Braindump2go Guarantee All Exams 100% Pass One Time!

- Vendor: Microsoft
- Exam Code: SC-200
- Exam Name: Microsoft Security Operations Analyst
- New Updated Questions from Braindump2go
- (Updated in July/2023)

Visit Braindump2go and Download Full Version SC-200 Exam Dumps

**QUESTION 150**
You are using the Microsoft 365 Defender portal to conduct an investigation into a multi-stage incident related to a suspected malicious document. After reviewing all the details, you have determined that the alert tied to the potentially malicious document is also related to another incident in your environment. However, the alert is not currently listed as a part of that second incident.
Your investigation into the alert is ongoing, as it is your investigation into the two related incidents.
You need to appropriately categorize the alert and ensure that it is associated with the second incident.
What two actions should you take in the Manage alert pane to fulfill this part of the investigation? (Choose two)

A. Set status to In progress
B. Set status to New
C. Set classification to True alert
D. Enter the Incident ID of the related incident in the Comment section.
E. Select the Link alert to another incident option.

**Answer:** AE
**Explanation:**
The correct action to classify the alert would be to set the status to In progress. While the alert may seem to be legitimate as it is linked to another incident, until a final determination is reached, you should set the status to In progress to ensure that others know it is being worked on. Once a determination is reached, you can then change it to Resolved and select the appropriate classification (True alert or False alert).
The correct action to correlate the alert to the other incident would be to select the Link alert to another incident option. While ideally, the alert would automatically be included in both incidents that are not always the case. If you notice an alert that is not linked to an incident that it is clearly connected to, using the Link alert to another incident option ensures they are tied together.
You should not set the classification to True alert. While a point can be made that it seems this malicious file involved in multiple incidents is likely to be a True alert, you cannot yet make that determination. It is also not the time to classify it as a false alert. The best practice while continuing an investigation would be not to change the classification at all, which means leaving it as the default Not set classification.
You should not enter the Incident ID of the related incident in the Comment section. While this might be helpful from an administrative perspective, it creates no link to the other incident.
You should not set the status to New. This is the default status of any alert. The question specifically seeks to ensure your peers know the alert is being investigated, so setting (or leaving) the status as New would make it impossible to differentiate from other uninvestigated alerts.
All of the actions mentioned in the options can be found in the Manage alert pane, which can be reached via the Alerts tab in the Incidents section of the Microsoft 365 Defender portal.
References:
https://docs.microsoft.com/en-us/microsoft-365/security/defender/investigate-alerts
https://docs.microsoft.com/en-us/microsoft-365/security/defender/investigate-incidents?view=o365-worldwide

SC-200 Exam Dumps SC-200 Exam Questions SC-200 PDF Dumps SC-200 VCE Dumps

https://www.braindump2go.com/sc-200.html

**QUESTION 151**
Which of the following choices best defines threat hunting using Microsoft Defender for Endpoint?

A. Sensing and blocking apps that are considered unsafe but may not be detected as malware.
B. Decrease vulnerabilities (attack surfaces) in your applications with intelligent rules that help stop malware.
C. You can proactively look at events in your network using a powerful search and query tool.
D. All of the above.

**Answer:** C
**Explanation:**
Option A is incorrect. This is an explanation of advanced protection provided by Windows Defender Antivirus.
Options B, D are incorrect. This is an explanation of attack surface reduction.
Option C is correct. Microsoft Defender for Endpoint advanced threat hunting is built on top of a query language that gives you flexibility.
Reference:
https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/advanced-hunting-overview?view=o365-worldwide

**QUESTION 152**
Which of the following is not a component of Microsoft Defender for Endpoint?

A. Endpoint detection and response
B. Cloud device management
C. Next generation protection
D. Integrity monitoring

**Answer:** B
**Explanation:**
Options A and C are incorrect. Threat and vulnerability management, attack surface reduction, next-generation protection, endpoint detection and response, automated investigation and remediation are all components of Microsoft Defender for Endpoint.
Option B is correct. Cloud device management is not a component of the security administration of Microsoft Defender for Endpoint.
Reference:
https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/microsoft-defender-endpoint?view=o365-worldwide

**QUESTION 153**
You are a SOC Analyst of a company XYZ that has implemented Microsoft Defender for Endpoint. You are allocated an incident with alerts related to a doubtful PowerShell command line. You start by going through the incident and apprehend all the related alerts, devices, and evidence.
You open the alert page to evaluate the Alert and choose to perform further analysis on the device. You open the Device page and decide that you require remote access to the device to collect more forensics information using a custom .ps1 script.
Which type of information is gathered in an Investigation package?

