Study guide for Exam SC-200: Microsoft Security Operations Analyst

Purpose of this document

This study guide should help you understand what to expect on the exam and includes a summary of the topics the exam might cover and links to additional resources. The information and materials in this document should help you focus your studies as you prepare for the exam.

Useful links	Description
Review the skills measured as of May 5, 2023	This list represents the skills measured AFTER the date provided. Study this list if you plan to take the exam AFTER that date.
Review the skills measured prior to May 5, 2023	Study this list of skills if you take your exam PRIOR to the date provided.
Change log	You can go directly to the change log if you want to see the changes that will be made on the date provided.
How to earn the certification	Some certifications only require passing one exam, while others require passing multiple exams.
Certification renewal	Microsoft associate, expert, and specialty certifications expire annually. You can renew by passing a **free** online assessment on Microsoft Learn.
Your Microsoft Learn profile	Connecting your certification profile to Learn allows you to schedule and renew exams and share and print certificates.
Passing score	A score of 700 or greater is required to pass.
Exam sandbox	You can explore the exam environment by visiting our exam sandbox.
Request accommodations	If you use assistive devices, require extra time, or need modification to any part of the exam experience, you can request an accommodation.

Useful links	Description
Take a practice test	Are you ready to take the exam or do you need to study a bit more?

Updates to the exam

Our exams are updated periodically to reflect skills that are required to perform a role. We have included two versions of the Skills Measured objectives depending on when you are taking the exam.

We always update the English language version of the exam first. Some exams are localized into other languages, and those are updated approximately eight weeks after the English version is updated. While Microsoft makes every effort to update localized versions as noted, there may be times when the localized versions of an exam are not updated on this schedule. Other available languages are listed in the **Schedule Exam** section of the **Exam Details** webpage. If the exam isn't available in your preferred language, you can request an additional 30 minutes to complete the exam.

Note

The bullets that follow each of the skills measured are intended to illustrate how we are assessing that skill. Related topics may be covered in the exam.

Note

Most questions cover features that are general availability (GA). The exam may contain questions on Preview features if those features are commonly used.

Skills measured as of May 5, 2023

Audience profile

Microsoft security operations analysts 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. They perform triage, incident response, vulnerability management, threat hunting, and cyber threat intelligence analysis.

Microsoft security operations analysts monitor, identify, investigate, and respond to threats in multicloud environments by using Microsoft Sentinel, Microsoft Defender for Cloud, Microsoft 365 Defender, and third-party security solutions. Microsoft security operations analysts collaborate with business stakeholders, architects, identity administrators, Azure administrators, and endpoint administrators to secure IT systems for the organization.

Candidates should be familiar with Microsoft 365, Azure cloud services, and Windows and Linux operating systems.

- Mitigate threats by using Microsoft 365 Defender (25–30%)
- Mitigate threats by using Defender for Cloud (15–20%)
- Mitigate threats by using Microsoft Sentinel (50–55%)

Mitigate threats by using Microsoft 365 Defender (25–30%)

Mitigate threats to the Microsoft 365 environment by using Microsoft 365 Defender

- Investigate, respond, and remediate threats to Microsoft Teams, SharePoint Online, and OneDrive
- Investigate, respond, and remediate threats to email by using Microsoft Defender for Office 365
- Investigate and respond to alerts generated from data loss prevention (DLP) policies
- Investigate and respond to alerts generated from insider risk policies
- Discover and manage apps by using Microsoft Defender for Cloud Apps
- Identify, investigate, and remediate security risks by using Defender for Cloud Apps

Mitigate endpoint threats by using Microsoft Defender for Endpoint

- Manage data retention, alert notification, and advanced features
- Recommend attack surface reduction (ASR) for devices
- Respond to incidents and alerts
- Configure and manage device groups
- Identify devices at risk by using the Microsoft Defender Vulnerability Management
- Manage endpoint threat indicators
- Identify unmanaged devices by using device discovery

Mitigate identity threats

- Mitigate security risks related to events for Microsoft Azure Active Directory (Azure AD), part of Microsoft Entra
- Mitigate security risks related to Azure AD Identity Protection events
- Mitigate security risks related to Active Directory Domain Services (AD DS) by using Microsoft Defender for Identity

Manage extended detection and response (XDR) in Microsoft 365 Defender

- Manage incidents and automated investigations in the Microsoft 365 Defender portal
- Manage actions and submissions in the Microsoft 365 Defender portal
- Identify threats by using KQL
- Identify and remediate security risks by using Microsoft Secure Score
- Analyze threat analytics in the Microsoft 365 Defender portal
- Configure and manage custom detections and alerts

