Microsoft Security Operations Analyst – Intensive Training («SC200»)

Learn how to investigate, respond to, and hunt for threats using Microsoft Azure Sentinel, Azure Defender, and Microsoft 365 Defender.

Duration: 4 days
Price: 3'400.–
Course documents: Official Microsoft Courseware and Microsoft Learn
Vendor code: SC-200

Content

In this course you will learn how to mitigate cyberthreats using these technologies. Specifically, you will configure and use Azure 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 modules:

Introduction to Microsoft 365 threat protection

- In this module, you'll learn how to use the Microsoft 365 Defender integrated threat protection suite.

Mitigate incidents using Microsoft 365 Defender

- Learn how the Microsoft 365 Defender portal provides a unified view of incidents from the Microsoft 365 Defender family of products.

Protect your identities with Azure AD Identity Protection

- Use the advanced detection and remediation of identity-based threats to protect your Azure Active Directory identities and applications from compromise.

Remediate risks with Microsoft Defender for Office 365

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

Safeguard your environment with Microsoft Defender for Identity

- Learn about the Microsoft Defender for Identity component of Microsoft 365 Defender.

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.

Respond to data loss prevention alerts using Microsoft 365

- As a Security Operations Analyst, you need to understand compliance related terminology and alerts. Learn how the data loss prevention alerts will help in your investigation to find the full scope of the incident.

Manage insider risk in Microsoft Purview

- Microsoft Purview Insider Risk Management helps organizations address internal risks, such as IP theft, fraud, and sabotage. Learn about insider risk management and how Microsoft technologies can help you detect, investigate, and take action on risky activities in your organization.

Investigate threats by using audit features in Microsoft 365 Defender and Microsoft Purview Standard

- This module examines how to search for audited activities using the Microsoft Purview Audit (UAL) solution, including how to export, configure, and view the audit log records that were retrieved from an audit log search.

Investigate threats using audit in Microsoft 365 Defender and Microsoft Purview (Premium)

- This module explores the differences between Microsoft Purview Audit (Standard) and Audit (Premium), plus the key functionality in Audit (Premium), including setup requirements, enabling audit logging, creating audit log retention policies, and performing forensics investigations.

Investigate threats with Content search in Microsoft Purview

- This module examines how to search for content in the Microsoft Purview compliance portal using Content Search functionality, including how to view and export the search results, and configure search permissions filtering.

Protect against threats with Microsoft Defender for Endpoint

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

Deploy the Microsoft Defender for Endpoint environment

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

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.

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 will aid in your investigations.

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.

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 will provide you with insight to understand the overall impact to your environment.

Configure and manage automation using Microsoft Defender for Endpoint

- Learn how to configure automation in Microsoft Defender for Endpoint by managing environmental settings.

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.

Utilize Vulnerability Management in Microsoft Defender for Endpoint

- Learn about your environment's weaknesses by using Vulnerability Management in Microsoft Defender for Endpoint.

Plan for cloud workload protections using Microsoft Defender for Cloud

- Learn the purpose of Microsoft Defender for Cloud and how to enable the system.

Connect Azure assets to Microsoft Defender for Cloud

- Learn how to connect your various Azure assets to Microsoft Defender for Cloud to detect threats.

Connect non-Azure resources to Microsoft Defender for Cloud

- Learn how you can add Microsoft Defender for Cloud capabilities to your hybrid environment.

Manage your cloud security posture management

- Microsoft Defender for Cloud, Cloud Security Posture Management (CSPM) provides visibility into vulnerable resources and provides hardening guidance.

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.

Remediate security alerts using Microsoft Defender for Cloud

- Learn how to remediate security alerts in Microsoft Defender for Cloud.

Construct KQL statements for Microsoft Sentinel

- 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.

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.

Build multi-table statements using KQL

- Learn how to work with multiple tables using KQL.

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.

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.

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.

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.

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.

Utilize threat intelligence in Microsoft Sentinel

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

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.

Connect Microsoft services to Microsoft Sentinel

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

Connect Microsoft 365 Defender to Microsoft Sentinel

- Learn about the configuration options and data provided by Microsoft Sentinel connectors for Microsoft 365 Defender.

Connect Windows hosts to Microsoft Sentinel

- One of the most common logs to collect is Windows security events. Learn how Microsoft Sentinel makes this easy with the Security Events connector.

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.

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.

Connect threat indicators to Microsoft Sentinel

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

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.

Automation in Microsoft Sentinel

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

Security incident management in Microsoft Sentinel

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

Identify threats with Behavioral Analytics

- Learn how to use entity behavior analytics in Microsoft Sentinel to identify threats inside your organization.

Data normalization in Microsoft Sentinel

- By the end of this module, you'll be able to use ASIM parsers to identify threats inside your organization.

Query, visualize, and monitor data in Microsoft Sentinel

- This module describes how to query, visualize, and monitor data in Microsoft Sentinel.

Manage content in Microsoft Sentinel

- By the end of this module, you'll be able to manage content in Microsoft Sentinel.

Explain threat hunting concepts in Microsoft Sentinel

- Learn the threat hunting process in Microsoft Sentinel.

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.

Use Search jobs in Microsoft Sentinel

- In Microsoft Sentinel, you can search across long time periods in large datasets by using a search job.

Hunt for threats using notebooks in Microsoft Sentinel

- Learn how to use notebooks in Microsoft Sentinel for advanced hunting.

Key Learnings

- Mitigating threats using Microsoft 365 Defender
- Mitigating threats using Azure Defender for Cloud
- Mitigating threats using Azure Sentinel

Methodology & didactics

Digicomp Flexible Learning Approach:

- **Training modality:** During a period of 4 weeks, 6-8 half-day (3h each) virtual live sessions with our Azure MCT experts will take place. The sessions are already planned and can be easily combined with the daily work routine. Between the sessions there is enough time to process the learned knowledge.
- **Detailed Session Plan:** Click «**Timetable**» at the bottom of the page where you select your desired date.

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 Azure Sentinel, Azure Defender, 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.

Requirements

- Basic understanding of Microsoft 365
- Fundamental understanding of Microsoft security, compliance, and identity products
- Intermediate understanding of Windows 10
- Familiarity with Azure services, specifically Azure SQL Database and Azure Storage
- Familiarity with Azure virtual machines and virtual networking
- Basic understanding of scripting concepts

Basic knowledge gained in the following course is recommended:

- Microsoft Security, Compliance, and Identity Fundamentals – Intensive Training («SC900»)
- Microsoft Security, Compliance, and Identity Fundamentals – Flexible Training («SC900V»)

Certification

This intensive training prepares you for:

- **Exam:** «SC-200: Microsoft Security Operations Analyst» for the
- **Certification:** «Microsoft Certified: Security Operations Analyst Associate»

Additional information

We recommend SC-5001: Configure SIEM Security Operations Using Microsoft Sentinel as self-study preparation for this course.

Further courses

- Microsoft Cybersecurity Architect – Intensive Training («SC100»)

Any questions?

We are happy to advise you on +41 44 447 21 21 or info@digicomp.ch. You can find detailed information about dates on www.digicomp.ch/courses-microsoft-technology/microsoft-security-compliance-and-identity/microsoft-certified-security-operations-analyst-associate/course-microsoft-security-operations-analyst-intensive-training-sc-200