Updated 03/06/2024

Sign up

SC-200 Certification Training

ALL-IN-ONE: EXAMINATION INCLUDED IN PRICE

3 days (21 hours)

Presentation

Microsoft Security Operations Analyst, known as SC-200, is a certification that validates your skills in managing security incidents and resolving threats using security solutions provided by Microsoft.

We'll cover topics such as threat analysis, incident response and protecting corporate environments. Your skills will be put to the test to handle and resolve all security incidents.

During this course, you'll use Microsoft tools and technologies such as Microsoft Sentinel for security information and event management (SIEM), and Microsoft Defender for threat protection (ATP).

Achieving SC-200 certification will reinforce your credibility as a security professional and enhance your career opportunities in the cybersecurity field.

As with all our training courses, this one will introduce you to the latest Microsoft news.

Objectives

- Mitigate threats with Microsoft Defender for the Cloud
- Configure your corporate environment with Microsoft Sentinel
- Create detections and carry out investigations
- Discover and analyze threats to the Microsoft 365 environment

Target audience

- Safety professionals
- SOC Analysts
- System administrators

Prerequisites

- Familiarity with Microsoft 365 and Azure
- Experience in IT security
- System administration skills

SC-200 TRAINING PROGRAM

Discovering threats to the Microsoft 365 environment

- Investigate, respond to and remediate threats to Microsoft Teams, SharePoint Online and OneDrive
- Review alerts generated by data loss prevention (DLP) policies, and then answer
- Discover and manage applications with Microsoft Defender for Cloud Apps
- Identify, investigate and remediate security risks with Defender for Cloud Apps
- Importance of LINQ in modern .NET projects

Reduce endpoint risks with Defender for Endpoint

- Manage data retention, alert notifications and advanced features
- Recommend reduction of the attack surface area (ASR) for aircraft
- Responding to incidents and alerts
- Configure and manage device groups
- Identify devices at risk using Microsoft Defender Vulnerability Management
- Manage terminal threat indicators
- Identify unmanaged devices using device discovery

Protect your identities

- Discover the features of Microsoft Entra
- Mitigate security risks associated with Azure AD identity protection events
- Reduce security risks using Microsoft Defender for Identity

Manage detection and extended response (XDR)

- Managing actions and submissions in the Microsoft 365 Defender portal
- Identifying threats using KQL
- Identify and remediate security risks using Microsoft Secure Score

- Analyze threat analyses in the Microsoft 365 Defender portal
- Configure and manage custom detections and alerts

Implement and maintain cloud security posture management

- Assign and manage regulatory compliance policies with Microsoft Cloud Security Benchmark (MCSB)
- Improving Defender's security score
- Configuring plans and agents for Microsoft Defender for Servers
- Configuring and managing Microsoft Defender for DevOps

Configuring environment settings in Defender for the Cloud

- Configuring Defender roles
- Assess and recommend protection for cloud workloads
- Activate Microsoft Defender plans
- Configure automatic integration for Azure resources
- Connecting computing resources using Azure Arc
- Connect multi-cloud resources using environment settings

Responding to alerts and incidents in Defender for Cloud

- Configure e-mail notifications
- Create and manage alert suppression rules
- Designing and configuring workflow automation in Defender
- Respond to alerts and incidents using Defender recommendations
- Managing security alerts and incidents
- Analyze Defender for Cloud threat intelligence reports

Designing and configuring a Microsoft Sentinel workspace

- Planning a Microsoft Sentinel workspace
- Configuring Microsoft Sentinel roles
- Designing and configuring Microsoft Sentinel data storage

Manage threats using entity behavioral analysis

- Configuring entity behavior parameters
- Investigate threats using entity pages
- Configure analytical rules for anomaly detection

Designing and configuring a Microsoft Sentinel workspace

- Planning a Microsoft Sentinel workspace

- Configuring Microsoft Sentinel roles
- Designing and configuring Microsoft Sentinel data storage

Manage threats using entity behavioral analysis

- Configuring entity behavior parameters
- Investigate threats using entity pages
- Configure analytical rules for anomaly detection

Companies concerned

This training course is aimed at both individuals and companies, large or small, wishing to train their teams in a new advanced computer technology, or to acquire specific business knowledge or modern methods.

Positioning on entry to training

Positioning at the start of training complies with Qualiopi quality criteria. As soon as registration is finalized, the learner receives a self-assessment questionnaire which enables us to assess his or her estimated level of proficiency in different types of technology, as well as his or her expectations and personal objectives for the training to come, within the limits imposed by the selected format. This questionnaire also enables us to anticipate any connection or security difficulties within the company (intra-company or virtual classroom) which could be problematic for the follow-up and smooth running of the training session.

Teaching methods

Practical course: 60% Practical, 40% Theory. Training material distributed in digital format to all participants.

Organization

The course alternates theoretical input from the trainer, supported by examples, with brainstorming sessions and group work.

Validation

At the end of the session, a multiple-choice questionnaire verifies the correct acquisition of skills.

Sanction

A certificate will be issued to each trainee who completes the course.