Investigate threats by using audit features in Microsoft 365 Defender and Microsoft Purview

- Perform threat hunting by using UnifiedAuditLog
- Perform threat hunting by using Content Search

Mitigate threats by using Defender for Cloud (15–20%)

Implement and maintain cloud security posture management

- Assign and manage regulatory compliance policies, including Microsoft cloud security benchmark (MCSB)
- Improve the Defender for Cloud secure score by remediating recommendations
- Configure plans and agents for Microsoft Defender for Servers
- Configure and manage Microsoft Defender for DevOps

Configure environment settings in Defender for Cloud

- Plan and configure Defender for Cloud settings, including selecting target subscriptions and workspaces
- Configure Defender for Cloud roles
- Assess and recommend cloud workload protection
- Enable Microsoft Defender plans for Defender for Cloud
- Configure automated onboarding for Azure resources
- Connect compute resources by using Azure Arc
- Connect multicloud resources by using Environment settings

Respond to alerts and incidents in Defender for Cloud

- Set up email notifications
- Create and manage alert suppression rules
- Design and configure workflow automation in Defender for Cloud
- Remediate alerts and incidents by using Defender for Cloud recommendations
- Manage security alerts and incidents
- Analyze Defender for Cloud threat intelligence reports

Mitigate threats by using Microsoft Sentinel (50–55%)

Design and configure a Microsoft Sentinel workspace

- Plan a Microsoft Sentinel workspace
- Configure Microsoft Sentinel roles
- Design and configure Microsoft Sentinel data storage, including log types and log retention

Plan and implement the use of data connectors for ingestion of data sources in Microsoft Sentinel

- Identify data sources to be ingested for Microsoft Sentinel
- Configure and use Microsoft Sentinel connectors for Azure resources, including Azure Policy and diagnostic settings
- Configure Microsoft Sentinel connectors for Microsoft 365 Defender and Defender for Cloud
- Design and configure Syslog and Common Event Format (CEF) event collections

- Design and configure Windows security event collections
- Configure threat intelligence connectors
- Create custom log tables in the workspace to store ingested data

Manage Microsoft Sentinel analytics rules

- Configure the Fusion rule
- Configure Microsoft security analytics rules
- Configure built-in scheduled query rules
- Configure custom scheduled query rules
- Configure near-real-time (NRT) query rules
- Manage analytics rules from Content hub
- Manage and use watchlists
- Manage and use threat indicators

Perform data classification and normalization

- Classify and analyze data by using entities
- Query Microsoft Sentinel data by using Advanced Security Information Model (ASIM) parsers
- Develop and manage ASIM parsers

Configure security orchestration automated response (SOAR) in Microsoft Sentinel

- Create and configure automation rules
- Create and configure Microsoft Sentinel playbooks
- Configure analytic rules to trigger automation rules
- Trigger playbooks manually from alerts and incidents

Manage Microsoft Sentinel incidents

- Create an incident
- Triage incidents in Microsoft Sentinel
- Investigate incidents in Microsoft Sentinel
- Respond to incidents in Microsoft Sentinel
- Investigate multi-workspace incidents

Use Microsoft Sentinel workbooks to analyze and interpret data

- Activate and customize Microsoft Sentinel workbook templates
- Create custom workbooks
- Configure advanced visualizations

Hunt for threats by using Microsoft Sentinel

- Analyze attack vector coverage by using MITRE ATT&CK in Microsoft Sentinel
- Customize content gallery hunting queries

- Create custom hunting queries
- Use hunting bookmarks for data investigations
- Monitor hunting queries by using Livestream
- Retrieve and manage archived log data
- Create and manage search jobs

Manage threats by using entity behavior analytics

- Configure entity behavior settings
- Investigate threats by using entity pages
- Configure anomaly detection analytics rules

Study resources

We recommend that you train and get hands-on experience before you take the exam. We offer self-study options and classroom training as well as links to documentation, community sites, and videos.

