



COURSE SYLLABUS

Microsoft Certified: Security Operations Analyst Associate

Prepare for exam SC-200 by learning to detect, investigate, and respond to threats and hunt with KQL in Microsoft Defender XDR and Microsoft Sentinel.

\$2,395 per person, including the SC-200 exam voucher

22 course hours (on-demand video and labs) plus 2 hours of coaching

On-demand asynchronous training with online support, plus 2 hours of coaching.

Microsoft Certified: Security Operations Analyst Associate

Prepare for exam SC-200 by learning to detect, investigate, and respond to threats and hunt with KQL in Microsoft Defender XDR and Microsoft Sentinel.

Credential type	Certificate, issued by We Can Code IT
Clock hours	24 (22 course hours plus 2 hours of coaching)
Price	\$2,395 per person, including the SC-200 exam voucher
Time	22 course hours (on-demand video and labs) plus 2 hours of coaching
Delivery	On-demand asynchronous training with online support, plus 2 hours of coaching.
Exam	Exam SC-200: Microsoft Security Operations Analyst (Microsoft Certified: Security Operations Analyst Associate) (SC-200). This course prepares you for exam SC-200, and one exam attempt voucher is included. KQL fluency and hands-on time in Defender and Sentinel are needed beyond the course hours, so most learners need additional self-study and lab time plus the free Microsoft practice assessment. Passing is not guaranteed. Microsoft is updating the English exam on October 21, 2026 with a minor change to Sentinel data ingestion.
Who it is for	This course is for security operations center analysts, incident responders, and IT security staff who triage alerts, investigate incidents, and hunt for threats using Microsoft security tools.
Prerequisites	Familiarity with Microsoft 365 and Azure cloud services; General knowledge of Windows and Linux operating systems; Basic awareness of Microsoft security, compliance, and identity tools
Requirements	A modern web browser for the Microsoft Defender portal and Microsoft Sentinel; An Azure subscription for Microsoft Sentinel labs; Sentinel data ingestion is paid and billed to the subscription after any free trial period; A time-limited Microsoft 365 E5 or Defender trial tenant, or paid Microsoft 365 E5 or Defender licensing, for Defender XDR labs

About this course

This course covers the three skill areas Microsoft measures on exam SC-200: managing a security operations environment, responding to incidents, and threat hunting. You configure Microsoft Defender XDR and Microsoft Sentinel, build detections and automation, work real incident scenarios, and write KQL hunting queries. Each module ends with a lab in a trial environment.

What you will be able to do

- You will be able to configure Microsoft Defender XDR and Defender for Endpoint settings for your organization.
- You will be able to set up Microsoft Sentinel, including roles, retention, and data connectors.
- You will be able to build analytics rules, automation rules, and playbooks that respond to threats.
- You will be able to investigate and resolve an incident in Defender XDR, including with Security Copilot.
- You will be able to write KQL queries to hunt for threats across Sentinel and Defender data.

Syllabus

Module	Hours
1. SOC orientation and Defender XDR and Defender for Endpoint configuration Security operations roles, Microsoft Defender XDR portal, Defender for Endpoint onboarding, Attack surface reduction settings. Lab: You onboard a test device to Defender for Endpoint and configure alert and attack surface reduction settings.	4 h
2. Microsoft Sentinel setup, roles, retention, and data ingestion Sentinel workspace design, Roles and permissions, Data retention, Data connectors, Sentinel data lake. Lab: You create a Sentinel workspace, connect Microsoft 365 and Entra ID data, and set retention.	3.5 h
3. Detections, analytics rules, automation rules, and playbooks Scheduled analytics rules, Custom detections, Automation rules, Playbooks with Logic Apps. Lab: You build an analytics rule for suspicious sign-ins and an automation rule that runs a playbook on each new incident.	3.5 h
4. Responding to incidents in Defender XDR, including Security Copilot Incident queue and triage, Alert investigation, Remediation actions, Security Copilot in incident response. Lab: You triage and resolve a simulated phishing incident in Defender XDR and summarize it with Security Copilot.	4 h
5. Endpoint investigations and Microsoft 365 activity investigations Device timeline, Device isolation and response actions, Audit log investigation, Identity activity. Lab: You investigate a compromised device timeline, isolate the device, and trace related Microsoft 365 activity.	3 h
6. Threat hunting with KQL, Sentinel data lake, and exam readiness KQL fundamentals, Advanced hunting, Hunting in Sentinel data lake, SC-200 practice assessment review. Lab: You write KQL hunting queries to find a planted threat and complete the free Microsoft practice assessment.	4 h

Coaching sessions

2 h

2 hours of coaching. One-on-one or small-group coaching, scheduled with your coach.

Live online or in-person sessions are available for an additional fee. Email admissions@wecancodeit.org for details.

Provider

We Can Code IT, LLC, 26300 Cedar Rd, Suite 1105, Beachwood, OH 44122. Registered with the Ohio State Board of Career Colleges and Schools, Registration No. 15-03-2064T. Contact: admissions@wecancodeit.org. Syllabus version 2026-10-10.