

PRACTICE QUESTIONS

Microsoft

SC-200

Microsoft Security Operations Analyst Associate

SHARED BY [u/proud_dolphin_45](#) on aiexamcerts

EDITION	Free Set 1
QUESTIONS	10
SHARED	October 15, 2026
EXAM	Microsoft SC-200, Microsoft Security Operations Analyst Associate

Shared by [u/proud_dolphin_45](#) 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. An analyst needs every device where a specific PowerShell command line ran in the last 24 hours. Which Defender XDR tool should be used?
 - A Secure score dashboard
 - B Automated investigation settings
 - C Advanced hunting with KQL against DeviceProcessEvents
 - D Attack surface reduction report

Answer: C

Advanced hunting runs Kusto Query Language queries over Defender tables, and DeviceProcessEvents records process creation with command-line details. The secure score dashboard reports configuration posture, not individual process events. Automated investigation settings control how the platform responds to alerts, so they cannot search historical process activity.

2. In Microsoft Defender XDR, the feature that automatically contains a high-confidence multi-domain attack by isolating devices and disabling compromised accounts is called attack _____.

Answer: disruption

Attack disruption correlates signals across identities, endpoints and cloud apps, then contains affected assets automatically when confidence is high. Automated investigation is tempting since it also runs without manual steps, but it examines individual alerts instead of correlating a multi-domain attack. Attack surface reduction focuses on blocking risky behaviors before they happen.

3. Which Advanced hunting table records one row per email message, including sender, recipients, subject and delivery action?
 - A DeviceFileEvents
 - B IdentityLogonEvents
 - C CloudAppEvents
 - D EmailEvents

Answer: D

EmailEvents is the Defender for Office 365 table for message-level data such as sender, recipients, subject, and delivery action. DeviceFileEvents is tempting when a malicious attachment is involved, but it records file activity on endpoints rather than mail delivery. IdentityLogonEvents covers authentication activity, so it does not describe messages.

4. Microsoft Defender for Identity can see Kerberos and NTLM authentication traffic on the domain controllers without any sensor installed on them.
- A True
 - B False

Answer: B (False)

Defender for Identity relies on sensors installed on domain controllers to observe Kerberos and NTLM traffic, which is how it detects attacks such as pass-the-hash and Kerberoasting. Without a sensor, that on-premises authentication traffic is not visible to the service.

5. Which two things does an analytics rule's entity mapping provide? (Choose two.)
- A Links query columns such as accounts and IP addresses to Sentinel entity types
 - B Sets the rule's severity automatically
 - C Limits the rule to a single workspace
 - D Encrypts the query results before alerting
 - E Populates the entity pages and investigation graph for an incident

Answer: A, E

Entity mapping connects fields such as Account, Host and IP address from query results to Sentinel entity types, and those mappings feed the entity pages and investigation graph. Severity is a separate rule property, which is tempting because it also appears on the rule, so it is not set by mapping. Workspace limits and encryption are not controlled by entity mapping.

6. Which agent and configuration model is recommended for collecting Windows Security Events and Syslog from on-premises machines into a Log Analytics workspace?
- A Azure Monitor Agent with data collection rules
 - B Legacy Log Analytics agent
 - C Azure Activity connector
 - D Event Grid subscription

Answer: A

The Azure Monitor Agent, configured through data collection rules, is the current agent for Windows Security Events and Syslog collection. The legacy Log Analytics agent is tempting because it also collects these logs, but it is deprecated and no longer the recommended agent. The Azure Activity connector covers subscription control-plane activity, and Event Grid routes events without collecting host logs.

7. Which Sentinel feature stores reference lists, such as approved executive travel IP addresses, that analytics rules and queries can join against?
- A Bookmarks
 - B Watchlists
 - C Notebooks
 - D Threat intelligence indicators

Answer: B

Watchlists hold reference lists in the workspace that KQL queries and analytics rules can join against, such as approved IPs or high-value accounts. Bookmarks save specific events from hunting, which is tempting because they also hold entities, but they are not reference lists. Notebooks run analysis code, and threat intelligence indicators store known bad observables.

8. Microsoft Sentinel pulls logs from a source such as Microsoft Entra ID into a workspace table by enabling a _____ connector.

Answer: data

A data connector configures ingestion so that a source's events land in workspace tables, such as SigninLogs for Entra ID. Analytics rules and workbooks read the data after ingestion rather than during it. Automation rules and playbooks run actions after an incident exists, so they do not collect logs.

9. Which Sentinel incident classification records that the detection was accurate but the activity was authorized, such as an approved admin script?
- A False Positive: incorrect alert logic
 - B True Positive: suspicious activity
 - C Benign Positive: suspicious but expected
 - D Undetermined

Answer: C

Benign positive means the detection fired on real activity that was expected, such as an approved administrative script. False positive means the detection logic was wrong, which is tempting here because both describe noisy alerts. True positive means the activity was malicious, and undetermined leaves the question open.

10. Which Sentinel feature streams new events that match a hunting query in real time, so an analyst can watch activity during an active incident?
- A Notebooks
 - B Bookmarks
 - C Playbook run history
 - D Livestream

Answer: D

Livestream runs a hunting query continuously and displays new matching events as they arrive, which helps during an active incident. Notebooks are tempting for real-time analysis, but they run code on demand rather than streaming events. Bookmarks save findings, and playbook run history records past executions.