SC-200: Microsoft Security Operations Analyst

Microsoft - Security

Live Training (também disponível em presencial)

- **Localidade:** Porto
- **Data:** 23 Oct 2023
- **Preço:** 1590 € (Os valores apresentados não incluem IVA. Oferta de IVA a particulares e estudantes.)
- **Horário:** Laboral das 09h00 - 17h00
- **Nível:** Intermédio
- **Duração:** 28h

Sobre o curso

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

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.

Destinatários

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.

Objetivos

- Analyze threat data across domains and rapidly remediate threats with built-in orchestration and automation in Microsoft 365 Defender
- Implement the Microsoft Defender for Endpoint platform to detect, investigate, and respond to advanced threats
- Use Microsoft Defender for Cloud, for Azure, hybrid cloud, and on-premises workload protection and security
- Write Kusto Query Language (KQL) statements to query log data to perform detections, analysis, and reporting in Microsoft Sentinel
- Confiure Microsoft Sentinel workspace
- Connect data at cloud scale across all users, devices, applications, and infrastructure, both on-premises and in multiple clouds to Microsoft Sentinel
- Detect previously uncovered threats and rapidly remediate threats with built-in orchestration and automation in Microsoft Sentinel
- Proactively hunt for security threats using the Microsoft Sentinel powerful threat hunting tools

Pré-requisitos

- 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.

Programa

- Introduction to Microsoft 365 threat protection
- Mitigate incidents using Microsoft 365 Defender
- Protect your identities with Microsoft Entra ID Protection
- Remediate risks with Microsoft Defender for Office 365
- Safeguard your environment with Microsoft Defender for Identity
- Secure your cloud apps and services with Microsoft Defender for Cloud Apps
- Respond to data loss prevention alerts using Microsoft 365
- Manage insider risk in Microsoft Purview

- Investigate threats by using audit features in Microsoft Defender XDR and Microsoft Purview Standard
- Investigate threats using audit in Microsoft Defender XDR and Microsoft Purview (Premium)
- Investigate threats with Content search in Microsoft Purview
- Protect against threats with Microsoft Defender for Endpoint
- Deploy the 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 using Microsoft Defender for Endpoint
- Perform evidence and entities investigations using Microsoft Defender for Endpoint
- Configure and manage automation using Microsoft Defender for Endpoint
- Configure for alerts and detections in Microsoft Defender for Endpoint
- Utilize Vulnerability Management in Microsoft Defender for Endpoint
- Plan for cloud workload protections using Microsoft Defender for Cloud
- Connect Azure assets to Microsoft Defender for Cloud
- Connect non-Azure resources to Microsoft Defender for Cloud
- Manage your cloud security posture management?
- Explain cloud workload protections in Microsoft Defender for Cloud
- Remediate security alerts using Microsoft Defender for Cloud
- Construct KQL statements for Microsoft Sentinel
- Analyze query results using KQL
- Build multi-table statements using KQL
- Work with data in Microsoft Sentinel using Kusto Query Language
- Introduction to Microsoft Sentinel
- Create and manage Microsoft Sentinel workspaces
- Query logs in Microsoft Sentinel
- Use watchlists in Microsoft Sentinel
- Utilize threat intelligence in 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 Common Event Format logs to Microsoft Sentinel

Introduction to Microsoft 365 threat protection

- Understand Microsoft Defender XDR solutions by domain
- Understand the Microsoft Defender XDR role in a Modern SOC

Mitigate incidents using Microsoft 365 Defender

- Manage incidents in Microsoft 365 Defender

- Investigate incidents in Microsoft 365 Defender
- Conduct advanced hunting in Microsoft 365 Defender

Protect your identities with Microsoft Entra ID Protection

- Describe the features of Microsoft Entra ID Protection.
- Describe the investigation and remediation features of Microsoft Entra ID Protection.

Case study: Design security solutions for infrastructure

- How to analyze business requirements
- How to match technical capabilities to meet those needs
- How to design cohesive solutions that incorporate all of the required functions

Remediate risks with Microsoft Defender for Office 365

- Define the capabilities of Microsoft Defender for Office 365.
- Understand how to simulate attacks within your network.
- Explain how Microsoft Defender for Office 365 can remediate risks in your environment.

Safeguard your environment with Microsoft Defender for Identity

- Define the capabilities of Microsoft Defender for Identity.
- Understand how to configure Microsoft Defender for Identity sensors.
- Explain how Microsoft Defender for Identity can remediate risks in your environment.

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

- Define the Defender for Cloud Apps framework
- Explain how Cloud Discovery helps you see what’s going on in your organization
- Understand how to use Conditional Access App Control policies to control access to the apps in your organization

Respond to data loss prevention alerts using Microsoft 365

- Describe data loss prevention (DLP) components in Microsoft 365
- Investigate DLP alerts in the Microsoft Purview compliance portal
- Investigate DLP alerts in Microsoft Defender for Cloud Apps

Manage insider risk in Microsoft Purview

- Explain how Microsoft Purview Insider Risk Management can help prevent, detect, and contain internal risks in an organization.
- Describe the types of built-in, pre-defined policy templates.

