Defend against cyberthreats with Microsoft's security operations platform (SC-200T00)

Duration: 4 days
Audience: Professionnel TI

Who is this training for?

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.

Training objectives

By the end of this

course, students will be able to:

- Investigate, analyse, and respond to cyberthreats using Microsoft Sentinel, Microsoft Defender XDR, and Microsoft Defender for Cloud.
- Detect and mitigate security incidents across identities, endpoints, cloud apps, and Microsoft 365 services.
- Strengthen identity protection using Entra ID Protection and Microsoft Defender for Identity.
- Remediate risks and protect data with Microsoft Defender for Office 365 and Microsoft Purview solutions.
- Build and interpret Kusto Query Language (KQL) queries to detect, analyse, and report on security events.
- Configure and manage Microsoft Sentinel workspaces, watchlists, threat intelligence, and integrations with Defender XDR.

- Connect and ingest logs from Microsoft services, Windows hosts, CEF sources, syslog systems, and threat indicators.
- Create analytics rules, automate responses, and manage security incidents within Microsoft Sentinel.
- Perform proactive threat hunting using search jobs, notebooks, and behavioural analytics.
- Deploy, configure, and manage Microsoft Defender for Endpoint, including investigations, automation, alerts, and vulnerability management.

Summary

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.

Course outline

Learning Path 1: Mitigate threats using Microsoft Defender XDR

- Module 1: Introduction to Microsoft 365 threat protection
- Module 2: Mitigate incidents using Microsoft Defender XDR
- Module 3: Protect your identities with Entra ID Protection
- Module 4: Remediate risks with Microsoft Defender for Office 365
- Module 5: Safeguard your environment with Microsoft Defender for Identity
- Module 6: Secure your cloud apps and services with Microsoft Defender for Cloud Apps

Learning Path 2: Get started with Microsoft Copilot for Security

- Module 1: Fundamentals of Generative AI
- Module 2: Describe Microsoft Copilot for Security

- Module 3: Describe the core features of Microsoft Copilot for Security
- Module 4: Describe the embedded experiences of Microsoft Copilot for Security

Learning Path 3: Mitigate threats using Microsoft Purview

- Module 1: Microsoft Purview Compliance Solutions
- Module 2: Respond to data loss prevention alerts using Microsoft Purview
- Module 3: Manage insider risk in Microsoft Purview
- Module 4: Investigate threats using Content Search in Microsoft Purview
- Module 5: Investigate threats using Microsoft Purview Audit

Learning Path 4:

Mitigate threats using Microsoft

Defender for Endpoint

- Module 1: Protect against threats with Microsoft Defender for Endpoint
- Module 2: Deploy the Microsoft Defender for Endpoint environment
- Module 3: Implement Windows security enhancements with Microsoft Defender for Endpoint
- Module 4: Perform device investigations in Microsoft Defender for Endpoint
- Module 5: Perform actions on a device using Microsoft Defender for Endpoint
- Module 6: Perform evidence and entities investigations using Microsoft Defender for Endpoint
- Module 7: Configure and manage automation using Microsoft Defender for Endpoint
- Module 8: Configure alerts and detections in Microsoft Defender for Endpoint
- Module 9: Utilize Vulnerability Management in Microsoft Defender for Endpoint

Learning Path 5: Create queries for Microsoft Sentinel using Kusto Query Language (KQL)

- Module 1: Construct KQL statements for Microsoft Sentinel
- Module 2: Analyze query results using KQL
- Module 3: Build multi table statements using KQL
- Module 4: Work with data in Microsoft Sentinel using Kusto Query Language

Learning Path 6: Configure your Microsoft Sentinel environment

- Module 1: Introduction to Microsoft Sentinel
- Module 2: Create and manage Microsoft Sentinel workspaces
- Module 3: Query logs in Microsoft Sentinel
- Module 4: Use watchlists in Microsoft Sentinel
- Module 5: Utilize threat intelligence in Microsoft Sentinel
- Module 6: Integrate Microsoft Defender XDR with Microsoft Sentinel

Learning Path 7: Connect logs to Microsoft Sentinel

- Module 1: Connect data to Microsoft Sentinel using data connectors
- Module 2: Connect Microsoft services to Microsoft Sentinel
- Module 3: Connect Microsoft Defender XDR to Microsoft Sentinel
- Module 4: Connect Windows hosts to Microsoft Sentinel
- Module 5: Connect Common Event Format logs to Microsoft Sentinel
- Module 6: Connect syslog data sources to Microsoft Sentinel
- Module 7: Connect threat indicators to Microsoft Sentinel

Learning Path 8: Create detections and perform investigations using Microsoft Sentinel

- Module 1: Threat detection with Microsoft Sentinel analytics
- Module 2: Automation in Microsoft Sentinel
- Module 3: Threat response with Microsoft Sentinel playbooks
- Module 4: Security incident management in Microsoft Sentinel
- Module 5: Identify threats with Entity Behavioral Analytics in Microsoft Sentinel
- Module 6: Data normalization in Microsoft Sentinel
- Module 7: Query, visualize, and monitor data in Microsoft Sentinel
- Module 8: Manage content in Microsoft Sentinel

Learning Path 9: Perform threat hunting in Microsoft Sentinel

-

Module 1: Explain threat hunting concepts in Microsoft Sentinel

- Module 2: Threat hunting with Microsoft Sentinel
- Module 3: Use Search jobs in Microsoft Sentinel
- Module 4: Hunt for threats using notebooks in Microsoft Sentinel

Approach and methodology

Practical and structured approach combining focused theory and guided workshops. Participants gradually set up and leverage security operations as a SOC analyst with Microsoft Sentinel through real-world exercises inspired by business scenarios, promoting immediate application of learnings.

They learn how to detect, analyze, and respond to security incidents using Microsoft protection and monitoring tools.

Led by a Microsoft Certified Trainer (MCT), the training emphasizes interactivity and the development of directly transferable technical skills to ensure surveillance and response to threats in a professional context.

Prerequisites

Students should have the following knowledge and experience before attending this course:

- Basic understanding of Microsoft 365
- Fundamental understanding of Microsoft security, compliance, and identity products
- Intermediate understanding of Microsoft Windows
- Familiarity with Azure services, specifically Azure SQL Database and Azure Storage
- Familiarity with Azure virtual machines and virtual networking
- Basic understanding of scripting concepts.

Recommendations

Optional Prerequisites:

- General understanding of security and threat management concepts
- Familiarity with Microsoft security tools (Sentinel, Defender XDR, Defender for Cloud)
- Basic knowledge of Kusto Query Language (KQL)
- Awareness of data governance and compliance principles
- Prior experience in security operations (SOC)
- Understanding of organizational risk and remediation practices
- Familiarity with Microsoft 365 and Azure environments

Certifications

Microsoft Certified: Security Operations Analyst Associate

Legal notices