A. Prefetch Files
B. Network transactions
C. Command History
D. Process History

**Answer:** A
**Explanation:**
Network transactions, Process and Command History are not collected. Only Prefetch files are collected.

An investigation package contains the following folders when you collect it from a device as part of the investigation process. These can help us identify the present state of devices and methods used by attackers.
Autoruns, installed programs, Network Connections, Prefetch files, Prefetch folder, Processes, Scheduled tasks, Security event log, Services, Windows Server Message Block (SMB) sessions, System Information, Temp Directories, Users and Groups, WdSupportLogs, CollectionSummaryReport.xls
Reference:
https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/respond-machine-alerts?view=o365-worldwide

**QUESTION 154**
You are a SOC Analyst of a company XYZ that has implemented Microsoft Defender for Endpoint. You are allocated an incident with alerts related to a doubtful PowerShell command line. You start by going through the incident and apprehend all the related alerts, devices, and evidence.
You open the alert page to evaluate the Alert and choose to perform further analysis on the device. You open the Device page and decide that you require remote access to the device to collect more forensics information using a custom .ps1 script.
Which one of the below is a Device action?

A. Reformat device
B. Isolate device
C. Reboot
D. Reinstall

**Answer:** B
**Explanation:**
You can't issue either reboot, reinstall or reformat action. You can perform isolation devices.
Depending on the severity of the attack and the sensitivity of the device, you might want to isolate the device from the network. This action can help prevent the attacker from controlling the compromised device and performing further activities such as data exfiltration and lateral movement.
Reference:
https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/respond-machine-alerts?view=o365-worldwide

**QUESTION 155**
Which of the below artifact types contains an investigation page?

A. Domain
B. Threat Actor
C. Hunter
D. Alert

**Answer:** A
**Explanation:**
Option A is correct. Domain contains an investigation page.
Option B is incorrect. Threat Actor is not a forensic artifact.
Option C is incorrect. Hunter does not have an investigation page.
Option D is incorrect. Alert does not have an investigation page.
Reference :
https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/investigate-machines?view=o365-worldwide

**QUESTION 156**
What information is shared by a deep file analysis?

A. Registry Modifications
B. Code change history
C. Command history

D. Process history

**Answer:** A
**Explanation:**
Command history, process and code change history are not reported. Only Registry modifications are reported.
Deep file analysis results contain the file's activities, behaviors, and artifacts like dropped files, registry changes and IP communication.
Reference:
https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/respond-file-alerts?view=o365-worldwide

**QUESTION 157**
Which information is shared on the user account page?

A. Security groups
B. Threat hunt ID
C. Associated alerts
D. All of the above

**Answer:** C
**Explanation:**
The security groups, user accounts belong to and threat hunt ID is not shown.
Associated alerts are made available.
Reference:
https://docs.microsoft.com/en-us/microsoft-365/security/defender/investigate-users?view=o365-worldwide

**QUESTION 158**
Multiple false positive alerts are generating in a company XYZ. A security operations analyst working for XYZ needs to exclude an executable file to reduce alerts - c:\myxyzapp\myxyzwinapp.exe, which exclusion type must they use?

A. Extension
B. Folder
C. File
D. Registry

**Answer:** C
**Explanation:**
File will exclude only this specific file, whereas extension would exclude all files with the extensions, and folder would exclude all files in a folder. Registry exclusion doesn't happen.
Reference:
https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/configure-extension-file-exclusions-microsoft-defender-antivirus?view=o365-worldwide

**QUESTION 159**
In advanced features, which setting must be turned on to obstruct files even if a 3rd party AV is used?

A. Turn on EDR with block mode.
B. Automated Investigation
C. Allow or block file
D. All of the above

**Answer:** A
**Explanation:**
Option A is correct. EDR with block mode can be used with third-party AV.
Option B is incorrect. The "Allow or block file" feature requires Defender AV.
Option C is incorrect. Automated investigations do not block files.
Reference:

https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/microsoft-defender-antivirus-compatibility?view=o365-worldwide

**QUESTION 160**
Microsoft Defender for Endpoint gives configuration selections for alerts and detections. These include notifications, custom indicators, and detection rules. Which filter is a part of an Alert notification rule?

