Data4Every1

Powered by EDUQE EXPERTS IN IT TRAINING

MS-SC200T00: DEFEND AGAINST CYBERTHREATS WITH MICROSOFT'S SECURITY OPERATIONS PLATFORM

DURATION	LEVEL	TECHNOLOGY	DELIVERY METHOD	CERTIFICATION
4 Days	Intermediate	Security	Instructor-led	SC-200 Exam

INTRODUCTION

Learn how to investigate, respond to, and hunt for threats using Microsoft Sentinel, Microsoft Defender XDR and Microsoft Defender for Cloud. 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.

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 XDR, Microsoft Defender for Cloud, 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.

PREREQUISITES

Before attending this course, delegates must have:

- Basic understanding of Microsoft security concepts and technologies
- Experience with Microsoft security tools
- Understanding of security operations and incident response
- Ability to analyse security logs, alerts, and telemetry
- Familiarity with threat detection and threat hunting concepts
- General understanding of Microsoft 365 and Azure environments

COURSE OBJECTIVES

After completing this course, students will be able to:

- Mitigate threats using Microsoft Defender for Cloud
- Mitigate threats using Microsoft Sentinel
- Manage a security operations environment
- Perform threat detection, investigation, and incident response
- Conduct proactive threat hunting

COURSE CONTENT

Module 1: Mitigate threats using Microsoft Defender XDR

Analyse threat data across domains and rapidly remediate threats with built-in orchestration and automation in Microsoft Defender XDR. This learning path aligns with exam SC-200: Microsoft Security Operations Analyst.

Module 1.1: Introduction to Microsoft Defender XDR threat protection

In this module, you'll learn how to use the Microsoft Defender XDR integrated threat protection suite.

Module 1.2: Mitigate incidents using Microsoft Defender

Learn how the Microsoft Defender portal provides a unified view of incidents from the Microsoft Defender family of products.

Module 1.3: Remediate risks with Microsoft Defender for Office 365

Learn about the Microsoft Defender for Office 365 component of Microsoft Defender XDR.

Module 1.4: Manage Microsoft Entra Identity Protection

Protecting a user's identity by monitoring their usage and sign-in patterns ensure a secure cloud solution. Explore how to design and implement Microsoft Entra Identity protection.

Data4Every1

Powered by EDUQE EXPERTS IN IT TRAINING

Module 1.5: Safeguard your environment with Microsoft Defender for Identity

Learn about the Microsoft Defender for Identity component of Microsoft Defender XDR.

Module 1.6: Secure your cloud apps and services with Microsoft Defender for Cloud Apps

Microsoft Defender for Cloud Apps is a cloud access security broker (CASB) that operates on multiple clouds. It provides rich visibility, control over data travel, and sophisticated analytics to identify and combat cyberthreats across all your cloud services. Learn how to use Defender for Cloud Apps in your organization.

Module 2: Mitigate threats using Microsoft Security Copilot

Get started with Microsoft Security Copilot. You're introduced to basic terminology, how Microsoft Security Copilot processes prompts, the elements of an effective prompt, and how to enable the solution. This learning path aligns with exam SC-200: Microsoft Security Operations Analyst.

Module 2.1: Introduction to generative AI and agents

Generative AI powers applications that can create content, answer questions, and assist with tasks. In this module, you'll explore the fundamentals of generative AI, including large language models (LLMs), prompts, and AI agents.

Module 2.2: Describe Microsoft Security Copilot

Get acquainted with Microsoft Security Copilot. You're introduced to some basic terminology, how Microsoft Security Copilot processes prompts, the elements of an effective prompt, and how to enable the solution.

Module 2.3: Describe the core features of Microsoft Security Copilot

Microsoft Security Copilot has a rich set of features. Learn about available plugins, promptbooks, the ways you can export and share information from Copilot, and much more.

Module 2.4: Describe the embedded experiences of Microsoft Security Copilot

Microsoft Security Copilot is accessible directly from some Microsoft security products. This is referred to as the embedded experience. Learn about the scenarios supported by the Copilot embedded experience in Microsoft's security solutions.

Module 2.5: Explore use cases of Microsoft Security Copilot

Explore use cases of Microsoft Security Copilot in the standalone and embedded experiences, through lab-like exercises.

Module 3: Mitigate threats using Microsoft Purview

In this Learning Path we focus on Microsoft Purview's risk and compliance solutions that assist security operations analysts detect threats to organizations and identify, classify, and protect sensitive data, as well as monitor and report on compliance. This learning path aligns with exam SC-200: Microsoft Security Operations Analyst.

Module 3.1: Investigate and respond to Microsoft Purview Data Loss Prevention alerts

Microsoft Purview and Microsoft Defender XDR help organizations detect potential data loss risks and respond quickly to protect sensitive information. Investigation and response activities include reviewing DLP alerts, applying appropriate remediation actions, and documenting findings in a structured and consistent way.

Module 3.2: Investigate insider risk alerts and related activity

Investigate insider risk alerts and manage related cases in Microsoft Purview to assess user behavior, take appropriate action, and coordinate deeper reviews across teams.

