

[Download Full Version SC-200 Exam Dumps\(Updated in Feb/2023\)](#)

Explanation:

<https://docs.microsoft.com/en-us/azure/security-center/continuous-export?tabs=azure-portal>

QUESTION 48

Your company uses Microsoft Defender for Endpoint.

The company has Microsoft Word documents that contain macros. The documents are used frequently on the devices of the company's accounting team.

You need to hide false positive in the Alerts queue, while maintaining the existing security posture. Which three actions should you perform? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

- A. Resolve the alert automatically.
- B. Hide the alert.
- C. Create a suppression rule scoped to any device.
- D. Create a suppression rule scoped to a device group.
- E. Generate the alert.

Correct Answer: BCE

Explanation:

<https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/manage-alerts>

QUESTION 49

DRAG DROP

You have a Microsoft Sentinel workspace named workspace1 and an Azure virtual machine named VM1.

You receive an alert for suspicious use of PowerShell on VM1.

You need to investigate the incident, identify which event triggered the alert, and identify whether the following actions occurred on VM1 after the alert:

- The modification of local group memberships
- The purging of event logs

Which three actions should you perform in sequence in the Azure portal? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

Actions	Answer Area
From the details pane of the incident, select Investigate .	
From the Investigation blade, select the entity that represents VM1.	
From the Investigation blade, select the entity that represents powershell.exe.	
From the Investigation blade, select Timeline .	
From the Investigation blade, select Info .	
From the Investigation blade, select Insights .	

Correct Answer:

[Download Full Version SC-200 Exam Dumps\(Updated in Feb/2023\)](#)

Actions	Answer Area
From the details pane of the incident, select Investigate .	From the Investigation blade, select Insights .
From the Investigation blade, select the entity that represents VM1.	
From the Investigation blade, select the entity that represents powershell.exe.	
From the Investigation blade, select Timeline .	From the Investigation blade, select the entity that represents VM1.
From the Investigation blade, select Info .	
From the Investigation blade, select Insights .	From the details pane of the incident, select Investigate .

QUESTION 50

You have a Microsoft 365 subscription that has Microsoft 365 Defender enabled.

You need to identify all the changes made to sensitivity labels during the past seven days.

What should you use?

- A. the Incidents blade of the Microsoft 365 Defender portal
- B. the Alerts settings on the Data Loss Prevention blade of the Microsoft 365 compliance center
- C. Activity explorer in the Microsoft 365 compliance center
- D. the Explorer settings on the Email & collaboration blade of the Microsoft 365 Defender portal

Correct Answer: C

Explanation:

Labeling activities are available in Activity explorer.

For example:

Sensitivity label applied

This event is generated each time an unlabeled document is labeled or an email is sent with a sensitivity label.

It is captured at the time of save in Office native applications and web applications.

It is captured at the time of occurrence in Azure Information protection add-ins.

Upgrade and downgrade labels actions can also be monitored via the Label event type field and filter.

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/compliance/data-classification-activity-explorer-available-events?view=o365-worldwide>

QUESTION 51

HOTSPOT

You have the following SQL query.

[Download Full Version SC-200 Exam Dumps\(Updated in Feb/2023\)](#)

```
let IPList = _GetWatchlist('Bad_IPs');
Event
| where Source == "Microsoft-Windows-Sysmon"
| where EventID == 3
| extend EvData = parse_xml(EventData)
| extend EventDetail = EvData.DataItem.EventData.Data
| extend SourceIP = EventDetail.[9].["#text"], DestinationIP = EventDetail.[14].["#text"]
| where SourceIP in (IPList) or DestinationIP in (IPList)
| extend IPMatch = case( SourceIP in (IPList), "SourceIP", DestinationIP in (IPList), "DestinationIP", "None")
| extend timestamp = TimeGenerated, AccountCustomEntity = UserName, HostCustomEntity = Computer, '
```