A. Subject IDs
B. Alert Severity
C. Account
D. Alert IDs

**Answer:** B
**Explanation:**
Reference:
https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/configure-email-notifications?view=o365-worldwide

**QUESTION 161**
You are in charge of working with the endpoint team to patch weaknesses reported by Threat Vulnerability Management. Which report keeps an inventory of the vulnerabilities of your systems that are wide-open by listing the CVE IDs?

A. Weakness
B. Software Inventory
C. Event Timeline
D. Incident

**Answer:** A
**Explanation:**
Option A is correct. This report is enumerated by the CVE ID.
Option B is incorrect. The software inventory page contains a list of software installed in your organization.
Option C is incorrect. The event timeline is a risk feed that lets you understand how risk is introduced in the organization.
Option D is incorrect. The incident report doesn't contain any weaknesses or vulnerabilities.
Reference:
https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/tvm-weaknesses?view=o365-worldwide

**QUESTION 162**
Which selection is an ASR (attack surface reduction) rule that can be implemented and blocked?

A. Content from mobile devices
B. PowerShell from executing
C. Process creations initiating from WMI and PSExec commands
D. None of the above

**Answer:** C
**Explanation:**
Option A is incorrect. This is not an ASR rule that can be implemented and blocked.
Option B is incorrect. .ps1 execution cannot be blocked with an ASR rule.
Option C is correct. This is an ASR rule that can be implemented and blocked.
Reference:
https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/attack-surface-reduction?view=o365-worldwide

**QUESTION 163**

From which of the following can a SOC (Security Operation Center) analyst make a customized detection?

A. Alert
B. Incident
C. Advanced Hunting
D. Request

**Answer:** C
**Explanation:**
Advanced hunting gives a choice to save the query as a detection, while Alert and Incident don't provide an option to save as a detection.
Reference:
https://docs.microsoft.com/en-us/microsoft-365/security/defender/advanced-hunting-query-results?view=o365-worldwide

**QUESTION 164**
Microsoft Defender for Endpoint gives a purpose based UI to manage and inspect security incidents and alerts. Which option can't be accomplished in the Action Center?

A. Review completed actions.
B. Configure action email notifications.
C. Manage pending actions.
D. None of the above

**Answer:** B
**Explanation:**
Reference:
https://docs.microsoft.com/en-us/azure/security-center/security-center-provide-security-contact-details

**QUESTION 165**
A SOC analyst found out about an event of interest. What is the next step to take it forward for further review?

A. Flag
B. Tag
C. Highlight
D. Close

**Answer:** A
**Explanation:**
While looking into the device timeline for suspicious activity, we can search and filter for specific events. We can set event flags by:
- Highlighting the most important events
- Marking events that require a deep dive
- Building a clean breach timeline
Find the event that we want to flag. Select the flag icon in the Flag column.
Once events are flagged, we can filter suspicious events more easily. In the timeline Filters section, enable Flagged events. Only flagged events are displayed. You can apply more filters that will only show events prior to the flagged event.
Reference:
https://docs.microsoft.com/en-us/defender-for-identity/investigate-entity

**QUESTION 166**
What type of Behavioural blocking can be utilized with 3rd-party AVs?

A. EDR with block mode
B. Feedback-loop blocking

C. Client behavior blocking
D. Malicious behavior blocking

**Answer:** A
**Explanation:**
Option A is correct. EDR with Block mode allows you for blocking even when another AV is in use.
Options B, C, D are incorrect. Feedback-loop and Client behavior blocking are used with Defender AV.
Reference:
https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/edr-in-block-mode?view=o365-worldwide

**QUESTION 167**
A Windows 10 system is not showing in the device inventory list. What may be the problem?

A. System is not having the latest KB's
B. System has no alerts in the past 30 days.
C. System was renamed.
D. None of the above

