Exam SC-200: Microsoft Security Operations Analyst – Skills Measured

The English language version of this exam was updated on January 28, 2022.

Following the current exam guide, we have included a version of the exam guide with Track Changes set to "On," showing the changes that were made to the exam on that date.

NOTE: Passing score: 700. Learn more about exam scores.

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.

Skills Measured

NOTE: The bullets that follow each of the skills measured are intended to illustrate how we are assessing that skill. This list Is NOT definitive or exhaustive.

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

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

Detect, investigate, respond, and remediate threats to the productivity environment by using Microsoft Defender for Office 365

- detect, investigate, respond, and remediate threats to Microsoft Teams, SharePoint, and OneDrive
- detect, investigate, respond, remediate threats to email by using Defender for Office 365
- manage data loss prevention policy alerts
- assess and recommend sensitivity labels
- assess and recommend insider risk policies

Detect, investigate, respond, and remediate endpoint threats by using Microsoft Defender for Endpoint

- manage data retention, alert notification, and advanced features
- configure device attack surface reduction rules
- configure and manage custom detections and alerts
- 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 Microsoft Defender for Endpoint threat indicators
- analyze Microsoft Defender for Endpoint threat analytics

Detect, investigate, respond, and remediate identity threats

- identify and remediate security risks related to sign-in risk policies
- identify and remediate security risks related to Conditional Access events
- identify and remediate security risks related to Azure Active Directory
- identify and remediate security risks using Secure Score
- identify, investigate, and remediate security risks related to privileged identities
- configure detection alerts in Azure AD Identity Protection
- identify and remediate security risks related to Active Directory Domain Services using Microsoft Defender for Identity

Detect, investigate, respond, and remediate application threats

- identify, investigate, and remediate security risks by using Microsoft Cloud Application Security (MCAS)
- configure MCAS to generate alerts and reports to detect threats

Manage cross-domain investigations in Microsoft 365 Defender portal

- manage incidents across Microsoft 365 Defender products
- manage actions pending approval across products

- perform advanced threat hunting

Mitigate threats using Microsoft Defender for Cloud (25-30%)

Design and configure a Microsoft Defender for Cloud implementation

- plan and configure Microsoft Defender for Cloud settings, including selecting target subscriptions and workspace
- configure Microsoft Defender for Cloud roles
- configure data retention policies
- assess and recommend cloud workload protection

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 on-premises computers
- connect AWS cloud resources
- connect GCP cloud resources
- configure data collection

Manage Microsoft Defender for Cloud alert rules

- validate alert configuration
- setup email notifications
- create and manage alert suppression rules

Configure automation and remediation

- configure automated responses in Microsoft Defender for Cloud
- design and configure workflow automation in Microsoft Defender for Cloud
- remediate incidents by using Microsoft Defender for Cloud recommendations
- create an automatic response using an Azure Resource Manager template

Investigate Microsoft Defender for Cloud alerts and incidents

- describe alert types for Azure workloads
- manage security alerts
- manage security incidents
- analyze Microsoft Defender for Cloud threat intelligence
- respond to Microsoft Defender Cloud for Key Vault alerts
- manage user data discovered during an investigation

Mitigate threats using Microsoft Sentinel (40-45%)

Design and configure a Microsoft Sentinel workspace

- plan a Microsoft Sentinel workspace

- configure Microsoft Sentinel roles
- design Microsoft Sentinel data storage
- configure security settings and access for Microsoft Sentinel

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 data connector
- configure and use Microsoft Sentinel data connectors
- configure data connectors by using Azure Policy
- design and configure Syslog and CEF event collections
- design and Configure Windows Security events collections
- configure custom threat intelligence connectors
- create custom logs in Azure Log Analytics to store custom data

Manage Microsoft Sentinel analytics rules

- design and configure analytics rules
- create custom analytics rules to detect threats
- activate Microsoft security analytics rules
- configure connector provided scheduled queries
- configure custom scheduled queries
- define incident creation logic

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

- create Microsoft Sentinel playbooks
- configure rules and incidents to trigger playbooks
- use playbooks to remediate threats
- use playbooks to manage incidents
- use playbooks across Microsoft Defender solutions

Manage Microsoft Sentinel Incidents

- investigate incidents in Microsoft Sentinel
- triage 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
- perform advanced hunting with notebooks
- track query results with bookmarks
- use hunting bookmarks for data investigations
- convert a hunting query to an analytical

The following exam guide below shows the changes that were implemented on January 28, 2022 to the English language version of this exam.

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 ~~Azure~~ Sentinel, ~~Azure~~ 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.

Skills Measured

NOTE: The bullets that follow each of the skills measured are intended to illustrate how we are assessing that skill. This list is NOT definitive or exhaustive.