- List the prerequisites that need to be met before creating insider risk policies.
- Explain the types of actions you can take on an insider risk management case.

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

- Describe the differences between Audit (Standard) and Audit (Premium).
- Start recording user and admin activity in the Unified Audit Log (UAL).
- Identify the core features of the Audit (Standard) solution.
- Set up and implement audit log searching using the Audit (Standard) solution.
- Export, configure, and view audit log records.
- Use audit log searching to troubleshoot common support issues.

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

- Describe the differences between Audit (Standard) and Audit (Premium).
- Set up and implement Microsoft Purview Audit (Premium).
- Create audit log retention policies.
- Perform forensic investigations of compromised user accounts.

Investigate threats with Content search in Microsoft Purview

- Describe how to use content search in the Microsoft Purview compliance portal.
- Design and create a content search.
- Preview the search results.
- View the search statistics.
- Export the search results and search report.
- Configure search permission filtering.

Protect against threats with Microsoft Defender for Endpoint

- Define the capabilities of Microsoft Defender for Endpoint.
- Understand how to hunt threats within your network.
- Explain how Microsoft Defender for Endpoint can remediate risks in your environment

Deploy the Microsoft Defender for Endpoint environment

- Create a Microsoft Defender for Endpoint environment
- Onboard devices to be monitored by Microsoft Defender for Endpoint
- Configure Microsoft Defender for Endpoint environment settings

Implement Windows security enhancements with Microsoft Defender for Endpoint

- Explain Attack Surface Reduction in Windows

- Enable Attack Surface Reduction rules on Windows 10 devices
- Configure Attack Surface Reduction rules on Windows 10 devices

Perform device investigations in Microsoft Defender for Endpoint

- Use the device page in Microsoft Defender for Endpoint
- Describe device forensics information collected by Microsoft Defender for Endpoint
- Describe behavioral blocking by Microsoft Defender for Endpoint

Perform actions on a device using Microsoft Defender for Endpoint

- Perform actions on a device using Microsoft Defender for Endpoint
- Conduct forensics data collection using Microsoft Defender for Endpoint
- Access devices remotely using Microsoft Defender for Endpoint

Perform evidence and entities investigations using Microsoft Defender for Endpoint

- Investigate files in Microsoft Defender for Endpoint
- Investigate domains and IP addresses in Microsoft Defender for Endpoint
- Investigate user accounts in Microsoft Defender for Endpoint

Configure and manage automation using Microsoft Defender for Endpoint

- Configure advanced features of Microsoft Defender for Endpoint
- Manage automation settings in Microsoft Defender for Endpoint

Configure for alerts and detections in Microsoft Defender for Endpoint

- Configure alert settings in Microsoft Defender for Endpoint
- Manage indicators in Microsoft Defender for Endpoint

Utilize Vulnerability Management in Microsoft Defender for Endpoint

- Describe Vulnerability Management in Microsoft Defender for Endpoint
- Identify vulnerabilities on your devices with Microsoft Defender for Endpoint
- Track emerging threats in Microsoft Defender for Endpoint

Plan for cloud workload protections using Microsoft Defender for Cloud

- Describe Microsoft Defender for Cloud features
- Microsoft Defender for Cloud workload protections
- Enable Microsoft Defender for Cloud

Connect Azure assets to Microsoft Defender for Cloud

- Explore Azure assets
- Configure auto-provisioning in Microsoft Defender for Cloud
- Describe manual provisioning in Microsoft Defender for Cloud

Connect non-Azure resources to Microsoft Defender for Cloud

- Connect non-Azure machines to Microsoft Defender for Cloud
- Connect AWS accounts to Microsoft Defender for Cloud
- Connect GCP accounts to Microsoft Defender for Cloud

Manage your cloud security posture management

- Describe Microsoft Defender for Cloud features.
- Explain the Microsoft Defender for Cloud security posture management protections for your resources.

Explain cloud workload protections in Microsoft Defender for Cloud

- Explain which workloads are protected by Microsoft Defender for Cloud
- Describe the benefits of the protections offered by Microsoft Defender for Cloud
- Explain how Microsoft Defender for Cloud protections function

Remediate security alerts using Microsoft Defender for Cloud

- Describe alerts in Microsoft Defender for Cloud
- Remediate alerts in Microsoft Defender for Cloud
- Automate responses in Microsoft Defender for Cloud

Construct KQL statements for Microsoft Sentinel

- Construct KQL statements
- Search log files for security events using KQL
- Filter searches based on event time, severity, domain, and other relevant data using KQL

Analyze query results using KQL

- Summarize data using KQL statements
- Render visualizations using KQL statements

Build multi-table statements using KQL

- Create queries using unions to view results across multiple tables using KQL
- Merge two tables with the join operator using KQL

Work with data in Microsoft Sentinel using Kusto Query Language

- Extract data from unstructured string fields using KQL
- Extract data from structured string data using KQL
- Create Functions using KQL

Introduction to Microsoft Sentinel

- Identify the various components and functionality of Microsoft Sentinel.
- Identify use cases where Microsoft Sentinel would be a good solution.

