SC-200: Microsoft Security Operations Analyst

Content

Module 1: Introduction to Microsoft 365 Threat Protection

- Understand Microsoft 365 Defender solution by domain
- Understand Microsoft 365 Defender's role in a Modern SOC

Module 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

Module 3: Protect Your Identities with Azure AD Identity Protection

- Describe features of Azure Active Directory Identity Protection
- Investigate and remediate features of Azure Active Directory Identity Protection

Module 4: Remediate Risks with Microsoft Defender for Office 365

- Define capabilities of Microsoft Defender for Office 365
- Simulate attacks within your network
- Remediate risks using Microsoft Defender for Office 365

Module 5: Safeguard Your Environment with Microsoft Defender for Identity

- Define capabilities of Microsoft Defender for Identity
- Configure Microsoft Defender for Identity sensors
- Remediate risks using Microsoft Defender for Identity

Module 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 see activities within your organization
- Use Conditional Access App Control policies to manage access to apps

Module 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

Module 8: Manage Insider Risk in Microsoft Purview

- Explain how Microsoft Purview Insider Risk Management prevents, detects, and contains internal risks
- Describe built-in, pre-defined policy templates
- List prerequisites for creating insider risk policies
- Detail actions in insider risk management cases

Module 9: Investigate Threats Using Audit Features in Microsoft 365 Defender & Microsoft Purview (Standard)

- Differentiate between Audit (Standard) and Audit (Premium)
- Record user and admin activity in the Unified Audit Log (UAL)
- Set up and implement audit log searches

Module 10: Investigate Threats Using Audit in Microsoft 365 Defender & Microsoft Purview (Premium)

- Set up Microsoft Purview Audit (Premium)
- Create audit log retention policies
- Perform forensic investigations of compromised user accounts

Module 11: Investigate Threats Using Content Search in Microsoft Purview

- Use content search in the Microsoft Purview compliance portal
- Design and create content searches
- Preview and export search results and reports

Module 12: Protect Against Threats with Microsoft Defender for Endpoint

- Define the capabilities of Microsoft Defender for Endpoint
- Hunt threats within your network using Microsoft Defender for Endpoint
- Remediate risks using Microsoft Defender for Endpoint

Module 13: Manage Insider Risk in Microsoft Purview

- Use Microsoft Purview Insider Risk Management to prevent, detect, and contain internal risks
- Describe built-in policy templates
- Explain the actions in insider risk management cases

Module 14: 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

Module 15: 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

Module 16: Perform Device Investigations in Microsoft Defender for Endpoint

- Use the device page in Microsoft Defender for Endpoint
- Investigate device forensics collected by Microsoft Defender for Endpoint
- Explain behavioral blocking by Microsoft Defender for Endpoint

Module 17: Perform Actions on a Device Using Microsoft Defender for Endpoint

- Perform actions on a device using Microsoft Defender for Endpoint
- Conduct forensic data collection
- Access devices remotely using Microsoft Defender for Endpoint

Module 18: Perform Evidence and Entities Investigations Using Microsoft Defender for Endpoint

- Investigate files in Microsoft Defender for Endpoint
- Investigate domains and IP addresses
- Investigate user accounts

Module 19: Configure and Manage Automation Using Microsoft Defender for Endpoint

- Configure advanced features in Microsoft Defender for Endpoint
- Manage automation settings

Module 20: Configure for Alerts and Detections in Microsoft Defender for Endpoint

- Configure alert settings
- Manage indicators in Microsoft Defender for Endpoint

Module 21: Utilize Vulnerability Management in Microsoft Defender for Endpoint

- Describe Vulnerability Management features in Microsoft Defender for Endpoint
- Identify vulnerabilities on your devices
- Track emerging threats

Module 22: Plan for Cloud Workload Protections Using Microsoft Defender for Cloud

- Describe Microsoft Defender for Cloud features
- Explain workload protections
- Enable Microsoft Defender for Cloud

Module 23: Connect Azure Assets to Microsoft Defender for Cloud

- Explore Azure assets
- Configure auto-provisioning in Microsoft Defender for Cloud
- Explain manual provisioning

Module 24: Connect Non-Azure Resources to Microsoft Defender for Cloud

- Connect non-Azure machines to Microsoft Defender for Cloud
- Connect AWS and GCP accounts to Microsoft Defender for Cloud