Statements	Yes	No
The UserName field is set as the account entity.	<input type="radio"/>	<input type="radio"/>
The watchlist cannot be updated after it is created.	<input type="radio"/>	<input type="radio"/>
The IPList variable is set as the IP address entity.	<input type="radio"/>	<input type="radio"/>

Correct Answer:

Statements	Yes	No
The UserName field is set as the account entity.	<input type="radio"/>	<input checked="" type="radio"/>
The watchlist cannot be updated after it is created.	<input type="radio"/>	<input checked="" type="radio"/>
The IPList variable is set as the IP address entity.	<input type="radio"/>	<input checked="" type="radio"/>

QUESTION 52

You have an Azure subscription that has Microsoft Defender for Cloud enabled.

You have a virtual machine that runs Windows 10 and has the Log Analytics agent installed.

You need to simulate an attack on the virtual machine that will generate an alert.

What should you do first?

- A. Run the Log Analytics Troubleshooting Tool.
- B. Copy a executable and rename the file as ASC_AlerTest_662jf10N.exe
- C. Modify the settings of the Microsoft Monitoring Agent.
- D. Run the MMASetup executable and specify the -foo argument

Correct Answer: A

QUESTION 53

[SC-200 Exam Dumps](#) [SC-200 PDF Dumps](#) [SC-200 VCE Dumps](#) [SC-200 Q&As](#)
<https://www.ensurepass.com/SC-200.html>

[Download Full Version SC-200 Exam Dumps\(Updated in Feb/2023\)](#)

DRAG DROP

You are investigating an incident by using Microsoft 365 Defender.

You need to create an advanced hunting query to detect failed sign-in authentications on three devices named CFOLaptop, CEOlaptop, and COOLaptop.

How should you complete the query? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Values	Answer Area
<code> project LogonFailures=count()</code>	
<code> summarize LogonFailures=count() by DeviceName, LogonType</code>	
<code> where ActionType == FailureReason</code>	
<code> where DeviceName in ("CFOLaptop, "CEOlaptop", "COOLaptop")</code>	
<code>ActionType == "LogonFailed"</code>	

Correct Answer:

Values	Answer Area
<code> project LogonFailures=count()</code>	<code> summarize LogonFailures=count() by DeviceName, LogonType</code>
<code> summarize LogonFailures=count() by DeviceName, LogonType</code>	<code> where DeviceName in ("CFOLaptop, "CEOlaptop", "COOLaptop")</code>
<code> where ActionType == FailureReason</code>	<code> where ActionType == FailureReason</code>
<code> where DeviceName in ("CFOLaptop, "CEOlaptop", "COOLaptop")</code>	<code>ActionType == "LogonFailed"</code>
<code>ActionType == "LogonFailed"</code>	<code> project LogonFailures=count()</code>

QUESTION 54

[Download Full Version SC-200 Exam Dumps\(Updated in Feb/2023\)](#)

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You are configuring Microsoft Defender for Identity integration with Active Directory.

From the Microsoft Defender for identity portal, you need to configure several accounts for attackers to exploit.

Solution: From Azure Identity Protection, you configure the sign-in risk policy.

Does this meet the goal?

- A. Yes
- B. No

Correct Answer: B

Explanation:

<https://docs.microsoft.com/en-us/defender-for-identity/manage-sensitive-honeytoken-accounts>

QUESTION 55

DRAG DROP

You have an Azure Functions app that generates thousands of alerts in Azure Security Center each day for normal activity.

You need to hide the alerts automatically in Security Center.

Which three actions should you perform in sequence in Security Center? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

Actions	Answer area
Select Pricing & settings .	
Select Security alerts .	
Select IP as the entity type and specify the IP address.	⏪ ⏩
Select Azure Resource as the entity type and specify the ID.	⏪ ⏩
Select Suppression rules , and then select Create new suppression rule .	
Select Security policy .	

Correct Answer: