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

Category: Networking & Security | **Vendor:** Microsoft Technical

Duration: 32.00 hours (4 days) **26.0 CPD Hours** **Rating:** ⭐ 4.6 (5,878 reviews)

Course Information

Delivery Format:	Instructor Led - Online
Certification:	Microsoft Certified: Security Operations Analyst Associate
Related Exam:	SC-200

Course Overview

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.

About This Course

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.

Who Should Attend

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.

Prerequisites & Entry Requirements

General Prerequisites:

- 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.

Detailed Course Outline

1 - Introduction to Microsoft Defender XDR threat protection

- Explore Extended Detection & Response (XDR) response use cases
- Understand Microsoft Defender XDR in a Security Operations Center (SOC)
- Explore Microsoft Security Graph
- Investigate security incidents in Microsoft Defender XDR
- Module assessment

2 - Mitigate incidents using Microsoft Defender

- Use the Microsoft Defender portal
- Manage incidents
- Investigate incidents
- Manage and investigate alerts
- Manage automated investigations
- Use the action center
- Explore advanced hunting
- Investigate Microsoft Entra sign-in logs
- Understand Microsoft Secure Score
- Analyze threat analytics
- Analyze reports
- Configure the Microsoft Defender portal
- Module assessment

3 - Remediate risks with Microsoft Defender for Office 365

- Automate, investigate, and remediate
- Configure, protect, and detect
- Simulate attacks

4 - Manage Microsoft Entra Identity Protection

- Review identity protection basics
- Implement and manage user risk policy
- Monitor, investigate, and remediate elevated risky users
- Implement security for workload identities
- Explore Microsoft Defender for Identity
- Module assessment

5 - Safeguard your environment with Microsoft Defender for Identity

- Configure Microsoft Defender for Identity sensors
- Review compromised accounts or data
- Integrate with other Microsoft tools

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

- Understand the Defender for Cloud Apps Framework
- Explore your cloud apps with Cloud Discovery
- Protect your data and apps with Conditional Access App Control
- Walk through discovery and access control with Microsoft Defender for Cloud Apps
- Classify and protect sensitive information
- Detect Threats
- Module assessment

7 - Introduction to generative AI and agents

- Large language models (LLMs)
- Prompts
- AI agents
- Module assessment

8 - Describe Microsoft Security Copilot

- Get acquainted with Microsoft Security Copilot
- Describe Microsoft Security Copilot terminology
- Describe how Microsoft Security Copilot processes prompt requests
- Describe the elements of an effective prompt
- Describe how to enable Microsoft Security Copilot
- Module assessment

9 - Describe the core features of Microsoft Security Copilot

- Describe the features available in the standalone experience of Microsoft Security Copilot
- Describe the features available in a session of the standalone experience
- Describe workspaces
- Describe the Microsoft plugins available in Microsoft Security Copilot
- Describe the non-Microsoft plugins supported by Microsoft Security Copilot
- Describe custom promptbooks
- Describe knowledge base connections
- Module assessment

10 - Describe the embedded experiences of Microsoft Security Copilot

- Describe Copilot in Microsoft Defender XDR
- Copilot in Microsoft Purview
- Copilot in Microsoft Entra
- Copilot in Microsoft Intune
- Copilot in Microsoft Defender for Cloud (Preview)
- Module assessment

11 - Explore use cases of Microsoft Security Copilot

- Explore the first run experience
- Explore the standalone experience
- Explore Security Copilot workspaces
- Configure the Microsoft Sentinel plugin
- Enable a custom plugin
- Explore file uploads as a knowledge base
- Create a custom promptbook
- Explore the capabilities of Copilot in Microsoft Defender XDR
- Explore the capabilities of Copilot in Microsoft Purview
- Explore the capabilities of Copilot in Microsoft Entra
- Module assessment

12 - Investigate and respond to Microsoft Purview Data Loss Prevention alerts

- Understand data loss prevention (DLP) alerts
- Understand the DLP alert lifecycle
- Configure DLP policies to generate alerts
- Investigate DLP alerts in Microsoft Purview
- Investigate DLP alerts in Microsoft Defender XDR
- Investigate DLP alerts with Security Copilot and AI agents
- Respond to DLP alerts
- Module assessment

