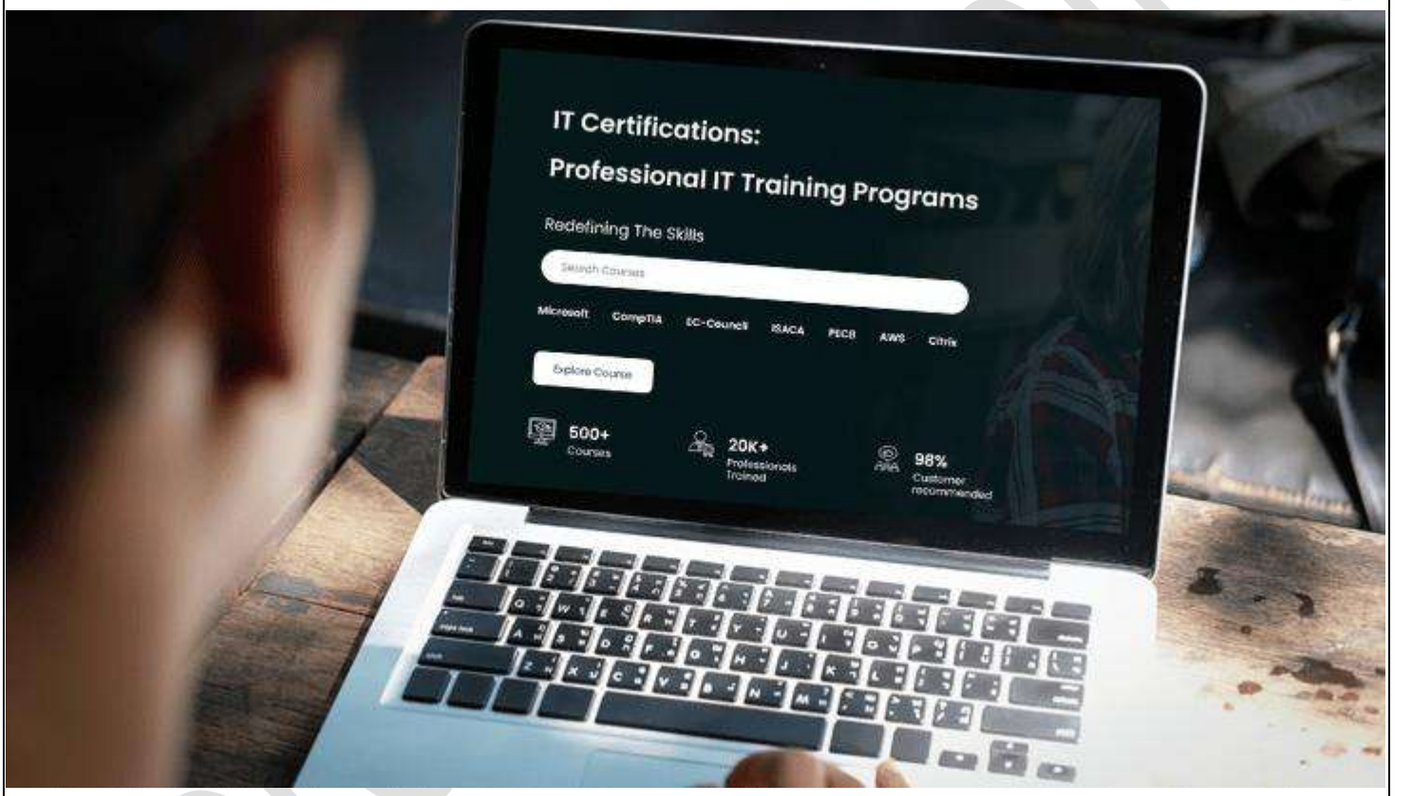
MICROTEK LEARNING | Redefining The Skills



SC-200: MICROSOFT SECURITY OPERATIONS ANALYST TRAINING

Duration: 4 Days

Course Description

SC-200: Microsoft Security Operations Analyst Training is designed for security engineers. This course lets Microsoft Security Operations Analysts amalgamate with the original stakeholders to develop secure IT systems. The main purpose of the course is to help professionals reduce the organizational threats for the firms.

By doing this course professionals will learn about threat mitigation using Microsoft 365 Defender, eliminating the threat using Azure Defender and Azure Sentinel.

After completion of this course Microsoft Security Operations Analysts as professionals can expect themselves to be upskilled from their current position. They can find themselves in the position of chief IT security engineer or Security Operation Analyst.

This training is designed based on the objectives of the course variant SC-200T00-A.

Who should attend this course?

