

MICROSOFT

SC-200T00: Defend against cyberthreats with Microsoft security operations platform Preparation Training

Delivered from Hacky Security's own curriculum, by instructors who also work our security operations centre. Classroom, online live, or at your office.

INTERMEDIATE

32 HOURS

4 DAYS

MICROSOFT SECURITY ENGINEER

At a glance

COURSE	SC-200T00: Defend against cyberthreats with Microsoft security operations platform	WHAT IS INCLUDED ✓ Instructor-led delivery by practitioners who also work our SOC ✓ Hands-on lab access for the duration of the course ✓ Course materials and lab guides ✓ Hacky Security certificate of completion ✓ Post-course support by email
TRACK	Microsoft	
DOMAIN	Cyber Security	
LEVEL	Intermediate	
DURATION	32 hours (about 4 days)	
DELIVERY	Classroom · Online live · On-site at your office	
LANGUAGE	English	
CLASS SIZE	Small cohorts — everyone gets lab time	

Who this is for

This is an intermediate course. It suits people already working in or moving into Cyber Security who want structured, hands-on preparation rather than a video library. If you are unsure whether the level fits your team, send us the job titles and we will tell you honestly — including if a different course would serve you better.

Course outline

About this course map

Three skill areas, mapped one-for-one to Microsoft's published skills-measured outline for Exam SC-200, and taught in the same order, so nothing on the exam is left uncovered. The exam itself has not been retired or renamed: Microsoft still titles it SC-200: Microsoft Security Operations Analyst, and it still leads to Microsoft Certified: Security Operations Analyst Associate. What has changed is underneath the title — the outline has been restructured around the Microsoft security operations platform, and Microsoft's own instructor-led course for it now runs under the name "Defend against cyberthreats with Microsoft's security operations platform". If you have seen that course title and assumed the certification was renamed, it was not.

Microsoft revises its exams continuously and dates every change. The skills measured for SC-200 are published as of 28 July 2026. The restructuring is substantial. Where the outline once separated Microsoft Sentinel from Microsoft Defender XDR, it now treats them as one platform: Sentinel objectives refer to the Sentinel SIEM and platform, retention is examined across Analytics, Data lake and XDR tiers, and hunting now includes Sentinel Graph, Data lake KQL jobs and notebook connections to the Sentinel MCP Server. Agentic AI investigation, including embedded Microsoft Security Copilot, is now an explicit objective. Each skill area below carries its published weighting range, and we give it classroom time in proportion. Microsoft publishes weightings as ranges rather than fixed percentages, and we have reproduced them as ranges rather than tidying them into single numbers.

SC-200 is an analyst's exam and it is tested the way analyst work is done. Expect scenario-driven items, KQL you have to read and sometimes write, and interactive components where you work in a simulated portal. The teaching is built around that: short explanation, then you configure it, then you make the detection fire and read what the platform tells you.

Skill area 01 — Manage a security operations environment

The heaviest skill area by some distance: building the environment before there is anything to respond to. 40–45% of the exam.

- Email and alert notifications in Microsoft Defender XDR, including incidents, actions, threat analytics, and the tuning, suppression and correlation that keep the queue survivable
- Advanced features, rules settings and custom data collection in Microsoft Defender for Endpoint
- Security policies for Defender for Endpoint, including attack surface reduction rules
- Automated investigation and response, automatic attack disruption, and managing device groups, permissions and automation levels
- Automation rules and playbooks in Microsoft Sentinel, and deciding what should never be automated
- Microsoft Sentinel roles, workbooks, and data retention across the Analytics, Data lake and XDR tiers
- Optimising the Sentinel platform, including working through SOC optimization recommendations rather than filing them
- Data connectors chosen against the source: Windows Security Events via AMA with data collection rules, Windows Event Forwarding, and Syslog and Common Event Format via AMA
- Collecting Azure activity through Azure Policy and resource diagnostic settings, ingesting threat indicators, and creating custom log tables in the workspace
- Detections end to end: custom detection rules built from Advanced Hunting in Defender XDR, scheduled, near-real-time, threat intelligence and machine learning analytics rules in Sentinel, anomalies, and coverage analysed against the MITRE ATT&CK matrix

Skill area 02 — Respond to security incidents

What you actually do when something fires, across every product that can raise an alert. 35–40% of the exam.

