Microsoft Security Operations Analyst

Duration: 4 Days

Course Description:

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.

Target Audience:

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.

Course Outline:

Introduction to Microsoft Defender XDR threat protection

- Introduction
- Explore Extended Detection & Response (XDR) response use cases
- Understand Microsoft Defender XDR in a Security Operations Center (SOC)
- Explore Microsoft Security Graph
- Investigate security incidents in Microsoft Defender XDR

Mitigate incidents using Microsoft 365 Defender

- Introduction
- Use the Microsoft Defender portal
- Manage incidents
- Investigate incidents
- Manage and investigate alerts
- Manage automated investigations
- Use the action center
- Explore advanced hunting
- Investigate Microsoft Entra sign-in logs
- Understand Microsoft Secure Score
- Analyze threat analytics
- Analyze reports
- Configure the Microsoft Defender portal
- Enable attack surface reduction rules

Protect your identities with Microsoft Entra ID Protection

- Introduction
- Microsoft Entra ID Protection overview
- Detect risks with Microsoft Entra ID Protection policies
- Investigate and remediate risks detected by Microsoft Entra ID Protection

Remediate risks with Microsoft Defender for Office 365

- Introduction
- Automate, investigate, and remediate
- Configure, protect, and detect
- Simulate attacks

Safeguard your environment with Microsoft Defender for Identity

- Introduction
- Configure Microsoft Defender for Identity sensors
- Review compromised accounts or data
- Integrate with other Microsoft tools

Secure your cloud apps and services with Microsoft Defender for Cloud Apps

- Introduction
- Understand the Defender for Cloud Apps Framework
- Explore your cloud apps with Cloud Discovery
- Protect your data and apps with Conditional Access App Control
- Walk through discovery and access control with Microsoft Defender for Cloud Apps
- Classify and protect sensitive information
- Detect Threats

Respond to data loss prevention alerts using Microsoft 365

- Introduction
- Describe data loss prevention alerts
- Investigate data loss prevention alerts in Microsoft Purview
- Investigate data loss prevention alerts in Microsoft Defender for Cloud Apps

Manage insider risk in Microsoft Purview

- Insider risk management overview
- Introduction to managing insider risk policies
- Create and manage insider risk policies
- Knowledge check
- Investigate insider risk alerts
- Take action on insider risk alerts through cases
- Manage insider risk management forensic evidence
- Create insider risk management notice templates
- Manage remediation

Investigate threats by using audit features in Microsoft Defender XDR and Microsoft Purview Standard

- Introduction to threat investigation with the Unified Audit Log (UAL)
- Explore Microsoft Purview Audit solutions
- Implement Microsoft Purview Audit (Standard)
- Start recording activity in the Unified Audit Log
- Search the Unified Audit Log (UAL)
- Export, configure, and view audit log records
- Use audit log searching to investigate common support issues

Investigate threats using audit in Microsoft Defender XDR and Microsoft Purview (Premium)

- Introduction to threat investigation with Microsoft Purview Audit (Premium)
- Explore Microsoft Purview Audit (Premium)
- Implement Microsoft Purview Audit (Premium)
- Manage audit log retention policies
- 10 min
- Investigate compromised email accounts using Purview Audit (Premium)

Investigate threats with Content search in Microsoft Purview

- Introduction
- Explore Microsoft Purview eDiscovery solutions
- Create a content search
- View the search results and statistics
- Export the search results and search report
- Configure search permissions filtering
- Search for and delete email messages

Protect against threats with Microsoft Defender for Endpoint

- Introduction to Microsoft Defender for Endpoint
- Practice security administration
- Hunt threats within your network

Deploy the Microsoft Defender for Endpoint environment

- Introduction
- Create your environment
- Understand operating systems compatibility and features
- Onboard devices
- Manage access
- Create and manage roles for role-based access control
- Configure device groups
- Configure environment advanced features

COURSE OUTLINE

Perform device investigations in Microsoft Defender for Endpoint

- Introduction
- Examine RBAC and user roles in Microsoft Entra ID
- Create and manage users in Microsoft Entra ID
- Create and manage groups in Microsoft Entra ID
- Manage Microsoft Entra objects with PowerShell