- 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.
- Responsibility also includes threat management, monitoring, and response by using a variety of security solutions across their environment
- Security Operations Analysts consuming the operational output of these tools, are also critical stakeholders in the configuration and deployment of these technologies.
- Given below are professionals who can use Microsoft Security Operations Analyst Training to upskill their current positions:
    - IT Security Engineers
    - Cloud Security Engineers
    - Compliance Officers who deal with cybersecurity
    - IT professionals willing to pursue a career in cybersecurity
    - Cybersecurity specialist
    - Incident response team
    - Threat Intelligence Analyst

What you will learn

- Comprehending how Microsoft Defender for Endpoint can remediate risks in your environment.
- Creating Microsoft Defender for the Endpoint environment
- Configuring Attach Surface Reduction rules on Windows 10 devices
- Performing actions on a device using Microsoft Defender for Endpoint
- Investigating domains and IP addresses in Microsoft Defender for Endpoint
- Investigating use accounts in Microsoft Defender for Endpoint
- Configuring alert settings in Microsoft Defender for Endpoint
- Learning how the threat landscape is evolving
- Conducting advanced hunting Microsoft 365 Defender
- Explaining how Microsoft Defender for Identity can remediate risks in your environment
- Investigate DLP alerts in Microsoft Cloud App Security
- Learning the types of actions you can take on an insider risk management case
- Configuring auto-provisioning in Azure Defender
- Remediate alerts in Azure Defender
- Construct KQL statements

- Filter searched based on the event time, severity, domain, and other relevant data using KQL
- Extracting data from unstructured string fields using KQL
- Managing an Azure Sentinel Workspace
- Using KQL to access the watchlist in Azure Sentinel
- Manage threat indicators in Azure Sentinel
- Explaining the Common Event Format and Syslog connector differences in Azure Sentinel
- Learning to connect Azure Windows Virtual Machines to Azure Sentinel
- Configuring Log Analytics agent to collect Sysmon events
- Creating new analytics rules and queries using the analytics rule wizard
- Creating a playbook to automate an incident response
- Using queries to hunt for threats
- Observing threats over time with Livestream

Prerequisites

- Basic understanding of Microsoft 365 and scripting concepts
- Fundamental understanding of Microsoft Security, compliance, and identity products
- Intermediate understanding of Windows 10
- Familiarity with Azure Services, specifically with Azure SQL Database and Azure Storage
- Familiarity with Azure virtual machines and virtual networking
- A basic understanding of Microsoft Defender XDR

Curriculum

Module 1: Mitigate threats using Microsoft Defender XDR

- Introduction to Microsoft Defender XDR threat protection
    - Understand Microsoft Defender XDR solutions by domain
    - Understand the Microsoft Defender XDR role in a Modern SOC
- Mitigate incidents using Microsoft Defender
    - Manage incidents in Microsoft Defender
    - Investigate incidents in Microsoft Defender
    - Conduct advanced hunting in Microsoft Defender
- 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.
- Manage Microsoft Entra Identity Protection
    - Implement and manage a user risk policy.
    - Implement and manage sign-in risk policies.
    - Implement and manage MFA registration policy.
    - Monitor, investigate, and remediate elevated risky users.
- 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.
- 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.

- 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.

Module 2: Mitigate threats using Microsoft Security Copilot

- Fundamentals of Generative AI
    - Understand generative AI's place in the development of artificial intelligence.
    - Understand language models and their role in intelligent applications.
    - Describe examples of copilots and good prompts.
- Describe Microsoft Security Copilot
    - Describe what Microsoft Security Copilot is.
    - Describe the terminology of Microsoft Security Copilot.
    - Describe how Microsoft Security Copilot processes prompt requests.
    - Describe the elements of an effective prompt
    - Describe how to enable Microsoft Security Copilot.
- Describe the core features of Microsoft Security Copilot
    - Describe the features available in the standalone Copilot experience.
    - Describe the plugins available in Copilot.
    - Describe custom promptbooks.
    - Describe knowledge base connections.
- Describe the embedded experiences of Microsoft Security Copilot
    - Describe Copilot in Microsoft Defender XDR.
    - Describe Copilot in Microsoft Purview.
    - Describe Copilot in Microsoft Entra.
    - Describe Copilot in Microsoft Intune.
    - Describe Copilot in Microsoft Defender for Cloud.
- Explore use cases of Microsoft Security Copilot
    - Set up Microsoft Security Copilot.
    - Work with sources in Copilot.
    - Create a custom promptbook.
    - Use the capabilities of Copilot in Defender XDR.
    - Use the capabilities of Copilot in Microsoft Purview.

Module 3: Mitigate threats using Microsoft Purview

- 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
- 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.
- Search and investigate with Microsoft Purview Audit
    - Identify the differences between Microsoft Purview Audit (Standard) and Audit (Premium).
    - Configure Microsoft Purview Audit for optimal log management.
    - Perform audits to assess compliance and security measures.
    - Analyze irregular access patterns using advanced tools in Purview Audit (Premium) and PowerShell.

- Ensure regulatory compliance through strategic data management.
- 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.

