KOENIG
step forward

MICROSOFT OFFICIAL COURSE SC-200T00 | 4 DAYS

Microsoft Security Operations Analyst

Defend against cyberthreats with Microsoft's security operations platform

Instructor-led training on investigating, responding to and hunting for threats with Microsoft Defender XDR, Microsoft Security Copilot, Microsoft Purview, Microsoft Defender for Endpoint, Kusto Query Language and Microsoft Sentinel.

PROGRAMME AT A GLANCE

4 DAYS	32 HOURS	9 PATHS	9 LABS
Training duration	Instructor-led learning	53 modules	Hands-on lab exercises

Audience: Security operations analysts, SOC engineers and security administrators who investigate, respond to and hunt for threats.

Certification: Prepares learners for Exam SC-200: Microsoft Certified: Security Operations Analyst Associate.

Course overview

The security operations analyst reduces organisational risk by rapidly remediating active attacks, advising on improvements to threat protection practices and referring policy violations to the right stakeholders. This course builds those skills across Microsoft's security operations platform and is weighted towards Microsoft Sentinel.

Learning outcomes

- Investigate and remediate incidents across identities, endpoints, email and cloud apps with Microsoft Defender XDR.
- Use Microsoft Security Copilot in standalone and embedded experiences to accelerate investigation and response.
- Respond to data loss prevention and insider risk alerts and investigate threats with Microsoft Purview Content search and Audit.
- Deploy, configure and operate Microsoft Defender for Endpoint, including device response actions and vulnerability management.
- Write KQL queries to analyse, correlate and parse security data.
- Configure Microsoft Sentinel workspaces, connect data sources and build detections, automation and playbooks.
- Manage incidents and hunt for threats in Microsoft Sentinel using hunting queries, search jobs and notebooks.

Prerequisites

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

Exam SC-200 skills measured

STUDY AREA	WEIGHTING
Manage a security operations environment	40-45%
Respond to security incidents	35-40%
Perform threat hunting	20-25%

Programme structure

Each day runs from 9:00 to 5:00 with two 15-minute breaks and a 1-hour lunch, giving 6.5 hours of instructor-led learning. Each day covers around two learning paths, each followed by a hands-on lab.

TIME	DAILY BLOCK	DURATION
9:00 - 10:30	Session 1	90 min
10:30 - 10:45	Tea break	15 min
10:45 - 12:30	Session 2	105 min
12:30 - 1:30	Lunch	60 min
1:30 - 3:15	Session 3	105 min
3:15 - 3:30	Tea break	15 min
3:30 - 5:00	Session 4	90 min

DAY	FOCUS	LEARNING PATHS
DAY 1	Microsoft Defender XDR, Microsoft Security Copilot, start Microsoft Purview	LP 1, LP 2, LP 3 (part)
DAY 2	Microsoft Purview, Microsoft Defender for Endpoint, start KQL	LP 3 (complete), LP 4, LP 5 (part)
DAY 3	KQL, Microsoft Sentinel setup and connecting data	LP 5 (complete), LP 6, LP 7, LP 8 (start)
DAY 4	Microsoft Sentinel detections, investigations and threat hunting	LP 8 (complete), LP 9

DAY 1

Microsoft Defender XDR, Security Copilot and Microsoft Purview

TIME	DAILY AGENDA
30 min	Course introduction
120 min	Learning Path 1: Mitigate threats using Microsoft Defender XDR
45 min	Lab 1: Explore Microsoft Defender XDR
60 min	Learning Path 2: Get started with Microsoft Security Copilot
45 min	Lab 2: Microsoft Security Copilot simulations
60 min	Learning Path 3: Mitigate threats using Microsoft Purview (Modules 1-3)
30 min	Lab 3: Microsoft Purview

LEARNING PATH 1 | Mitigate threats using Microsoft Defender XDR

6 modules

#	MODULE	KEY TOPICS
1	Introduction to Microsoft 365 threat protection	Microsoft Defender XDR and the unified security operations portal; incident correlation across identities, endpoints, email and cloud apps; Microsoft Secure Score.
2	Mitigate incidents using Microsoft Defender XDR	Manage incidents and alerts; investigate the attack story; automated investigation and response; advanced hunting basics; threat analytics; Microsoft Sentinel in the unified portal.
3	Protect your identities with Microsoft Entra ID Protection	User and sign-in risk detections; risk-based Conditional Access policies; investigate and remediate risky users and sign-ins.
4	Remediate risks with Microsoft Defender for Office 365	Safe Links, Safe Attachments and anti-phishing; Threat Explorer and real-time detections; Attack simulation training; automated remediation of email threats.
5	Safeguard your environment with Microsoft Defender for Identity	Sensors and on-premises Active Directory signals; reconnaissance, lateral movement and domain dominance detections; identity security posture assessments.
6	Secure your cloud apps and services with Microsoft Defender for Cloud Apps	Cloud app discovery and shadow IT; app connectors and conditional access app control; activity and file policies; anomaly detection and alert investigation.

HANDS-ON LAB 1 Explore Microsoft Defender XDR: workspace, incidents, Secure Score and the guided demonstrations.

