

SC-200: Security Operations Analyst

Hunt, investigate and respond to threats with Microsoft Defender XDR and Microsoft Sentinel, and prepare for the SC-200 exam.

DURATION

4 days · 32 hours

LEVEL

Intermediate

CURRICULUM

13 modules · 11 labs

DELIVERYLive online, Onsite,
Corporate

Course overview

A security operations analyst spends the day separating real threats from noise, investigating what happened and containing it before damage spreads. Microsoft Defender XDR and Microsoft Sentinel are central tools for that work in many organisations. This four-day course trains you to use them the way a working SOC does.

Day one sets up the security operations environment: connecting data sources to Sentinel, configuring Defender XDR settings, and learning Kusto Query Language from first principles, because almost every later task depends on it. Day two configures protections and detections — Defender for Endpoint policies, attack surface reduction, Defender for Office 365 and identity protections, and custom detection and analytics rules.

Day three focuses on incident response: triaging incidents in the unified portal, investigating alerts across email, endpoint, identity and cloud apps, and automating response with Sentinel playbooks and automation rules. Day four covers threat hunting, threat intelligence, workbooks and reporting, followed by exam preparation.

Throughout the course you investigate simulated attacks — phishing, credential theft and lateral movement — so the tools are learned in the order an analyst actually uses them.

The course is aligned to the SC-200 exam. Microsoft security products change frequently and the outline is revised periodically, so check the current skills measured on Microsoft Learn before booking.

Highlights

- 32 hours of live, hands-on SOC sessions
- Simulated attacks investigated end to end
- KQL taught from basics to hunting queries
- Sentinel analytics rules, playbooks and workbooks
- Mapped to the SC-200 skill areas

What's included

- Simulated attack scenarios investigated end to end
- KQL from first principles to hunting queries
- Sentinel data connectors, analytics rules and workbooks
- Automation with playbooks and automation rules
- Defender XDR incident triage and response
- Threat hunting and threat intelligence labs
- 30 days of post-training doubt support

Who this course is for

Who should attend

- SOC analysts and incident responders
- Security engineers working with Microsoft security tools
- IT administrators moving into security operations
- Threat hunters and detection engineers
- SC-900 holders progressing to associate level

Prerequisites

- Understanding of Microsoft 365 and Azure basics
- Familiarity with common attack techniques and security concepts (SC-900 level)
- Basic scripting or query experience helps

Detailed curriculum — 4 days, 32 hours, 13 modules, 11 hands-on labs

Day 1 Security Operations Environment and KQL

8 hours

1.1 Microsoft Sentinel set-up

- Workspace design and roles
- Syslog and CEF ingestion
- Data connectors for Microsoft and third-party sources
- Data retention and cost

LAB Deploy Sentinel and connect Microsoft data sources · 45 min

1.2 Defender XDR environment

- Unified security operations portal
- Device groups and settings
- Role-based access
- Integrating Sentinel with Defender XDR

LAB Configure Defender XDR settings and device groups · 35 min

1.3 Kusto Query Language

- Query structure, where and project
- Joins and unions
- Parsing logs
- Summarise, extend and render
- Working with time and dynamic data

LAB Write KQL queries against sign-in and device logs · 60 min

Day 2 Protections and Detections

8 hours

2.1 Endpoint protection

- Defender for Endpoint onboarding
- Vulnerability management
- Attack surface reduction rules
- Device isolation and live response

LAB Configure ASR rules and investigate a device alert · 50 min

2.2 Email, identity and cloud apps

- Defender for Office 365 policies
- Defender for Cloud Apps policies
- Defender for Identity detections
- Defender for Cloud workload alerts

LAB Investigate a phishing campaign in Defender for Office 365 · 45 min

2.3 Detection engineering

- Scheduled and near-real-time analytics rules
- Entity mapping
- Custom detection rules in Defender XDR
- Tuning false positives

LAB Create and tune an analytics rule · 50 min

Day 3 Incident Response

8 hours

3.1 Triage and investigation

- Incident queue and prioritisation
- Investigation graphs
- Alert correlation and attack stories
- Evidence and entities