Module 3.3: Search and investigate with Microsoft Purview Audit

Enhance data security and compliance with Microsoft Purview Audit by configuring detailed audits, managing logs, and analyzing access patterns.

Module 3.4: Search for content with Microsoft Purview eDiscovery

Use Microsoft Purview eDiscovery to search for content across Microsoft 365. This module covers how to configure cases, define search criteria, and locate messages, files, and other organizational data.

Module 4: Mitigate threats using Microsoft Defender for Endpoint

Implement the Microsoft Defender for Endpoint platform to detect, investigate, and respond to advanced threats. This learning path aligns with exam SC-200: Microsoft Security Operations Analyst.

Module 4.1: Protect against threats with Microsoft Defender for Endpoint

Learn how Microsoft Defender for Endpoint can help your organization stay secure.

Module 4.2: Deploy the Microsoft Defender for Endpoint environment

Learn how to deploy the Microsoft Defender for Endpoint environment, including onboarding devices and configuring security.

Data4Every1

Powered by EDUQE EXPERTS IN IT TRAINING

Module 4.3: Implement Windows security enhancements with Microsoft Defender for Endpoint
Microsoft Defender for Endpoint gives you various tools to eliminate risks by reducing the surface area for attacks without blocking user productivity. Learn about Attack Surface Reduction (ASR) with Microsoft Defender for Endpoint.

Module 4.4: Perform device investigations in Microsoft Defender for Endpoint
Microsoft Defender for Endpoint provides detailed device information, including forensics information. Learn about information available to you through Microsoft Defender for Endpoint that aids in your investigations.

Module 4.5: Perform actions on a device using Microsoft Defender for Endpoint
Learn how Microsoft Defender for Endpoint provides the remote capability to contain devices and collect forensics data.

Module 4.6: Perform evidence and entities investigations using Microsoft Defender for Endpoint
Learn about the artifacts in your environment and how they relate to other artifacts and alerts that provide you with insight to understand the overall impact to your environment.

Module 4.7: Configure and manage automation using Microsoft Defender for Endpoint
Learn how to configure automation in Microsoft Defender for Endpoint by managing environmental settings.

Module 4.8: Configure for alerts and detections in Microsoft Defender for Endpoint
Learn how to configure settings to manage alerts and notifications. You'll also learn to enable indicators as part of the detection process.

Module 4.9: Utilize Vulnerability Management in Microsoft Defender for Endpoint
Learn about your environment's weaknesses by using Vulnerability Management in Microsoft Defender for Endpoint.

Module 5: Mitigate threats using Microsoft Defender for Cloud

Use Microsoft Defender for Cloud, for Azure, hybrid cloud, and on-premises workload protection and security.

Module 5.1: Plan for cloud workload protections using Microsoft Defender for Cloud
Learn the purpose of Microsoft Defender for Cloud and how to enable the system.

Module 5.2: Connect Azure assets to Microsoft Defender for Cloud
Learn how to connect your various Azure assets to Microsoft Defender for Cloud to detect threats.

Module 5.3: Connect non-Azure resources to Microsoft Defender for Cloud
Learn how you can add Microsoft Defender for Cloud capabilities to your hybrid environment.

Module 5.4: Manage your cloud security posture management
Microsoft Defender for Cloud, Cloud Security Posture Management (CSPM) provides visibility into vulnerable resources and provides hardening guidance.

Module 5.5: Explain cloud workload protections in Microsoft Defender for Cloud
Learn about the protections and detections provided by Microsoft Defender for Cloud with each cloud workload.

Module 5.6: Remediate security alerts using Microsoft Defender for Cloud
Learn how to remediate security alerts in Microsoft Defender for Cloud.

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

Write Kusto Query Language (KQL) statements to query log data to perform detections, analysis, and reporting in Microsoft Sentinel. This learning path will focus on the most used operators. The example KQL statements will showcase security related table queries.

Module 6.1: Construct KQL statements for Microsoft Sentinel
Kusto Query Language (KQL) is the query language used to perform analysis on data to create analytics, workbooks, and perform hunting in Microsoft Sentinel. Learn how basic KQL statement structure provides the foundation to build more complex statements.

Module 6.2: Analyze query results using KQL
Learn how to summarize and visualize data with a KQL statement provides the foundation to build detections in Microsoft Sentinel.

Module 6.3: Build multi-table statements using KQL
Learn how to work with multiple tables using KQL.

Module 6.4: Work with data in Microsoft Sentinel using Kusto Query Language
Learn how to use the Kusto Query Language (KQL) to manipulate string data ingested from log sources.

Data4Every1

Powered by EDUQE EXPERTS IN IT TRAINING

Module 7: Configure your Microsoft Sentinel environment

Get started with Microsoft Sentinel by properly configuring the Microsoft Sentinel workspace.