LEARNING PATH 2 | Get started with Microsoft Security Copilot

4 modules

#	MODULE	KEY TOPICS
1	Fundamentals of Generative AI	Large language models, prompts and responses, copilots and responsible AI principles.

#	MODULE	KEY TOPICS
2	Describe Microsoft Security Copilot	What Security Copilot is, how it works, security compute units, terminology and how analysts use it across the SOC.
3	Describe the core features of Microsoft Security Copilot	The standalone experience: sessions, prompts and promptbooks, plugins, pinboard, sharing and admin settings.
4	Describe the embedded experiences of Microsoft Security Copilot	Copilot inside Defender XDR, Microsoft Sentinel, Intune, Entra and Purview: incident summaries, guided response, script analysis and KQL generation.

HANDS-ON LAB 2 Explore Microsoft Security Copilot through web-based simulations of the standalone and embedded experiences.

LEARNING PATH 3 | Mitigate threats using Microsoft Purview

5 modules

#	MODULE	KEY TOPICS
1	Microsoft Purview Compliance Solutions	The Purview portal and solution catalogue; how data security and compliance signals reach the security operations analyst.
2	Respond to data loss prevention alerts using Microsoft Purview	DLP policies and alerts; investigate and triage DLP alerts in Purview and Defender XDR; remediation actions.
3	Manage insider risk in Microsoft Purview	Insider risk management policies, indicators and alerts; case investigation and collaboration with HR and legal stakeholders.
4	Investigate threats using Content search in Microsoft Purview	Build and run content searches with conditions; review, export and act on results; search and purge for malicious email.
5	Investigate threats using Microsoft Purview Audit	Audit (Standard) and Audit (Premium); search the unified audit log; investigate compromised accounts and intelligent insights.

HANDS-ON LAB 3 Mitigate threats using Microsoft Purview: investigate alerts, run a content search and search the audit log.

DAY 2

Microsoft Purview, Defender for Endpoint and KQL

TIME	DAILY AGENDA
20 min	Recap of Day 1
40 min	Learning Path 3: Mitigate threats using Microsoft Purview (Modules 4-5)
135 min	Learning Path 4: Mitigate threats using Microsoft Defender for Endpoint
75 min	Lab 4: Microsoft Defender for Endpoint
120 min	Learning Path 5: Create queries for Microsoft Sentinel using KQL (Modules 1-3)

LEARNING PATH 4 | Mitigate threats using Microsoft Defender for Endpoint

9 modules

#	MODULE	KEY TOPICS
1	Protect against threats with Microsoft Defender for Endpoint	Defender for Endpoint capabilities, licensing and the security operations workflow for endpoints.
2	Deploy the Microsoft Defender for Endpoint environment	Tenant setup, device onboarding methods, roles, device groups and environment settings.
3	Implement Windows security enhancements with Microsoft Defender for Endpoint	Attack surface reduction rules, controlled folder access, exploit and network protection.
4	Perform device investigations in Microsoft Defender for Endpoint	Device inventory, device timeline, alerts and behavioural blocking and containment.
5	Perform actions on a device using Microsoft Defender for Endpoint	Isolate devices, restrict app execution, run antivirus scans, collect investigation packages and use live response.
6	Perform evidence and entities investigations using Microsoft Defender for Endpoint	Investigate files, users, IP addresses and domains; file actions and deep analysis.
7	Configure and manage automation using Microsoft Defender for Endpoint	Automated investigation levels, remediation settings, indicators and the Action centre.
8	Configure for alerts and detections in Microsoft Defender for Endpoint	Advanced features, alert notifications, alert suppression and custom indicators of compromise.
9	Utilize Vulnerability Management in Microsoft Defender for Endpoint	Exposure score, security recommendations, software inventory, weaknesses and remediation tracking.

HANDS-ON LAB 4 Mitigate threats using Microsoft Defender for Endpoint: onboard a device, configure the environment and investigate and respond to an alert.

LEARNING PATH 5 | Create queries for Microsoft Sentinel using Kusto Query Language (KQL)

4 modules

#	MODULE	KEY TOPICS
1	Construct KQL statements for Microsoft Sentinel	KQL statement structure; let, search, where, extend, order by and project; working with strings and time.

#	MODULE	KEY TOPICS
2	Analyze query results using KQL	Summarize, aggregation functions, arg_max and arg_min, and visualising results with render.
3	Build multi-table statements using KQL	Union and join operators and choosing the right join kind for investigations.
4	Work with data in Microsoft Sentinel using Kusto Query Language	Extract data from unstructured strings, parse JSON and dynamic fields, and use KQL functions.

HANDS-ON LAB 5 Create queries for Microsoft Sentinel using KQL.