Deploy device data protection

- Introduction
- Use the device inventory list
- Investigate the device
- Use behavioral blocking
- Detect devices with device discovery

Perform actions on a device using Microsoft Defender for Endpoint

- Introduction
- Explain device actions
- Run Microsoft Defender antivirus scan on devices
- Collect investigation package from devices
- Initiate live response session

Perform evidence and entities investigations using Microsoft Defender for Endpoint

- Introduction
- Investigate a file
- Investigate a user account
- Investigate an IP address
- Investigate a domain

Configure and manage automation using Microsoft Defender for Endpoint

- Introduction
- Configure advanced features
- Manage automation upload and folder settings
- Configure automated investigation and remediation capabilities
- Block at risk devices

Configure for alerts and detections in Microsoft Defender for Endpoint

- Introduction
- Configure advanced features
- Configure alert notifications
- Manage alert suppression
- Manage indicators

Utilize Vulnerability Management in Microsoft Defender for Endpoint

- Introduction
- Understand vulnerability management
- Explore vulnerabilities on your devices

Plan for cloud workload protections using Microsoft Defender for Cloud

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

Connect Azure assets to Microsoft Defender for Cloud

- Introduction
- Explore and manage your resources with asset inventory
- Configure auto provisioning
- Manual log analytics agent provisioning

Connect non-Azure resources to Microsoft Defender for Cloud

- Introduction
- Protect non-Azure resources
- Connect non-Azure machines
- Connect your AWS accounts
- Connect your GCP accounts

Manage your cloud security posture management

- Introduction
- Explore Secure Score
- Explore Recommendations
- Measure and enforce regulatory compliance
- Understand Workbooks

Explain cloud workload protections in Microsoft Defender for Cloud

- Introduction
- Understand Microsoft Defender for servers
- Understand Microsoft Defender for App Service
- Understand Microsoft Defender for Storage
- Understand Microsoft Defender for SQL
- Understand Microsoft Defender for open-source databases
- Understand Microsoft Defender for Key Vault
- Understand Microsoft Defender for Resource Manager
- Understand Microsoft Defender for DNS
- Understand Microsoft Defender for Containers
- Understand Microsoft Defender additional protections

Remediate security alerts using Microsoft Defender for Cloud

- Introduction
- Understand security alerts
- Remediate alerts and automate responses
- Suppress alerts from Defender for Cloud
- Generate threat intelligence reports
- Respond to alerts from Azure resources

Connect Common Event Format logs to Microsoft Sentinel

- Introduction
- Plan for Common Event Format connector
- Connect your external solution using the Common Event Format connector

Implement Windows security enhancements with Microsoft Defender for Endpoint

- Introduction
- Understand attack surface reduction

Construct KQL statements for Microsoft Sentinel

- Introduction
- Understand the Kusto Query Language statement structure
- Use the search operator
- Use the where operator
- Use the let statement
- Use the extend operator
- Use the order by operator
- Use the project operators

Analyze query results using KQL

- Introduction
- Use the summarize operator
- Use the summarize operator to filter results
- Use the summarize operator to prepare data
- Use the render operator to create visualizations

Build multi-table statements using KQL

- Introduction
- Use the union operator
- Use the join operator

Work with data in Microsoft Sentinel using Kusto Query Language

- Introduction
- Extract data from unstructured string fields
- Extract data from structured string data
- Integrate external data
- Create parsers with functions

Introduction to Microsoft Sentinel

- Introduction
- What is Microsoft Sentinel?
- How Microsoft Sentinel works
- When to use Microsoft Sentinel

Connect Azure assets to Microsoft Defender for Cloud

- Introduction
- Explore and manage your resources with asset inventory
- Configure auto provisioning
- Manual log analytics agent provisioning

Create and manage Microsoft Sentinel workspaces

- Introduction
- Plan for the Microsoft Sentinel workspace
- Create a Microsoft Sentinel workspace
- Manage workspaces across tenants using Azure Lighthouse
- Understand Microsoft Sentinel permissions and roles
- Manage Microsoft Sentinel settings
- Configure logs
- Understand Microsoft Defender XDR tables