Module 7.1: Introduction to Microsoft Sentinel

Traditional security information and event management (SIEM) systems typically take a long time to set up and configure. They're also not necessarily designed with cloud workloads in mind. Microsoft Sentinel enables you to start getting valuable security insights from your cloud and on-premises data quickly. This module helps you get started.

Module 7.2: Create and manage Microsoft Sentinel workspaces

Learn about the architecture of Microsoft Sentinel workspaces to ensure you configure your system to meet your organization's security operations requirements.

Module 7.3: Query logs in Microsoft Sentinel

As a Security Operations Analyst, you must understand the tables, fields, and data ingested in your workspace. Learn how to query the most used data tables in Microsoft Sentinel.

Module 7.4: Use watchlists in Microsoft Sentinel

Learn how to create Microsoft Sentinel watchlists that are a named list of imported data. Once created, you can easily use the named watchlist in KQL queries.

Module 7.5: Utilize threat intelligence in Microsoft Sentinel

Learn how the Microsoft Sentinel Threat Intelligence page enables you to manage threat indicators.

Module 7.6: Integrate Microsoft Defender XDR with Microsoft Sentinel

In this module, you learn how the Microsoft Defender portal integrates Microsoft Defender XDR with Microsoft Sentinel.

Module 8: Connect logs to Microsoft Sentinel

Connect data at cloud scale across all users, devices, applications, and infrastructure, both on-premises and in multiple clouds to Microsoft Sentinel.

Module 8.1: Connect data to Microsoft Sentinel using data connectors

The primary approach to connect log data is using the Microsoft Sentinel provided data connectors. This module provides an overview of the available data connectors.

Module 8.2: Connect Microsoft services to Microsoft Sentinel

Learn how to connect Microsoft 365 and Azure service logs to Microsoft Sentinel.

Module 8.3: Connect Microsoft Defender XDR to Microsoft Sentinel

Learn about the configuration options and data provided by Microsoft Sentinel connectors for Microsoft Defender XDR.

Module 8.4: Connect Windows hosts to Microsoft Sentinel

Two of the most common logs to collect are Windows security events and Sysmon. Learn how Microsoft Sentinel makes this easy with the Microsoft Windows Events data connectors.

Module 8.5: Connect Common Event Format logs to Microsoft Sentinel

Most vendor-provided connectors utilize the CEF connector. Learn about the Common Event Format (CEF) connector's configuration options.

Module 8.6: Connect syslog data sources to Microsoft Sentinel

Learn about the Azure Monitor Agent Linux Syslog Data Collection Rule configuration options, which enable you to parse Syslog data.

Module 8.7: Connect threat indicators to Microsoft Sentinel

Learn how to connect Threat Intelligence Indicators to the Microsoft Sentinel workspace using the provided data connectors.

Module 9: Create detections and perform investigations using Microsoft Sentinel

Detect previously uncovered threats and rapidly remediate threats with built-in orchestration and automation in Microsoft Sentinel.

Module 9.1: Threat detection with Microsoft Sentinel analytics

In this module, you learned how Microsoft Sentinel Analytics can help the SecOps team identify and stop cyber-attacks.

Module 9.2: Automation in Microsoft Sentinel

By the end of this module, you're able to use automation rules in Microsoft Sentinel to automated incident management.

Module 9.3: Threat response with Microsoft Sentinel playbooks

Module 9.4: Security incident management in Microsoft Sentinel

This module describes how to create Microsoft Sentinel playbooks to respond to security threats.

Learn about security incidents, incident evidence and entities, incident management, and how to use Microsoft Sentinel to handle incidents.

Module 9.5: Identify threats with Behavioural Analytics
Learn how to use entity behavior analytics in Microsoft Sentinel to identify threats inside your organization.

Module 9.6: Data normalization in Microsoft Sentinel
By the end of this module, you're able to use Advanced Security Information Model (ASIM) parsers to identify threats inside your organization.

Module 9.7: Query, visualize, and monitor data in Microsoft Sentinel
This module describes how to query, visualize, and monitor data in Microsoft Sentinel.

Module 9.8: Manage content in Microsoft Sentinel
By the end of this module, you're able to manage content in Microsoft Sentinel.

Module 10: Perform threat hunting in Microsoft Sentinel

Proactively hunt for security threats using the Microsoft Sentinel powerful threat hunting tools.

Module 10.1: Explain threat hunting concepts in Microsoft Sentinel
Learn the threat hunting process in Microsoft Sentinel.

Module 10.2: Threat hunting with Microsoft Sentinel
In this module, you'll learn to proactively identify threat behaviors by using Microsoft Sentinel queries. You'll also learn to use bookmarks and livestream to hunt threats.

Module 10.3: Use Search jobs in Microsoft Sentinel
In Microsoft Sentinel, you can search across long time periods in large datasets by using a search job.

Module 10.4: Hunt for threats using notebooks in Microsoft Sentinel
Learn how to use notebooks in Microsoft Sentinel for advanced hunting.

ASSOCIATED CERTIFICATIONS & EXAM

This course will prepare delegates to write the SC-200 Microsoft Certified: Security Operations Analyst Associate Exam.