LAB Investigate a credential theft and lateral movement incident · 60 min

3.2 Response actions

- Containing users and devices
- Remediation and closure
- Automated investigation and response
- Documenting incidents

LAB Contain a compromised account and device · 35 min

3.3 Automation

- Automation rules
- Enrichment and notification patterns
- Playbooks with Logic Apps

LAB Build a playbook that enriches and notifies on incidents · 45 min

Day 4 Threat Hunting, Reporting and Exam Readiness

8 hours

4.1 Threat hunting

- Hypothesis-driven hunting
- Sentinel hunting queries and bookmarks
- Advanced hunting in Defender XDR
- MITRE ATT&CK mapping

LAB Hunt for persistence techniques with KQL · 50 min

4.2 Threat intelligence

- Threat intelligence indicators
- Watchlists
- Microsoft Defender Threat Intelligence overview

LAB Match indicators against logs with a watchlist · 30 min

4.3 Workbooks and reporting

- Sentinel workbooks
- Copilot for Security overview
- SOC metrics and reporting

4.4 Exam readiness

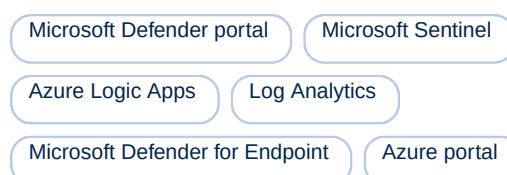
- Exam structure and case studies
- Practice questions with review

Skills and tools

Skills you will build



Tools used in class



Certification exam

This course is aligned to the exam below and prepares you for it. The exam itself is booked and taken with the vendor.

Exam Microsoft Certified: Security Operations Analyst Associate

Exam code SC-200

Duration	100 minutes
Passing score	700 / 1000 (scaled)
Format	Multiple choice, Multiple response, Drag and drop, Case study
Delivery	Online proctored, Test centre
Validity	1 year (free online renewal assessment)
Official page	https://learn.microsoft.com/credentials/certifications/exams/sc-200/

Exam skill areas covered

Manage a secure operations environment

Manage security incidents

Exam details are pending verification. Confirm the current exam code, format and fee on the official vendor page before booking.

Frequently asked questions

Do I need to know KQL before joining?

No. KQL is taught from first principles on Day 1 and used throughout the course.

Are the attack scenarios realistic?

Yes. Labs use simulated phishing, credential theft and lateral movement data so you investigate the kind of incidents a SOC sees.

Is SC-200 suitable for freshers?

It is best after SC-900 or some IT experience. Complete beginners should start with SC-900 or a security fundamentals course.

What happens if Microsoft updates the SC-200 exam?

We map the curriculum to the current published skills outline and revise it when Microsoft changes the exam. Always check the latest outline on Microsoft Learn before booking.

Do you run weekend batches?

Yes. Weekend batches cover the same 32 hours across consecutive Saturdays and Sundays, with timings in IST that also suit learners in the Gulf.

Can you run a private batch for our team?

Yes. We run private online or onsite batches for corporate teams, and we can weight the labs towards your SOC's tools and use cases. Request a corporate quote with your team size and preferred dates.

Book a batch or talk to an advisor

Course page: aceskillsconsulting.com/course/sc-200-security-operations-analyst · Email: info@aceskillsconsulting.com

Chennai office

Guindy, Chennai, Tamil Nadu

Delhi office

B-95, Old Post Office Street, Shakarpur
New Delhi 110092
Office: 98180 12523

Microsoft, Azure, Microsoft 365, Power BI and Microsoft Entra are trademarks of the Microsoft group of companies. All product names, logos, brands, trademarks and registered trademarks are the property of their respective owners. Ace Skills Consulting is an independent training provider; unless explicitly stated, it is not affiliated with, endorsed by or sponsored by any vendor mentioned on this site. Exam details are provided for guidance and may change — always confirm on the vendor's official website. Curriculum generated on 23 Oct 2026; topics and order may be adjusted by the trainer to suit each batch.