13 - Investigate insider risk alerts and related activity

- Understand insider risk alerts and investigations
- Manage alert volume in insider risk management
- Investigate and triage insider risk alerts in Microsoft Purview
- Investigate insider risk alerts with Security Copilot and AI agents
- Analyze alert context with the All risk factors tab
- Investigate activity details with the Activity explorer tab
- Review patterns over time with the User activity tab
- Investigate insider risk alerts in Microsoft Defender XDR
- Manage and take action on insider risk cases
- Module assessment

14 - Search and investigate with Microsoft Purview Audit

- Microsoft Purview Audit overview
- Configure and manage Microsoft Purview Audit
- Conduct searches with Audit (Standard)
- Audit Microsoft Copilot for Microsoft 365 interactions
- Investigate activities with Audit (Premium)
- Export audit log data
- Configure audit retention with Audit (Premium)
- Module assessment

15 - Search for content with Microsoft Purview eDiscovery

- Understand eDiscovery and content search capabilities
- Prerequisites for using eDiscovery in Microsoft Purview
- Create an eDiscovery search
- Conduct an eDiscovery search
- Export eDiscovery search results
- Module assessment

16 - Protect against threats with Microsoft Defender for Endpoint

- Practice security administration
- Hunt threats within your network

17 - Deploy the Microsoft Defender for Endpoint environment

- Create your environment
- Understand operating systems compatibility and features
- Onboard devices
- Manage access
- Create and manage roles for role-based access control
- Configure device groups
- Configure environment advanced features
- Module assessment

18 - Implement Windows security enhancements with Microsoft Defender for Endpoint

- Understand attack surface reduction
- Enable attack surface reduction rules
- Module assessment

19 - Perform device investigations in Microsoft Defender for Endpoint

- Use the device inventory list
- Investigate the device
- Use behavioral blocking
- Detect devices with device discovery
- Module assessment

20 - Perform actions on a device using Microsoft Defender for Endpoint

- Explain device actions
- Run Microsoft Defender antivirus scan on devices
- Collect investigation package from devices
- Initiate live response session
- Module assessment

21 - Perform evidence and entities investigations using Microsoft Defender for Endpoint

- Investigate a file
- Investigate a user account
- Investigate an IP address
- Investigate a domain
- Module assessment

22 - Configure and manage automation using Microsoft Defender for Endpoint

- Configure advanced features
- Manage automation upload and folder settings
- Configure automated investigation and remediation capabilities
- Block at risk devices
- Module assessment

23 - Configure for alerts and detections in Microsoft Defender for Endpoint

- Configure advanced features
- Configure alert notifications
- Manage alert suppression
- Manage indicators
- Module assessment

24 - Utilize Vulnerability Management in Microsoft Defender for Endpoint

- Understand vulnerability management
- Explore vulnerabilities on your devices
- Manage remediation
- Module assessment

25 - Plan for cloud workload protections using Microsoft Defender for Cloud

- Explain Microsoft Defender for Cloud
- Describe Microsoft Defender for Cloud workload protections
- Enable Microsoft Defender for Cloud
- Module assessment

26 - Connect Azure assets to Microsoft Defender for Cloud

- Explore and manage your resources with asset inventory
- Configure auto provisioning
- Manual agent provisioning
- Module assessment

27 - Connect non-Azure resources to Microsoft Defender for Cloud

- Protect non-Azure resources
- Connect non-Azure machines
- Connect your AWS accounts
- Connect your GCP accounts
- Module assessment

28 - Manage your cloud security posture management

- Explore Secure Score
- Explore Recommendations
- Measure and enforce regulatory compliance
- Understand Workbooks
- Module assessment

29 - Explain cloud workload protections in Microsoft Defender for Cloud

- Understand Microsoft Defender for servers
- Understand Microsoft Defender for App Service
- Understand Microsoft Defender for Storage
- Understand Microsoft Defender for SQL
- Understand Microsoft Defender for open-source databases
- Understand Microsoft Defender for Key Vault
- Understand Microsoft Defender for Resource Manager
- Understand Microsoft Defender for DNS
- Understand Microsoft Defender for Containers
- Understand Microsoft Defender additional protections
- Module assessment

30 - Remediate security alerts using Microsoft Defender for Cloud

- Understand security alerts
- Remediate alerts and automate responses
- Suppress alerts from Defender for Cloud
- Generate threat intelligence reports
- Respond to alerts from Azure resources
- Module assessment

31 - Construct KQL statements for Microsoft Sentinel

- Understand the Kusto Query Language statement structure
- Use the search operator
- Use the where operator
- Use the let statement
- Use the extend operator
- Use the order by operator
- Use the project operators
- Module assessment