DAY 3

KQL and configuring Microsoft Sentinel

TIME	DAILY AGENDA
20 min	Recap of Day 2
30 min	Learning Path 5: KQL (Module 4)
60 min	Lab 5: KQL queries
75 min	Learning Path 6: Configure your Microsoft Sentinel environment
30 min	Lab 6: Microsoft Sentinel environment
75 min	Learning Path 7: Connect logs to Microsoft Sentinel
60 min	Lab 7: Connect logs to Microsoft Sentinel
40 min	Learning Path 8: Create detections and perform investigations (Modules 1-3)

LEARNING PATH 6 | Configure your Microsoft Sentinel environment

6 modules

#	MODULE	KEY TOPICS
1	Introduction to Microsoft Sentinel	SIEM and SOAR capabilities, Microsoft Sentinel architecture and when to use it.
2	Create and manage Microsoft Sentinel workspaces	Workspace design (single, multiple, multi-tenant), roles, permissions and data retention.
3	Query logs in Microsoft Sentinel	The Logs page, Microsoft Sentinel tables and querying data with KQL.
4	Use watchlists in Microsoft Sentinel	Create and use watchlists to enrich detections and investigations.
5	Utilize threat intelligence in Microsoft Sentinel	Threat indicators, threat intelligence management and using indicators in queries.
6	Integrate Microsoft Defender XDR with Microsoft Sentinel	Onboard Microsoft Sentinel to the Defender portal and work with the unified security operations platform.

HANDS-ON LAB 6 Configure the Microsoft Sentinel environment: workspace, roles, watchlist and threat indicators.

LEARNING PATH 7 | Connect logs to Microsoft Sentinel

7 modules

#	MODULE	KEY TOPICS
1	Connect data to Microsoft Sentinel using data connectors	Content hub solutions, data connector types and connector health.
2	Connect Microsoft services to Microsoft Sentinel	Microsoft Entra ID, Azure Activity and other Microsoft service connectors.
3	Connect Microsoft Defender XDR to Microsoft Sentinel	Incident and alert synchronisation and streaming raw Defender XDR events.
4	Connect Windows hosts to Microsoft Sentinel	Azure Monitor Agent, data collection rules and Windows security events.

#	MODULE	KEY TOPICS
5	Connect Common Event Format logs to Microsoft Sentinel	CEF via the Azure Monitor Agent and a Linux log forwarder.
6	Connect syslog data sources to Microsoft Sentinel	Syslog collection, data collection rules and parsing syslog with KQL.
7	Connect threat indicators to Microsoft Sentinel	Threat intelligence platform, TAXII and upload API connectors, and viewing indicators.

HANDS-ON LAB 7 Connect logs to Microsoft Sentinel: connect Microsoft services, Defender XDR and Linux hosts using data connectors.

DAY 4

Microsoft Sentinel detections, investigations and threat hunting

TIME	DAILY AGENDA
20 min	Recap of Day 3
75 min	Learning Path 8: Create detections and perform investigations (Modules 4-8)
150 min	Lab 8: Detections and investigations
60 min	Learning Path 9: Perform threat hunting in Microsoft Sentinel
45 min	Lab 9: Threat hunting
15 min	Recap of Day 4
25 min	Course wrap-up and exam readiness

LEARNING PATH 8 | Create detections and perform investigations using Microsoft Sentinel

8 modules

#	MODULE	KEY TOPICS
1	Threat detection with Microsoft Sentinel analytics	Analytics rule types: scheduled, NRT, Microsoft security and Fusion; rule templates and custom rules; entity mapping.
2	Automation in Microsoft Sentinel	Automation rules for incident triage, assignment and closure.
3	Threat response with Microsoft Sentinel playbooks	Logic Apps playbooks, triggers and running playbooks on alerts and incidents.
4	Security incident management in Microsoft Sentinel	Incident triage, investigation graph, entities, comments and closure.
5	Identify threats with Entity behavioral analytics in Microsoft Sentinel	UEBA configuration, entity pages and behavioural anomalies.
6	Data normalization in Microsoft Sentinel	Advanced Security Information Model (ASIM) schemas and parsers.
7	Query, visualize, and monitor data in Microsoft Sentinel	Workbooks, built-in templates and custom visualisations for monitoring.
8	Manage content in Microsoft Sentinel	Content hub, solutions, standalone content and repositories.

HANDS-ON LAB 8 Create detections and perform investigations: analytics rules, automation rules, playbooks, incidents, UEBA, ASIM and workbooks.

LEARNING PATH 9 | Perform threat hunting in Microsoft Sentinel

4 modules

#	MODULE	KEY TOPICS
1	Explain threat hunting concepts in Microsoft Sentinel	Hypothesis-driven hunting, MITRE ATT&CK and the hunting process.

#	MODULE	KEY TOPICS
2	Threat hunting with Microsoft Sentinel	Hunting queries, bookmarks, livestream and promoting findings to incidents.
3	Use Search jobs in Microsoft Sentinel	Search jobs across long-term and archived data, and restoring archived logs.
4	Hunt for threats using notebooks in Microsoft Sentinel	Jupyter notebooks, MSTICPy and advanced hunting with Python.

HANDS-ON LAB 9 Perform threat hunting in Microsoft Sentinel: hunting queries, bookmarks, livestream and search jobs.

Lab environment

- Each learner receives a hosted lab environment with the Microsoft 365 and Azure services needed for all nine labs.
- Security Copilot labs use guided simulations, so no Security Copilot capacity is required.
- Content is aligned to the current Microsoft Learn SC-200T00 course and exam SC-200 skills measured.