COURSE OUTLINE

Use watchlists in Microsoft Sentinel

- Introduction
- Plan for watchlists
- Create a watchlist
- Manage watchlists

Utilize threat intelligence in Microsoft Sentinel

- Introduction
- Define threat intelligence
- Manage your threat indicators
- View your threat indicators with KQL

Connect data to Microsoft Sentinel using data connectors

- Introduction
- Ingest log data with data connectors
- Understand data connector providers
- View connected hosts

Connect Microsoft services to Microsoft Sentinel

- Introduction
- Plan for Microsoft services connectors
- Connect the Microsoft Office 365 connector
- Connect the Microsoft Entra connector
- Connect the Microsoft Entra ID Protection connector
- Connect the Azure Activity connector

Connect Microsoft Defender XDR to Microsoft Sentinel

- Introduction
- Plan for Microsoft Defender XDR connectors
- Connect the Microsoft Defender XDR connector
- Connect Microsoft Defender for Cloud connector
- Connect Microsoft Defender for IoT
- Connect Microsoft Defender legacy connectors

Connect Windows hosts to Microsoft Sentinel

- Introduction
- Plan for Windows hosts security events connector
- Connect using the Windows Security Events via AMA Connector
- Connect using the Security Events via Legacy Agent Connector
- Collect Sysmon event logs

Connect syslog data sources to Microsoft Sentinel

- Introduction
- Plan for syslog data collection
- Collect data from Linux-based sources using syslog
- Configure the Data Collection Rule for Syslog Data Sources
- Parse syslog data with KQL

Connect threat indicators to Microsoft Sentinel

- Introduction
- Plan for threat intelligence connectors
- Connect the threat intelligence TAXII connector
- Connect the threat intelligence platforms connector
- View your threat indicators with KQL

Threat detection with Microsoft Sentinel analytics

- Introduction
- Exercise - Detect threats with Microsoft Sentinel analytics
- What is Microsoft Sentinel Analytics?
- Types of analytics rules
- Create an analytics rule from templates
- Create an analytics rule from wizard
- Manage analytics rules

Automation in Microsoft Sentinel

- Introduction
- Understand automation options
- Create automation rules

Threat response with Microsoft Sentinel playbooks

- Introduction
- Exercise - Create a Microsoft Sentinel playbook
- What are Microsoft Sentinel playbooks?
- Trigger a playbook in real-time
- Run playbooks on demand

Security incident management in Microsoft Sentinel

- Introduction
- Exercise - Set up the Azure environment
- Understand incidents
- Incident evidence and entities
- Incident management

Identify threats with Behavioral Analytics

- Introduction
- Understand behavioral analytics
- Explore entities

Query logs in Microsoft Sentinel

- Introduction
- Query logs in the logs page
- Understand Microsoft Sentinel tables
- Understand common tables
- Display entity behavior information
- Use Anomaly detection analytical rule templates

Data normalization in Microsoft Sentinel

- Introduction
- Understand data normalization
- Use ASIM Parsers
- Understand parameterized KQL functions
- Create an ASIM Parser
- Configure Azure Monitor Data Collection Rules

Query, visualize, and monitor data in Microsoft Sentinel

- Introduction
- Exercise - Query and visualize data with Microsoft Sentinel Workbooks
- Monitor and visualize data
- Query data using Kusto Query Language
- Use default Microsoft Sentinel Workbooks
- Create a new Microsoft Sentinel Workbook

Manage content in Microsoft Sentinel

- Introduction
- Use solutions from the content hub
- Use repositories for deployment

Explain threat hunting concepts in Microsoft Sentinel

- Introduction
- Understand cybersecurity threat hunts
- Develop a hypothesis
- Explore MITRE ATT&CK

Threat hunting with Microsoft Sentinel

- Introduction
- Exercise setup
- Explore creation and management of threat-hunting queries
- Save key findings with bookmarks
- Observe threats over time with livestream

Use Search jobs in Microsoft Sentinel

- Introduction
- Hunt with a Search Job
- Restore historical data

Hunt for threats using notebooks in Microsoft Sentinel

- Introduction
- Access Azure Sentinel data with external tools
- Hunt with notebooks
- Create a notebook
- Explore notebook code