Microsoft Security Operations Analyst (SC-200T00)

Duration: 4 days
Audience: Professionnel TI

Who is this training for?

Microsoft's Security Operations Analyst collaborates with stakeholders across the organization to secure the organization's information technology systems. Its goal is to reduce organizational risk by quickly remediating active attacks in the environment, advising on improvements to threat protection practices, and reporting violations of organizational policies to appropriate stakeholders. Responsibilities include managing, monitoring, and responding to threats using a variety of security solutions in their environment. The role is primarily to investigate, respond to, and hunt threats using Microsoft Azure Sentinel, Azure Defender, Microsoft 365 Defender, and third-party security products. Since the security operations analyst consumes the operational output of these tools, he is also a critical stakeholder in the configuration and deployment of these technologies.

Training objectives

- Explain how Microsoft Defender for Endpoint can remediate risks in your environment.
- Create a Microsoft Defender for Endpoint environment.
- Configure attack surface reduction rules on Windows 10 devices.
- Perform actions on a device using Microsoft Defender for Endpoint
- Investigate domains and IP addresses in Microsoft Defender for Endpoint
- Investigate user accounts in Microsoft Defender for Endpoint
- Configure alert settings in Microsoft Defender for Endpoint
- Explain how the threat landscape is evolving
- Conduct advanced hunting in Microsoft 365 Defender
- Manage incidents in Microsoft 365 Defender
- Explain how Microsoft Defender for Identity can remediate risks in your environment
- Investigate DLP alerts in Microsoft Cloud App Security
- Explain the types of actions you can take on an insider risk management case
-

Configure auto-provisioning in Azure Defender

- Remediate alerts in Azure DefenderConstruct KQL statements
- Filter searches based on event time, severity, domain, and other relevant data using KQL
- Extract data from unstructured string fields using KQL
- Manage an Azure Sentinel workspace
- Use KQL to access the watchlist in Azure Sentinel
- Manage threat indicators in Azure Sentinel
- Explain the Common Event Format and Syslog connector differences in Azure Sentinel
- Connect Azure Windows Virtual Machines to Azure Sentinel
- Configure Log Analytics agent to collect Sysmon events
- Create new analytics rules and queries using the analytics rule wizard
- Create a playbook to automate an incident response
- Use queries to hunt for threats
- Observe threats over time with livestream

Summary

Learn how to investigate, respond, and hunt for threats using Microsoft Sentinel, Microsoft Defender XDR, and Microsoft Defender for Cloud. In this course, you will learn how to mitigate cyber threats using these technologies. Specifically, you'll set up and use Microsoft Sentinel, as well as leverage the Kusto query language (KQL) to perform detections, analysis, and reporting. This course is designed for professionals working in a security operations related role and helps learners prepare for the SC-200: Microsoft Security Operations Analyst exam.

Course outline

Learning Path 1: Reduce threats with Microsoft Defender XDR

- Introduction to threat protection in Microsoft 365
- Reduce incidents using Microsoft Defender XDR
- Protect identities with Microsoft Entra ID Protection

- Remediate risk with Microsoft Defender for Office 365
- Protect the environment with Microsoft Defender for Identity
- Secure cloud apps and services with Microsoft Defender for Cloud Apps

Learning Path 2 : Get started with Microsoft Copilot for Security

- Generative AI Fundamentals
- Describe Microsoft Copilot for Security
- Describe the core features of Microsoft Copilot for Security
- Describe Microsoft Copilot for Security built-in experiences

Learning Path 3 : Reduce threats with Microsoft Purview

- Microsoft Purview compliance solutions
- Respond to data loss prevention alerts using Microsoft Purview
- Manage insider risks with Microsoft Purview
- Investigate Threat research using Content Search in Microsoft Purview
- Investigate threats using Microsoft Purview auditing

Learning Path 4 : Reduce threats with Microsoft Defender for Endpoint

- Protect against threats with Microsoft Defender for Endpoint
- Deploy Microsoft Defender for Endpoint environment
- Implement Windows security enhancements with Microsoft Defender for Endpoint
- Perform device investigations in Microsoft Defender for Endpoint
- Perform actions on a device with Microsoft Defender for Endpoint
- Investigate evidence and entities in Microsoft Defender for Endpoint
- Set up and manage automation with Microsoft Defender for Endpoint
- Configure alerts and detections in Microsoft Defender for Endpoint
- Use vulnerability management in Microsoft Defender for Endpoint

Learning Path 5 : Reduce threats with Microsoft Defender for Cloud

- Plan for load protection Cloud work with Microsoft Defender for Cloud
- Connect Azure resources to Microsoft Defender for Cloud
- Connect non-Azure resources to Microsoft Defender for Cloud
- Manage cloud security posture
- Explain cloud workload protection in Microsoft Defender for Cloud
- Remediate security alerts with Microsoft Defender for Cloud

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

- Build KQL statements for Microsoft Sentinel
- Analyze query results using KQL
- Create multi-table statements with KQL
- Work with data in Microsoft Sentinel using Kusto Query Language

Learning Path 7 : Set up your Microsoft Sentinel environment

- Introduction to Microsoft Sentinel
- Create and manage Microsoft Sentinel workspaces
- Query logs in Microsoft Sentinel
- Use watchlists in Microsoft Sentinel
- Work with threat intelligence in Microsoft Sentinel
- Integrate Microsoft Defender XDR with Microsoft Sentinel

Learning Path 8 : Connect logs to Microsoft Sentinel

- Connect data to Microsoft Sentinel using data connectors
- Connect Microsoft services to Microsoft Sentinel
- Connect Microsoft Defender XDR to Microsoft Sentinel
- Connect Windows hosts to Microsoft Sentinel
- Connect logs in Common Event Format to Microsoft Sentinel
- Connect syslog data sources to Microsoft Sentinel
-

Connect threat indicators to Microsoft Sentinel

Learning Path 9 : Create detections and perform investigations using Microsoft Sentinel

- Detect threats with Microsoft Sentinel analytics
- Automate in Microsoft Sentinel
- Respond to threats with Microsoft Sentinel playbooks
- Manage security incidents in Microsoft Sentinel
- Identify threats with behavioral entity analysis in Microsoft Sentinel
- Normalizing data in Microsoft Sentinel
- Querying, visualizing, and monitoring data in Microsoft Sentinel
- Managing content in Microsoft Sentinel

Learning Path 10 : Performing threat searches in Microsoft Sentinel

- Explaining threat research concepts in Microsoft Sentinel
- Threat research with Microsoft Sentinel
- Using search tasks in Microsoft Sentinel
- Finding 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, the training emphasizes interactivity and the development of directly transferable technical skills to ensure surveillance and response to threats in a professional context.

Prerequisites

- Basic knowledge of security, compliance, and Microsoft identity Familiarity with Microsoft 365 and Azure services
- General understanding of cybersecurity concepts (detection, incident response)

Recommendations

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