Study resources	Links to learning and documentation
Get trained	Choose from self-paced learning paths and modules or take an instructor-led course
Find documentation	Microsoft security documentation Microsoft 365 Defender documentation Microsoft Defender for Cloud documentation Microsoft Sentinel documentation
Ask a question	Microsoft Q&A | Microsoft Docs
Get community support	Security, compliance, and identity community hub
Follow Microsoft Learn	Microsoft Learn - Microsoft Tech Community
Find a video	Exam Readiness Zone Browse other Microsoft Learn shows

Change log

Key to understanding the table: The topic groups (also known as functional groups) are in bold typeface followed by the objectives within each group. The table is a comparison between the two versions of the exam skills measured and the third column describes the extent of the changes.

Skill area prior to May 5, 2023	Skill area as of May 5, 2023	Changes
Audience profile		Major
Mitigate threats using Microsoft 365 Defender	**Mitigate threats by using Microsoft 365 Defender**	No change
Mitigate threats to the productivity environment by using Microsoft 365 Defender	Mitigate threats to the Microsoft 365 environment by using Microsoft 365 Defender	Minor
Mitigate endpoint threats by using Microsoft Defender for Endpoint	Mitigate endpoint threats by using Microsoft Defender for Endpoint	Major
Mitigate identity threats	Mitigate identity threats	Minor
Manage extended detection and response (XDR) in Microsoft 365 Defender	Manage extended detection and response (XDR) in Microsoft 365 Defender	Minor
	Investigate threats by using audit features in Microsoft 365 Defender and Microsoft Purview	New
Mitigate threats using Microsoft Defender for Cloud	**Mitigate threats by using Microsoft Defender for Cloud**	No change
Implement and maintain cloud security posture management and workload protection	Implement and maintain cloud security posture management	Major
Plan and implement the use of data connectors for ingestion of data sources in Microsoft Defender for Cloud	Configure environment settings in Microsoft Defender for Cloud	Major
Configure and respond to alerts and incidents in Microsoft Defender for Cloud	Respond to alerts and incidents in Microsoft Defender for Cloud	Major
Mitigate threats using Microsoft Sentinel	**Mitigate threats by using Microsoft Sentinel**	No change
Design and configure a Microsoft Sentinel workspace	Design and configure a Microsoft Sentinel workspace	Minor
Plan and implement the use of data connectors for ingestion of data sources in Microsoft Sentinel	Plan and implement the use of data connectors for ingestion of data sources in Microsoft Sentinel	Minor
Manage Microsoft Sentinel analytics rules	Manage Microsoft Sentinel analytics rules	Major

Skill area prior to May 5, 2023	Skill area as of May 5, 2023	Changes
Perform data classification and normalization	Perform data classification and normalization	Minor
Configure Security Orchestration, Automation, and Response (SOAR) in Microsoft Sentinel	Configure Security Orchestration, Automation, and Response (SOAR) in Microsoft Sentinel	Major
Manage Microsoft Sentinel incidents	Manage Microsoft Sentinel incidents	Minor
Use Microsoft Sentinel workbooks to analyze and interpret data	Use Microsoft Sentinel workbooks to analyze and interpret data	Major
Hunt for threats using Microsoft Sentinel	Hunt for threats by using Microsoft Sentinel	Major
	Manage threats by using entity behavior analytics	New

Skills measured prior to May 5, 2023

Audience profile

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 for Cloud, Microsoft 365 Defender, 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.

Candidates for this role should be familiar with attack vectors, cyberthreats, incident management, and Kusto Query Language (KQL). Candidates should also be familiar with Microsoft 365 and Azure services.

- Mitigate threats using Microsoft 365 Defender (25–30%)
- Mitigate threats using Microsoft Defender for Cloud (20–25%)
- Mitigate threats using Microsoft Sentinel (50–55%)

Mitigate threats using Microsoft 365 Defender (25–30%)

Mitigate threats to the productivity environment by using Microsoft 365 Defender

- Investigate, respond, and remediate threats to Microsoft Teams, SharePoint, and OneDrive
- Investigate, respond, and remediate threats to email by using Microsoft Defender for Office 365
- Investigate and respond to alerts generated from Data Loss Prevention policies
- Investigate and respond to alerts generated from insider risk policies
- Identify, investigate, and remediate security risks by using Microsoft Defender for Cloud Apps
- Configure Microsoft Defender for Cloud Apps to generate alerts and reports to detect threats

Mitigate endpoint threats by using Microsoft Defender for Endpoint

- Manage data retention, alert notification, and advanced features
- Recommend security baselines for devices
- Respond to incidents and alerts
- Manage automated investigations and remediations
- Assess and recommend endpoint configurations to reduce and remediate vulnerabilities by using the Microsoft's threat and vulnerability management solution
- Manage endpoint threat indicators

