

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

QUESTION 56

HOTSPOT

You have a Microsoft 365 subscription that uses Microsoft 365 Defender and contains a user named User1.

You are notified that the account of User1 is compromised.

You need to review the alerts triggered on the devices to which User1 signed in.

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

NOTE: Each correct selection is worth one point.


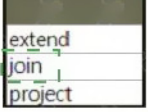
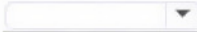
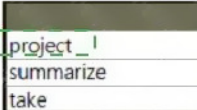
```
DeviceInfo
| where LoggedOnUsers contains 'user1'
| distinct DeviceId
|  kind=inner AlertEvidence on DeviceId
| 
| project AlertId
| join AlertInfo on AlertId
|  AlertId, Timestamp, Title, Severity, Category
| 
```

extend
join
project

project
summarize
take

Correct Answer:

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

```
DeviceInfo
| where LoggedOnUsers contains 'user1'
| distinct DeviceId
|  kind=inner AlertEvidence on DeviceId
| 
| project AlertId
| join AlertInfo on AlertId
|  AlertId, Timestamp, Title, Severity, Category
| 
```

QUESTION 57

HOTSPOT

You have an Azure subscription that uses Azure Defender.


You plan to use Azure Security Center workflow automation to respond to Azure Defender threat alerts.

You need to create an Azure policy that will perform threat remediation automatically.


What should you include in the solution? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Set available effects to:


Append
DeployIfNotExists
EnforceRegoPolicy

To perform remediation use:


An Azure Automation runbook that has a webhook
An Azure Logic Apps app that has the trigger set to When an Azure Security Center Alert is created or triggered
An Azure Logic Apps app that has the trigger set to When a response to an Azure Security Center alert is triggered

Correct Answer:

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

Set available effects to:

Append
DeployIfNotExists
EnforceRegoPolicy

To perform remediation use:

An Azure Automation runbook that has a webhook
An Azure Logic Apps app that has the trigger set to When an Azure Security Center Alert is created or triggered
An Azure Logic Apps app that has the trigger set to When a response to an Azure Security Center alert is triggered

QUESTION 58

You have an Azure subscription named Sub1 and a Microsoft 365 subscription. Sub1 is linked to an Azure Active Directory (Azure AD) tenant named contoso.com.

You create an Azure Sentinel workspace named workspace1. In workspace1, you activate an Azure AD connector for contoso.com and an Office 365 connector for the Microsoft 365 subscription.

You need to use the Fusion rule to detect multi-staged attacks that include suspicious sign-ins to contoso.com followed by anomalous Microsoft Office 365 activity.

Which two actions should you perform? Each correct answer present part of the solution.

NOTE: Each correct selection is worth one point.

- A. Create custom rule based on the Office 365 connector templates.
- B. Create a Microsoft incident creation rule based on Azure Security Center.
- C. Create a Microsoft Cloud App Security connector.
- D. Create an Azure AD Identity Protection connector.

Correct Answer: AB

QUESTION 59

DRAG DROP

You have an Azure subscription. The subscription contains 10 virtual machines that are onboarded to Microsoft Defender for Cloud.

You need to ensure that when Defender for Cloud detects digital currency mining behavior on a virtual machine, you receive an email notification. The solution must generate a test email.

Which three actions should you perform in sequence? 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 Workflow automation in Defender for Cloud, change the status of the workflow automation.	
From Logic App Designer, run a trigger.	
From Security alerts in Defender for Cloud, create a sample alert.	
From Logic App Designer, create a logic app.	
From Workflow automation in Defender for Cloud, add a workflow automation.	

Correct Answer:

[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\(Updated in Feb/2023\)](#)

Actions	Answer Area
From Workflow automation in Defender for Cloud, change the status of the workflow automation.	From Logic App Designer, create a logic app.
From Logic App Designer, run a trigger.	
From Security alerts in Defender for Cloud, create a sample alert.	From Logic App Designer, run a trigger.
From Logic App Designer, create a logic app.	
From Workflow automation in Defender for Cloud, add a workflow automation.	From Workflow automation in Defender for Cloud, add a workflow automation.

QUESTION 60

You plan to create a custom Azure Sentinel query that will track anomalous Azure Active Directory (Azure AD) sign-in activity and present the activity as a time chart aggregated by day. You need to create a query that will be used to display the time chart. What should you include in the query?

- A. extend
- B. bin
- C. makeset
- D. workspace

Correct Answer: B

Explanation:

<https://docs.microsoft.com/en-us/azure/azure-monitor/logs/get-started-queries>

QUESTION 61

You have a playbook in Azure Sentinel.

When you trigger the playbook, it sends an email to a distribution group.

You need to modify the playbook to send the email to the owner of the resource instead of the distribution group.

What should you do?

- A. Add a parameter and modify the trigger.
- B. Add a custom data connector and modify the trigger.
- C. Add a condition and modify the action.
- D. Add a parameter and modify the action.

Correct Answer: D

Explanation:

<https://azsec.azurewebsites.net/2020/01/19/notify-azure-sentinel-alert-to-your-email-automatically/>

QUESTION 62

You implement Safe Attachments policies in Microsoft Defender for Office 365.

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

Users report that email messages containing attachments take longer than expected to be received.

You need to reduce the amount of time it takes to deliver messages that contain attachments without compromising security. The attachments must be scanned for malware, and any messages that contain malware must be blocked.

What should you configure in the Safe Attachments policies?

- A. Dynamic Delivery
- B. Replace
- C. Block and Enable redirect
- D. Monitor and Enable redirect

Correct Answer: A

Explanation:

<https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/safe-attachments?view=o365-worldwide>

QUESTION 63

You have an existing Azure logic app that is used to block Azure Active Directory (Azure AD) users. The logic app is triggered manually.

You deploy Azure Sentinel.

You need to use the existing logic app as a playbook in Azure Sentinel. What should you do first?

- A. Add a new scheduled query rule.
- B. Add a data connector to Azure Sentinel.
- C. Configure a custom Threat Intelligence connector in Azure Sentinel.
- D. Modify the trigger in the logic app.

Correct Answer: D

Explanation:

<https://docs.microsoft.com/en-us/azure/sentinel/playbook-triggers-actions>

<https://docs.microsoft.com/en-us/azure/sentinel/tutorial-respond-threats-playbook>

QUESTION 64

HOTSPOT

You purchase a Microsoft 365 subscription.

You plan to configure Microsoft Cloud App Security.

You need to create a custom template-based policy that detects connections to Microsoft 365 apps that originate from a botnet network.

What should you use? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.