

PRACTICE QUESTIONS

Microsoft

SC-200

Microsoft Security Operations Analyst Associate

SHARED BY [u/sc200_notes](#) on aiexamcerts

EDITION	Free Set 2
QUESTIONS	10
SHARED	October 15, 2026
EXAM	Microsoft SC-200, Microsoft Security Operations Analyst Associate

Shared by [u/sc200_notes](#) on aiexamcerts

10 practice questions for the Microsoft SC-200 exam, Microsoft Security Operations Analyst Associate, each followed by its answer and a short explanation. More free sets and the full practice exam:

www.aiexamcerts.com/microsoft/sc-200. Spotted a mistake? Email support@aiexamcerts.com with the exam code SC-200 and the question number.

1. Which Defender for Endpoint feature lets an analyst allow or block a file hash, IP address or URL across the organization, with an optional expiration?

 - A Custom indicators
 - B Automated investigation
 - C Device groups
 - D Exclusion rules

Answer: A

Custom indicators let analysts allow or block file hashes, IP addresses, URLs, and domains, and they can be given an expiration. Automated investigation analyzes alerts after they fire, so it does not create blocklists. Exclusion rules are tempting because they change detection, but they let activity bypass scanning rather than block it.

2. Defender for Office 365 Safe Attachments protects files stored in SharePoint, OneDrive and Teams as well as email attachments.

 - A True
 - B False

Answer: A (True)

Safe Attachments can scan files in SharePoint, OneDrive and Teams, not just email attachments, so the protection is configured as its own policy scope. Limiting it to mail is a common assumption that leaves collaboration files exposed. The sandbox detonation process applies to these files as well.

3. A user's credentials are suspected to be compromised and an attacker may hold active sessions. Which Entra ID action signs the user out of existing sessions so they must authenticate again?

 - A Require MFA re-registration
 - B Revoke sessions
 - C Remove the user from all security groups
 - D Disable the user's mailbox

Answer: B

Revoke sessions invalidates refresh tokens so an attacker's existing sessions stop working and the user must sign in again. Requiring MFA re-registration is tempting after a compromise, but it does not end sessions that already exist. Removing group memberships changes future authorization but does not invalidate the refresh tokens behind existing sessions.

4. Advanced hunting queries in Defender XDR are written in the _____ query language, which Microsoft Sentinel also uses.

Answer: KQL (also accepted: Kusto Query Language)

Advanced hunting and Microsoft Sentinel both use Kusto Query Language, so analyst skills transfer between them. SQL is tempting for anyone with database experience, but KQL uses a pipeline syntax with operators such as where and summarize. Splunk SPL is a separate product language and is not used here.

5. Which two KQL operators are used together to count failed sign-ins per user per hour? (Choose two.)

- A project
- B summarize
- C bin
- D mv-expand
- E top

Answer: B, C

summarize aggregates the counts per user, and bin groups timestamps into hourly buckets so each result row represents one hour. project chooses columns and mv-expand flattens arrays, so both are tempting but do not produce hourly counts. top returns the largest rows rather than per-hour totals.

6. Which Log Analytics setting caps how much data a workspace ingests per day to control cost?

- A Interactive retention period
- B Analytics table plan
- C Daily cap
- D Resource lock

Answer: C

The daily cap limits how much data a workspace ingests each day, which protects cost but can stop collection once the limit is reached. Interactive retention controls how long data stays queryable, which is tempting in cost discussions, but it does not limit intake. A resource lock prevents deletion or changes and has no effect on ingestion volume.

7. Which analytics rule type uses machine learning to correlate low-severity signals from several sources into one multistage attack incident?
- A Threat intelligence matching
 - B Scheduled
 - C Microsoft Security
 - D Fusion

Answer: D

Fusion uses machine learning to correlate low-severity signals from multiple sources into a single multistage attack incident. Threat intelligence matching compares log data to indicator lists, which is tempting because it also uses external signals, but it does not chain alerts into attack stories. Scheduled rules run a KQL query on an interval, and Microsoft Security rules copy alerts from a service.

8. A Microsoft Security analytics rule in Microsoft Sentinel creates incidents from alerts that Microsoft security services such as Defender XDR generate, without a separate scheduled query.
- A True
 - B False

Answer: A (True)

Microsoft Security rules create incidents from alerts produced by Microsoft security services, so the SOC does not have to rebuild those detections as scheduled queries. These rules can still be filtered. Creating a second scheduled query for the same alert is the duplicate detection to avoid.

9. Which Sentinel feature displays dashboards and charts built on workspace queries, and can be customized for SOC reporting?
- A Workbooks
 - B Playbooks
 - C Notebooks
 - D Bookmarks

Answer: A

Workbooks are Azure Monitor based visualizations that run Log Analytics queries and can be customized into dashboards. Playbooks run Logic Apps workflows for response actions rather than displays. Notebooks run code for deep analysis, and bookmarks store individual findings from a hunting session.

10. A playbook must post a message to a Microsoft Teams channel when a high-severity incident is created. Which component runs that workflow?
- A A Logic Apps playbook using the Teams connector
 - B A watchlist with a Teams column
 - C A Sentinel workbook tile
 - D A hunting bookmark

Answer: A

Playbooks are Azure Logic Apps workflows, so one can call the Teams connector when an incident is created. A watchlist holds reference data and cannot send messages. A workbook tile is tempting for reporting, but it only displays data, and a hunting bookmark stores a finding.