- Investigating and remediating threats in Microsoft Defender for Office 365, including automatic attack disruption
- Threats and compromised entities surfaced by Microsoft Purview, and alerts and incidents from Microsoft Defender for Cloud workload protections
- Security risks identified by Microsoft Defender for Cloud Apps
- Compromised identities identified by Microsoft Entra ID, and security alerts from Microsoft Defender for Identity
- Alerts and incidents raised in Microsoft Sentinel, and case management for incidents that outlive a single shift
- Investigating with agentic AI, including embedded Microsoft Security Copilot, and knowing what to verify before accepting a conclusion it hands you
- Complex attacks: multi-stage, multi-domain and lateral movement, reconstructed as one story rather than several alerts
- Responding in Defender for Endpoint: device timelines, live response, collecting investigation packages, and evidence and entity investigation
- Investigating Microsoft 365 activity with Microsoft Purview Audit, Content search in Microsoft Purview eDiscovery, and Microsoft Graph activity logs

Skill area 03 — Perform threat hunting

Going looking before an alert exists, and being able to query at the volume the platform now holds. 20–25% of the exam.

- Identifying the right table for a query, which is most of the difficulty in practice
- Writing Kusto Query Language that returns something you can act on rather than something that merely runs
- Building Advanced Hunting queries in Microsoft Defender XDR
- Interpreting threat analytics, and turning a report into a hunt against your own estate
- Creating hunting graphs, including blast radius
- Analysing relationships between entities using Sentinel Graph
- Creating and monitoring hunting queries in the Microsoft Sentinel platform
- Creating and managing KQL jobs in Data lake, and summary rule tables for querying large volumes efficiently
- Hunting in notebooks, including connecting to the Sentinel MCP Server

Who should take this

Security operations centre analysts, incident responders, threat hunters, and security engineers who own detection content. It also suits infrastructure and identity administrators moving into a defensive role, and managed service staff running Microsoft security tooling for clients.

Microsoft states recommendations rather than requirements — there is no gate on booking the exam. It recommends experience with Microsoft Defender XDR, Microsoft Sentinel, Microsoft Defender for Cloud and Microsoft Entra ID, familiarity with Microsoft 365 and Azure services, and comfort with Kusto Query Language.

In our experience the honest minimum is that you have worked an alert queue somewhere and are prepared to write queries rather than only read dashboards. If your KQL is weak, say so when you enrol — that is the single most common reason delegates struggle, and we send pre-course material for it.

The exam

Exam SC-200 is set and awarded by Microsoft and delivered through Pearson VUE, at a test centre or online with a proctor.

- 100 minutes
- Microsoft does not publish a question count for SC-200, and no range is published — plan by topic coverage rather than by pace
- A score of 700 or greater out of 1000 is required to pass, and the score is scaled rather than a raw percentage
- Proctored, and includes interactive components alongside standard question types
- Available in English, Chinese (Simplified), Chinese (Traditional), French, German, Italian, Japanese, Korean, Portuguese (Brazil) and Spanish
- The certification runs for twelve months and is renewed through a free online assessment on Microsoft Learn rather than by resitting the exam

The exam is purchased separately from Microsoft. We arrange it on your behalf and send you the booking details, and you choose your own exam date.

How we deliver it

Four days, classroom or online live, or at your office for a private group. Every delegate works in their own tenant with Defender XDR and Microsoft Sentinel for the week, so detections you build on day one are the ones you investigate on day three.

Short teaching blocks then hands-on work, with a checkpoint at the end of each skill area and a full-length mock in exam conditions on the final afternoon. A standing block of each day is KQL, written rather than read, because the hunting skill area and a good deal of the response skill area both come down to whether you can query the data.

Mapped to Microsoft's SC-200 skills-measured outline as of 28 July 2026. Taught from Hacky Security's own curriculum by instructors who run security operations for a living. These are our own preparation courses; they are not official Microsoft courseware and we are not a Microsoft Learning Partner.

Sitting the official exam

Exam voucher sold separately. We buy it from the certification body on your behalf and send you the code — you book your own exam date. This course is Hacky Security's own preparation training. The certification itself is awarded by the certification body, not by us.

Investment

FROM

₹69,000

per person

INR	₹69,000 per person
USD	\$829 per person
GBP	£649 per person
AED	AED 2,999 per person

Group, corporate and repeat-cohort pricing on request. Prices are reviewed quarterly and exclude the exam voucher.

Book this course

Tell us how many people, where, and when — we will come back with dates and a quote within one working day.

+91-8091900310 · info@hackysecurity.com

<https://hackysecurity.com/courses/hacky-sc-200-exam-training/>

CHANDIGARH · SHIMLA · DELHI · DUBAI · LONDON

Independent preparation training delivered from Hacky Security's own curriculum. Hacky Security Private Limited is not affiliated with or endorsed by the certification body named in this document. Certification names and codes are the trademarks of their respective owners and are used only to describe what this course prepares you for. Prices, durations and outlines are indicative and may change; the quotation we send you is the binding one. Issued 12 September 2026.