Module 4: Mitigate threats using Microsoft Defender for Endpoint

- 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.
- 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
- 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
- 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
- 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
- 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
- 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
- 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
- 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

Module 5: Mitigate threats using Microsoft Defender for Cloud

- 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

- 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
- 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
- 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.
- 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
- 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

Module 6: Create queries for Microsoft Sentinel using Kusto Query Language (KQL)

- 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
- Analyze query results using KQL
    - Summarize data using KQL statements
    - Render visualizations using KQL statements
- 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
- 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

Module 7: Configure your Microsoft Sentinel environment

- Introduction to Microsoft Sentinel
    - Identify the various components and functionality of Microsoft Sentinel.
    - Identify use cases where Microsoft Sentinel would be a good solution.
- Create and manage Microsoft Sentinel workspaces
    - Describe Microsoft Sentinel workspace architecture
    - Install Microsoft Sentinel workspace
    - Manage a Microsoft Sentinel workspace
- Query logs in Microsoft Sentinel
    - Use the Logs page to view data tables in Microsoft Sentinel
    - Query the most used tables using Microsoft Sentinel
- Use watchlists in Microsoft Sentinel
    - Create a watchlist in Microsoft Sentinel
    - Use KQL to access the watchlist in Microsoft Sentinel

- Utilize threat intelligence in Microsoft Sentinel
    - Manage threat indicators in Microsoft Sentinel
    - Use KQL to access threat indicators in Microsoft Sentinel
- Integrate Microsoft Defender XDR with Microsoft Sentinel
    - Understand the differences between Microsoft Sentinel capabilities in Azure and Defender portals
    - Know the prerequisites for integrating Microsoft Defender XDR with Microsoft Sentinel
    - Connect a Microsoft Sentinel workspace to Microsoft Defender XDR

Module 8: Connect logs to Microsoft Sentinel

- Connect data to Microsoft Sentinel using data connectors
    - Describe how to install Content Hub Solutions to provision Microsoft Sentinel 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
- Connect Microsoft services to Microsoft Sentinel
    - Connect Microsoft service connectors
    - Explain how connectors auto-create incidents in Microsoft Sentinel
- Connect Microsoft Defender XDR to Microsoft Sentinel
    - Activate the Microsoft Defender XDR connector in Microsoft Sentinel
    - Activate the Microsoft Defender for Cloud connector in Microsoft Sentinel
    - Activate the Microsoft Defender for IoT connector in Microsoft Sentinel
- 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
- 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
- Connect syslog data sources to Microsoft Sentinel
    - Describe the Azure Monitor Agent Data Collection Rule (DCR) for Syslog
    - Install and Configure the Azure Monitor Linux Agent extension with the Syslog DCR
    - Run the Azure Arc Linux deployment and connection scripts
    - Verify Syslog log data is available in Microsoft Sentinel
    - Create a parser using KQL in Microsoft Sentinel
- 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

Module 9: Create detections and perform investigations using Microsoft Sentinel

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

- Threat response with Microsoft Sentinel playbooks
    - Explain Microsoft Sentinel SOAR capabilities.
    - Explore the Microsoft Sentinel Logic Apps connector.
    - Create a playbook to automate an incident response.
    - Run a playbook on demand in response to an incident.
- Security incident management in Microsoft Sentinel
    - Learn about security incidents and Microsoft Sentinel incident management.
    - Explore Microsoft Sentinel incident evidence and entities.
    - Use Microsoft Sentinel to investigate security incidents and manage incident resolution.
- Identify threats with Behavioral Analytics
    - Explain User and Entity Behavior Analytics in Azure Sentinel
    - Explore entities in Microsoft Sentinel
- Data normalization in Microsoft Sentinel
    - Use ASIM Parsers
    - Create ASIM Parser
    - Create parameterized KQL functions
- 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.
- Manage content in Microsoft Sentinel
    - Install a content hub solution in Microsoft Sentinel
    - Connect a GitHub repository to Microsoft Sentinel

Module 10: Perform threat hunting in Microsoft Sentinel

- 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
- Threat hunting with Microsoft Sentinel
    - Use queries to hunt for threats.
    - Save key findings with bookmarks.
    - Observe threats over time with livestream.
- Use Search jobs in Microsoft Sentinel
    - Use Search Jobs in Microsoft Sentinel
    - Restore archive logs in Microsoft Sentinel
- 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

LAB Outline

- Explore Microsoft Defender XDR
- Deploy Microsoft Defender for Endpoint
- Mitigate Attacks with Microsoft Defender for Endpoint
- Enable Microsoft Defender for Cloud
- Mitigate threats using Microsoft Defender for Cloud
- Create queries for Microsoft Sentinel using Kusto Query Language (KQL)
- Configure your Microsoft Sentinel environment
- Connect data to Microsoft Sentinel using data connectors
- Connect Windows devices to Microsoft Sentinel using data connectors

- Connect Linux hosts to Microsoft Sentinel using data connectors
- Connect Defender XDR to Microsoft Sentinel using data connectors
- Create workbooks
- Use Repositories in Microsoft Sentinel
- Modify a Microsoft Security rule
- Create a Playbook
- Create a Scheduled Query from a template
- Explore Entity Behavior Analytics
- Understand Detection Modeling
- Conduct attacks
- Create Detections
- Investigate Incidents
- Create ASIM parsers
- Perform Threat Hunting in Microsoft Sentinel
- Threat Hunting using Notebooks with Microsoft Sentinel

For any query Contact Us – Microtek Learning