Mitigate identity threats

- Identify and remediate security risks related to events for Microsoft Azure Active Directory (Azure AD), part of Microsoft Entra
- Identify and remediate security risks related to Azure AD Identity Protection events
- Identify and remediate security risks related to Azure AD Conditional Access events
- Identify and remediate security risks related to Active Directory Domain Services using Microsoft Defender for Identity

Manage extended detection and response (XDR) in Microsoft 365 Defender

- Manage incidents across Microsoft 365 Defender products
- Manage investigation and remediation actions in the Action Center
- Perform threat hunting
- Identify and remediate security risks using Microsoft Secure Score
- Analyze threat analytics
- Configure and manage custom detections and alerts

Mitigate threats using Microsoft Defender for Cloud (20–25%)

Implement and maintain cloud security posture management and workload protection

- Plan and configure Microsoft Defender for Cloud settings, including selecting target subscriptions and workspaces
- Configure Microsoft Defender for Cloud roles
- Assess and recommend cloud workload protection
- Identify and remediate security risks using the Microsoft Defender for Cloud Secure Score
- Manage policies for regulatory compliance
- Review and remediate security recommendations

Plan and implement the use of data connectors for ingestion of data sources in Microsoft Defender for Cloud

- Identify data sources to be ingested for Microsoft Defender for Cloud
- Configure automated onboarding for Azure resources
- Connect multi-cloud and on-premises resources
- Configure data collections

Configure and respond to alerts and incidents in Microsoft Defender for Cloud

- Validate alert configuration
- Set up email notifications
- Create and manage alert suppression rules
- Design and configure workflow automation in Microsoft Defender for Cloud
- Remediate alerts and incidents by using Microsoft Defender for Cloud recommendations
- Manage security alerts and incidents
- Analyze Microsoft Defender for Cloud threat intelligence reports
- Manage user data discovered during an investigation

Mitigate threats using Microsoft Sentinel (50–55%)

Design and configure a Microsoft Sentinel workspace

- Plan a Microsoft Sentinel workspace
- Configure Microsoft Sentinel roles
- Design and configure Microsoft Sentinel data storage
- Implement and use Content hub, repositories, and community resources

Plan and implement the use of data connectors for ingestion of data sources in Microsoft Sentinel

- Identify data sources to be ingested for Microsoft Sentinel
- Identify the prerequisites for a Microsoft Sentinel data connector

- Configure and use Microsoft Sentinel data connectors
- Configure Microsoft Sentinel data connectors by using Azure Policy
- Configure Microsoft Sentinel connectors for Microsoft 365 Defender and Microsoft Defender for Cloud
- Design and configure Syslog and CEF event collections
- Design and configure Windows Security event collections
- Configure custom threat intelligence connectors

Manage Microsoft Sentinel analytics rules

- Design and configure analytics rules
- Activate Microsoft security analytics rules
- Configure built-in scheduled queries
- Configure custom scheduled queries
- Define incident creation logic
- Manage and use watchlists
- Manage and use threat indicators

Perform data classification and normalization

- Classify and analyze data by using entities
- Create custom logs in Azure Log Analytics to store custom data
- Query Microsoft Sentinel data by using Advanced SIEM Information Model (ASIM) parsers
- Develop and manage ASIM parsers

Configure Security Orchestration, Automation, and Response (SOAR) in Microsoft Sentinel

- Configure automation rules
- Create and configure Microsoft Sentinel playbooks
- Configure alerts and incidents to trigger automation
- Use automation to remediate threats
- Use automation to manage incidents

Manage Microsoft Sentinel incidents

- Triage incidents in Microsoft Sentinel
- Investigate incidents in Microsoft Sentinel
- Respond to incidents in Microsoft Sentinel
- Investigate multi-workspace incidents
- Identify advanced threats with User and Entity Behavior Analytics (UEBA)

Use Microsoft Sentinel workbooks to analyze and interpret data

- Activate and customize Microsoft Sentinel workbook templates
- Create custom workbooks

- Configure advanced visualizations
- View and analyze Microsoft Sentinel data using workbooks
- Track incident metrics using the security operations efficiency workbook

Hunt for threats using Microsoft Sentinel

- Create custom hunting queries
- Run hunting queries manually
- Monitor hunting queries by using Livestream
- Configure and use MSTICPy in notebooks
- Perform hunting by using notebooks
- Track query results with bookmarks
- Use hunting bookmarks for data investigations
- Convert a hunting query to an analytical rule