**Answer:** B
**Explanation:**
Options A, C, D are incorrect. Neither renaming any device nor KB's has any impact on the Device inventory list.
Option B is correct. We can modify the "time setting" to find the system.
Reference:
https://docs.microsoft.com/en-us/azure/security-center/asset-inventory

**QUESTION 168**
Microsoft 365 Defender gives a purpose-based UI to manage and examine security incidents and alerts across Microsoft 365 services.
You are a SOC Analyst working at a company XYZ that has configured Microsoft 365 Defender solutions, including Defender for Endpoint, Defender for Identity, Defender for Office 365, and Cloud App Security.
You are required to monitor related alerts across all the solutions as a single incident to observe the incident's full impact and do an RCA (root cause investigation). The Microsoft Security center portal has a fused view of incidents and actions are taken on them.
Which tab is present on the incident page when investigating a particular incident?

A. Machines
B. Mailboxes
C. Networks
D. Incidents

**Answer:** B
**Explanation:**
Reference:
https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/investigate-incidents?view=o365-worldwide

**QUESTION 169**
Microsoft 365 Defender gives a purpose-based UI to manage and examine security incidents and alerts across Microsoft 365 services.
You are a SOC Analyst working at a company XYZ that has configured Microsoft 365 Defender solutions, including Defender for Endpoint, Defender for Identity, Defender for Office 365, and Cloud App Security.
You are required to monitor related alerts across all the solutions as a single incident to observe the incident's full impact and do an RCA (root cause investigation). The Microsoft Security center portal has a fused view of incidents and actions taken on them.
Which of the following can be classified as an Incident?

A. Test alert

B. True alert
C. High alert
D. Positive alert

**Answer:** B
**Explanation:**
Reference:
https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/investigate-incidents?view=o365-worldwide

**QUESTION 170**
You have a Microsoft 365 subscription. The subscription uses Microsoft 365 Defender and has data loss prevention (DLP) policies that have aggregated alerts configured.
You need to identify the impacted entities in an aggregated alert.
What should you review in the DLP alert management dashboard of the Microsoft 365 compliance center?

A. the Events tab of the alert
B. the Sensitive Info Types tab of the alert
C. Management log
D. the Details tab of the alert

**Answer:** A
**Explanation:**
In order to identify the impacted entities in an aggregated alert, you should review the "Events" tab of the DLP alert management dashboard in the Microsoft 365 compliance center. This tab will display a list of all the events that triggered the alert, including the specific entities (e.g. files, emails, etc.) that were affected. You can further investigate each event to identify the specific user, device and action that caused the alert to be triggered.
https://learn.microsoft.com/en-us/microsoft-365/compliance/dlp-configure-view-alerts-policies?view=o365-worldwide

**QUESTION 171**
You have a Microsoft 365 subscription that uses Microsoft 365 Defender.
You plan to create a hunting query from Microsoft Defender.
You need to create a custom tracked query that will be used to assess the threat status of the subscription.
From the Microsoft 365 Defender portal, which page should you use to create the query?

A. Threat analytics
B. Advanced Hunting
C. Explorer
D. Policies & rules

**Answer:** B
**Explanation:**
"Use Advance mode if you're comfortable creating custom queries."
https://learn.microsoft.com/en-us/microsoft-365/security/defender/advanced-hunting-overview?view=o365-worldwide
https://learn.microsoft.com/en-us/microsoft-365/security/defender/advanced-hunting-modes?view=o365-worldwide#get-started-with-guided-hunting-mode

**QUESTION 172**
You have a Microsoft 365 subscription that uses Microsoft Defender for Endpoint.
You need to add threat indicators for all the IP addresses in a range of 171.23.34.32-171.23.34.63. The solution must minimize administrative effort.
What should you do in the Microsoft 365 Defender portal?

A. Create an import file that contains the individual IP addresses in the range. Select Import and import the file.
B. Create an import file that contains the IP address of 171.23.34.32/27. Select Import and import the file.

C. Select Add indicator and set the IP address to 171.23.34.32-171.23.34.63.
D. Select Add indicator and set the IP address to 171.23.34.32/27.

**Answer:** A