Create and manage Microsoft Sentinel workspaces

- Describe Microsoft Sentinel workspace architecture
- Install Microsoft Sentinel workspace
- Manage a Microsoft Sentinel workspace

Query logs in Microsoft Sentinel

- Use the Logs page to view data tables in Microsoft Sentinel
- Query the most used tables using Microsoft Sentinel

Use watchlists in Microsoft Sentinel

- Create a watchlist in Microsoft Sentinel
- Use KQL to access the watchlist in Microsoft Sentinel

Utilize threat intelligence in Microsoft Sentinel

- Manage threat indicators in Microsoft Sentinel
- Use KQL to access threat indicators in Microsoft Sentinel

Connect data to Microsoft Sentinel using data connectors

- Describe how to install Content Hub Solutions to provision Microsoft Sentinel Data connectors
- Explain the use of data connectors in Microsoft Sentinel
- Describe the Microsoft Sentinel data connector providers
- Explain the Common Event Format and Syslog connector differences in Microsoft Sentinel

Connect Microsoft services to Microsoft Sentinel

- Connect Microsoft service connectors
- Explain how connectors auto-create incidents in Microsoft Sentinel

Connect Microsoft Defender XDR to Microsoft Sentinel

- Activate the Microsoft Defender XDR connector in Microsoft Sentinel

- Activate the Microsoft Defender for Cloud connector in Microsoft Sentinel
- Activate the Microsoft Defender for IoT connector in Microsoft Sentinel

Connect Windows hosts to Microsoft Sentinel

- Connect Azure Windows Virtual Machines to Microsoft Sentinel
- Connect non-Azure Windows hosts to Microsoft Sentinel
- Configure Log Analytics agent to collect Sysmon events

Connect syslog data sources to Microsoft Sentinel

- Describe the Azure Monitor Agent Data Collection Rule (DCR) for Syslog
- Install and Configure the Azure Monitor Linux Agent extension with the Syslog DCR
- Run the Azure Arc Linux deployment and connection scripts
- Verify Syslog log data is available in Microsoft Sentinel
- Create a parser using KQL in Microsoft Sentinel

Connect threat indicators to Microsoft Sentinel

- Configure the TAXII connector in Microsoft Sentinel
- Configure the Threat Intelligence Platform connector in Microsoft Sentinel
- View threat indicators in Microsoft Sentinel

Threat detection with Microsoft Sentinel analytics

- Explain the importance of Microsoft Sentinel Analytics.
- Explain different types of analytics rules.
- Create rules from templates.
- Create new analytics rules and queries using the analytics rule wizard.
- Manage rules with modifications.

Automation in Microsoft Sentinel

- Explain automation options in Microsoft Sentinel
- Create automation rules in Microsoft Sentinel

Threat response with Microsoft Sentinel playbooks

- Explain Microsoft Sentinel SOAR capabilities.
- Explore the Microsoft Sentinel Logic Apps connector.
- Create a playbook to automate an incident response.
- Run a playbook on demand in response to an incident.

Security incident management in Microsoft Sentinel

- Learn about security incidents and Microsoft Sentinel incident management.
- Explore Microsoft Sentinel incident evidence and entities.
- Use Microsoft Sentinel to investigate security incidents and manage incident resolution.

Identify threats with Behavioral Analytics

- Explain User and Entity Behavior Analytics in Azure Sentinel
- Explore entities in Microsoft Sentinel

Data normalization in Microsoft Sentinel

- Use ASIM Parsers
- Create ASIM Parser
- Create parameterized KQL functions

Query, visualize, and monitor data in Microsoft Sentinel

- Visualize security data using Microsoft Sentinel Workbooks.
- Understand how queries work.
- Explore workbook capabilities.
- Create a Microsoft Sentinel Workbook.

Manage content in Microsoft Sentinel

- Install a content hub solution in Microsoft Sentinel
- Connect a GitHub repository to Microsoft Sentinel

Explain threat hunting concepts in Microsoft Sentinel

- Describe threat hunting concepts for use with Microsoft Sentinel
- Define a threat hunting hypothesis for use in Microsoft Sentinel

Threat hunting with Microsoft Sentinel

- Use queries to hunt for threats.
- Save key findings with bookmarks.
- Observe threats over time with livestream.

Use Search jobs in Microsoft Sentinel

- Use Search Jobs in Microsoft Sentinel
- Restore archive logs in Microsoft Sentinel

Hunt for threats using notebooks in Microsoft Sentinel

- Explore API libraries for advanced threat hunting in Microsoft Sentinel
- Describe notebooks in Microsoft Sentinel
- Create and use notebooks in Microsoft Sentinel