32 - Analyze query results using KQL

- Use the summarize operator
- Use the summarize operator to filter results
- Use the summarize operator to prepare data
- Use the render operator to create visualizations
- Module assessment

33 - Build multi-table statements using KQL

- Use the union operator
- Use the join operator
- Module assessment

34 - Work with data in Microsoft Sentinel using Kusto Query Language

- Extract data from unstructured string fields
- Extract data from structured string data
- Integrate external data
- Create parsers with functions
- Module assessment

35 - Introduction to Microsoft Sentinel

- What is Microsoft Sentinel?
- How Microsoft Sentinel works
- When to use Microsoft Sentinel
- Module assessment

36 - Create and manage Microsoft Sentinel workspaces

- Plan for the Microsoft Sentinel workspace
- Create a Microsoft Sentinel workspace
- Manage workspaces across tenants using Azure Lighthouse
- Understand Microsoft Sentinel permissions and roles
- Manage Microsoft Sentinel settings
- Configure logs
- Module assessment

37 - Query logs in Microsoft Sentinel

- Query logs in the logs page
- Understand Microsoft Sentinel tables
- Understand common tables
- Understand Microsoft Defender XDR tables
- Module assessment

38 - Use watchlists in Microsoft Sentinel

- Plan for watchlists
- Create a watchlist
- Manage watchlists
- Module assessment

39 - Utilize threat intelligence in Microsoft Sentinel

- Define threat intelligence
- Manage your threat indicators
- View your threat indicators with KQL
- Module assessment

40 - Integrate Microsoft Defender XDR with Microsoft Sentinel

- Understand the benefits of integrating Microsoft Sentinel with Defender XDR
- Explore the capability differences between Microsoft Defender XDR and Microsoft Sentinel portals
- Onboarding Microsoft Sentinel to Microsoft Defender XDR
- Explore Microsoft Sentinel features in Microsoft Defender XDR
- Module assessment

41 - Connect data to Microsoft Sentinel using data connectors

- Ingest log data with data connectors
- Understand data connector providers
- View connected hosts
- Module assessment

42 - Connect Microsoft services to Microsoft Sentinel

- Plan for Microsoft services connectors
- Connect the Microsoft 365 connector
- Connect the Microsoft Entra connector
- Connect the Microsoft Entra ID Protection connector
- Connect the Azure Activity connector
- Module assessment

43 - Connect Microsoft Defender XDR to Microsoft Sentinel

- Plan for Microsoft Defender XDR connectors
- Connect the Microsoft Defender XDR connector
- Connect Microsoft Defender for Cloud connector
- Connect Microsoft Defender for IoT
- Connect Microsoft Defender legacy connectors
- Module assessment

44 - Connect Windows hosts to Microsoft Sentinel

- Plan for Windows hosts security events connector
- Connect using the Windows Security Events via AMA Connector
- Connect using the Security Events via Legacy Agent Connector
- Collect Sysmon event logs
- Module assessment

45 - Connect Common Event Format logs to Microsoft Sentinel

- Plan for Common Event Format connector
- Connect your external solution using the Common Event Format connector
- Module assessment

46 - Connect syslog data sources to Microsoft Sentinel

- Plan for syslog data collection
- Collect data from Linux-based sources using syslog
- Configure the Data Collection Rule for Syslog Data Sources
- Parse syslog data with KQL
- Module assessment

47 - Connect threat indicators to Microsoft Sentinel

- Plan for threat intelligence connectors
- Connect the Defender Threat Intelligence connector
- Connect the threat intelligence TAXII connector
- Connect the threat intelligence Upload API connector
- View your threat indicators with KQL
- Module assessment

48 - Threat detection with Microsoft Sentinel analytics

- What is Microsoft Sentinel Analytics?
- Types of analytics rules
- Create an analytics rule from templates
- Create an analytics rule from wizard
- Manage analytics rules

49 - Automation in Microsoft Sentinel

- Understand automation options
- Create automation rules
- Module assessment

50 - Threat response with Microsoft Sentinel playbooks

- What are Microsoft Sentinel playbooks?
- Trigger a playbook in real-time
- Run playbooks on demand

51 - Security incident management in Microsoft Sentinel

- Understand incidents
- Incident evidence and entities
- Incident management

52 - Identify threats with Behavioral Analytics

- Understand behavioral analytics
- Explore entities
- Display entity behavior information
- Use Anomaly detection analytical rule templates
- Module assessment