Module 25: Deploy the Microsoft Defender for Endpoint Environment

- Create a Microsoft Defender for Endpoint environment
- Onboard devices
- Configure environment settings

Module 26: Manage Cloud Security Posture Using Microsoft Defender for Cloud

- Describe security posture management
- Explain Microsoft Defender for Cloud protections

Module 27: Explain Cloud Workload Protections in Microsoft Defender for Cloud

- Define which workloads are protected
- Explain the function of workload protections

Module 28: Remediate Security Alerts Using Microsoft Defender for Cloud

- Describe security alerts in Microsoft Defender for Cloud
- Remediate alerts and automate responses

Module 29: Construct KQL Statements for Microsoft Sentinel

- Construct KQL statements for security event searches
- Filter searches based on event time, severity, domain, and other data

Module 30: Analyze Query Results Using KQL

- Summarize data using KQL
- Render visualizations from KQL data

Module 31: Build Multi-Table Statements Using KQL

- Create queries with unions across multiple tables
- Merge tables with the join operator

Module 32: Work with Data in Microsoft Sentinel Using Kusto Query Language (KQL)

- Extract data from structured and unstructured string fields

- Create KQL functions

Module 33: Introduction to Microsoft Sentinel

- Identify the components and functionalities of Microsoft Sentinel
- Understand use cases for Microsoft Sentinel

Module 34: Create and Manage Microsoft Sentinel Workspaces

- Describe Microsoft Sentinel workspace architecture
- Install and manage Microsoft Sentinel workspaces

Module 35: Query Logs in Microsoft Sentinel

- Use the Logs page to view and query data tables

Module 36: Use Watchlists in Microsoft Sentinel

- Create and use watchlists
- Use KQL to access watchlist data

Module 37: Utilize Threat Intelligence in Microsoft Sentinel

- Manage threat indicators
- Use KQL to access threat indicators

Module 38: Connect Data to Microsoft Sentinel Using Data Connectors

- Install Content Hub solutions to provision data connectors
- Explain the use of Common Event Format (CEF) and Syslog connectors

Module 39: Connect Microsoft Services to Microsoft Sentinel

- Connect Microsoft service connectors
- Auto-create incidents using service connectors

Module 40: Connect Microsoft 365 Defender to Microsoft Sentinel

- Activate Microsoft 365 Defender and other connectors in Microsoft Sentinel

Module 41: Connect Windows Hosts to Microsoft Sentinel

- Connect Azure and non-Azure Windows Virtual Machines to Microsoft Sentinel
- Configure Log Analytics agents for Sysmon events

Module 42: Connect Common Event Format Logs to Microsoft Sentinel

- Explain deployment options for CEF connectors
- Run deployment scripts for CEF connectors

Module 43: Connect Syslog Data Sources to Microsoft Sentinel

- Configure Azure Monitor Agent Data Collection Rule (DCR) for Syslog
- Install and configure the Azure Monitor Linux Agent extension

Module 44: Connect Threat Indicators to Microsoft Sentinel

- Configure the TAXII and Threat Intelligence Platform connectors
- View threat indicators in Microsoft Sentinel

Module 45: Threat Detection with Microsoft Sentinel Analytics

- Explain the importance of analytics in Microsoft Sentinel
- Create rules from templates and the analytics rule wizard

Module 46: Automation in Microsoft Sentinel

- Create and manage automation rules

Module 47: Security Incident Management in Microsoft Sentinel

- Learn about security incidents and incident management in Microsoft Sentinel
- Investigate incidents and manage resolution

Module 48: Identify Threats with Behavioral Analytics

- Use User and Entity Behavior Analytics (UEBA) in Microsoft Sentinel
- Explore entities in Microsoft Sentinel

Module 49: Data Normalization in Microsoft Sentinel

- Use ASIM Parsers
- Create parameterized KQL functions

Module 50: Query, Visualize, and Monitor Data in Microsoft Sentinel

- Visualize security data using Microsoft Sentinel Workbooks
- Create a Microsoft Sentinel Workbook

Module 51: Manage Content in Microsoft Sentinel

- Install and manage content hub solutions
- Connect a GitHub repository to Microsoft Sentinel

Module 52: Explain Threat Hunting Concepts in Microsoft Sentinel

- Define threat hunting concepts and develop hypotheses

Module 53: Threat Hunting with Microsoft Sentinel

- Use queries to hunt threats
- Save key findings with bookmarks