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

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

Detect, investigate, respond, and remediate threats to the productivity environment by using Microsoft Defender for Office 365

- detect, investigate, respond, and remediate threats to Microsoft Teams, SharePoint, and OneDrive
- detect, investigate, respond, remediate threats to email by using Defender for Office 365
- manage data loss prevention policy alerts
- assess and recommend sensitivity labels
- assess and recommend insider risk policies

Detect, investigate, respond, and remediate endpoint threats by using Microsoft Defender for Endpoint

- manage data retention, alert notification, and advanced features
- configure device attack surface reduction rules
- configure and manage custom detections and alerts
- 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 Microsoft Defender for Endpoint threat indicators
- analyze Microsoft Defender for Endpoint threat analytics

Detect, investigate, respond, and remediate identity threats

- identify and remediate security risks related to sign-in risk policies
- identify and remediate security risks related to Conditional Access events
- identify and remediate security risks related to Azure Active Directory
- identify and remediate security risks using Secure Score
- identify, investigate, and remediate security risks related to privileged identities
- configure detection alerts in Azure AD Identity Protection
- identify and remediate security risks related to Active Directory Domain Services using Microsoft Defender for Identity

Detect, investigate, respond, and remediate application threats

- identify, investigate, and remediate security risks by using Microsoft Cloud Application Security (MCAS)
- configure MCAS to generate alerts and reports to detect threats

Manage cross-domain investigations in Microsoft 365 Defender portal

- manage incidents across Microsoft 365 Defender products
- manage actions pending approval across products

- perform advanced threat hunting

Mitigate threats using ~~Azure~~ Microsoft Defender for Cloud (25-30%)

Design and configure a~~n Azure Defender~~Microsoft Defender for Cloud implementation

- plan and configure ~~Azure Defender~~Microsoft Defender for Cloud settings, including selecting target subscriptions and workspace
- configure ~~Azure Defender~~Microsoft Defender for Cloud roles
- configure data retention policies
- assess and recommend cloud workload protection

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

- identify data sources to be ingested for ~~Azure Defender~~Microsoft Defender for Cloud
- configure automated onboarding for Azure resources
- connect on-premises computers
- connect AWS cloud resources
- connect GCP cloud resources
- configure data collection

Manage ~~Azure Defender~~Microsoft Defender for Cloud alert rules

- validate alert configuration
- setup email notifications
- create and manage alert suppression rules

Configure automation and remediation

- configure automated responses in ~~Azure Security Center~~Microsoft Defender for Cloud
- design and configure ~~playbook~~ workflow automation in ~~Azure Security Center~~Microsoft Defender for Cloud
- remediate incidents by using ~~Azure Security Center~~Microsoft Defender for Cloud recommendations
- create an automatic response using an Azure Resource Manager template

Investigate ~~Azure Defender~~Microsoft Defender for Cloud alerts and incidents

- describe alert types for Azure workloads
- manage security alerts
- manage security incidents
- analyze ~~Azure Security Center~~Microsoft Defender for Cloud threat intelligence
- respond to ~~Azure Defender~~Microsoft Defender Cloud for Key Vault alerts
- manage user data discovered during an investigation

Mitigate threats using ~~Azure Sentinel~~Microsoft Sentinel (40-45%)

Design and configure a~~n~~ ~~Azure Sentinel~~Microsoft Sentinel workspace

- plan a~~n~~ ~~Azure Sentinel~~Microsoft Sentinel workspace
- configure ~~Azure Sentinel~~Microsoft Sentinel roles
- design ~~Azure Sentinel~~Microsoft Sentinel data storage
- configure security settings and access for ~~Azure~~ Microsoft Sentinel ~~service security~~

Plan and Implement the use of data connectors for ingestion of data sources in ~~Azure Sentinel~~Microsoft Sentinel

- identify data sources to be ingested for ~~Azure Sentinel~~Microsoft Sentinel
- identify the prerequisites for a data connector
- configure and use ~~Azure Sentinel~~Microsoft Sentinel data connectors
- configure data connectors by using Azure Policy
- design and configure Syslog and CEF event collections
- design and Configure Windows Security events collections
- configure custom threat intelligence connectors
- create custom logs in Azure Log Analytics to store custom data

Manage ~~Azure Sentinel~~Microsoft Sentinel analytics rules

- design and configure analytics rules
- create custom analytics rules to detect threats
- activate Microsoft security analytics rules
- configure connector provided scheduled queries
- configure custom scheduled queries
- define incident creation logic

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

- create ~~Azure~~ Microsoft Sentinel playbooks
- configure rules and incidents to trigger playbooks
- use playbooks to remediate threats
- use playbooks to manage incidents
- use playbooks across Microsoft Defender solutions

Manage ~~Azure Sentinel~~Microsoft Sentinel Incidents

- investigate incidents in ~~Azure Sentinel~~Microsoft Sentinel
- triage incidents in ~~Azure Sentinel~~Microsoft Sentinel
- respond to incidents in ~~Azure Sentinel~~Microsoft Sentinel
- investigate multi-workspace incidents
- identify advanced threats with User and Entity Behavior Analytics (UEBA)

Use ~~Azure Sentinel~~Microsoft Sentinel workbooks to analyze and interpret data

- activate and customize ~~Azure Sentinel~~Microsoft Sentinel workbook templates

- create custom workbooks
- configure advanced visualizations
- view and analyze ~~Azure ~~Microsoft Sentinel data using workbooks
- track incident metrics using the security operations efficiency workbook

Hunt for threats using ~~the Azure Sentinel~~Microsoft Sentinel ~~portal~~

- create custom hunting queries
- run hunting queries manually
- monitor hunting queries by using Livestream
- perform advanced hunting with notebooks
- track query results with bookmarks
- use hunting bookmarks for data investigations
- convert a hunting query to an analytical