53 - Data normalization in Microsoft Sentinel

- Understand data normalization
- Use ASIM Parsers
- Understand parameterized KQL functions
- Create an ASIM Parser
- Configure Azure Monitor Data Collection Rules
- Module assessment

54 - Query, visualize, and monitor data in Microsoft Sentinel

- Monitor and visualize data
- Query data using Kusto Query Language
- Use default Microsoft Sentinel Workbooks
- Create a new Microsoft Sentinel Workbook

55 - Manage content in Microsoft Sentinel

- Use solutions from the content hub
- Use repositories for deployment
- Module assessment

56 - Explain threat hunting concepts in Microsoft Sentinel

- Understand cybersecurity threat hunts
- Develop a hypothesis
- Explore MITRE ATT&CK
- Module assessment

57 - Threat hunting with Microsoft Sentinel

- Explore creation and management of threat-hunting queries
- Save key findings with bookmarks
- Observe threats over time with livestream

58 - Use Search jobs in Microsoft Sentinel

- Hunt with a Search Job
- Restore historical data
- Module assessment

59 - Hunt for threats using notebooks in Microsoft Sentinel

- Access Azure Sentinel data with external tools
- Hunt with notebooks
- Create a notebook
- Explore notebook code
- Module assessment

□□ Certification Path

Microsoft Certified: Security Operations Analyst Associate

Exam: SC-200

Upcoming Schedule

Available training dates for SC-200T00 Defend against cyberthreats with Microsoft's security operations platform:

Start Date	End Date	Location	Delivery	Price
21 Sep 2026	24 Sep 2026	Online	Virtual	€2,495.00
16 Nov 2026	19 Nov 2026	Online	Virtual	€2,495.00
11 Jan 2027	14 Jan 2027	Online	Virtual	€2,495.00

Frequently Asked Questions

Q: What delivery options are available for SC-200T00 Defend against cyberthreats with Microsoft's security operations platform?

We offer multiple delivery formats:

- Live Instructor-Led Classroom Online (Virtual/Live Online)
- Traditional Instructor-Led Classroom Training (ILT)
- On-site delivery at your offices anywhere in United Kingdom
- Private dedicated courses customized for your team

Q: What certification does this course prepare me for?

The SC-200T00 Defend against cyberthreats with Microsoft's security operations platform course helps prepare you for the Microsoft Certified: Security Operations Analyst Associate certification path.

Q: Which exam does this course prepare me for?

This course prepares you for the SC-200 official exam. You can take this exam at any exam center across United Kingdom including London, Manchester, Birmingham, Edinburgh, or live online wherever you are located.

Q: How many CPD hours does this course provide?

The 4-day SC-200T00 Defend against cyberthreats with Microsoft's security operations platform course provides up to 26.0 CPD hours of structured learning. CPD certificates can be provided upon request.

Q: What is the duration of the SC-200T00 Defend against cyberthreats with Microsoft's security operations platform training?

The training takes place over 4 day(s), with each day lasting approximately 32.00 hours including breaks for lunch and refreshments.

Q: Do you provide corporate training for SC-200T00 Defend against cyberthreats with Microsoft's security operations platform?

Yes, we provide corporate training, dedicated training, and closed classes for SC-200T00 Defend against cyberthreats with Microsoft's security operations platform. Training can take place anywhere in United Kingdom including London, Manchester, Birmingham, Edinburgh, or live online allowing teams from across United Kingdom or internationally to attend.

Q: What related terms do people search for?

Popular related searches include: SC-200T00: Defend against cyberthreats with Microsoft's security operations platform, Microsoft, vILT, SC-200T00

Q: Why choose Nexus Human for SC-200T00 Defend against cyberthreats with Microsoft's security operations platform?

Nexus Human is recognized as one of the leading training providers. Our trainers have won multiple awards including:

- Small Firms Best Trainer Award
- National Training Partner of the Year (Ireland) - Multiple Years
- Global Top 30 Instructor Awards (2012, 2019, 2021)
- Tech Excellence Award Nominations
- Learning Performance Institute (LPI) External Training Provider Sponsor 2024

Q: Are there any discount codes available?

Yes! Use discount code **PENPAL5** when booking your SC-200T00 Defend against cyberthreats with Microsoft's security operations platform training. Please note that only one discount code can be used per booking and cannot be combined with other special offers.

Nexus Human

Professional Training & Development

Email: info@nexushuman.com

Website: www.nexushuman.com

Phone: +353 1 XXX XXXX (Ireland) | +44 20 XXXX XXXX (UK)