

Microsoft

Exam Questions SC-200

Microsoft Security Operations Analyst



NEW QUESTION 1

- (Topic 2)

You need to modify the anomaly detection policy settings to meet the Cloud App Security requirements. Which policy should you modify?

- A. Activity from suspicious IP addresses
- B. Activity from anonymous IP addresses
- C. Impossible travel
- D. Risky sign-in

Answer: C

Explanation:

Reference:

<https://docs.microsoft.com/en-us/cloud-app-security/anomaly-detection-policy>

NEW QUESTION 2

- (Topic 4)

Your company uses Azure Security Center and Azure Defender.

The security operations team at the company informs you that it does NOT receive email notifications for security alerts.

What should you configure in Security Center to enable the email notifications?

- A. Security solutions
- B. Security policy
- C. Pricing & settings
- D. Security alerts
- E. Azure Defender

Answer: C

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/security-center/security-center-provide-security-contact-details>

NEW QUESTION 3

HOTSPOT - (Topic 4)

You have an Azure subscription that has Azure Defender enabled for all supported resource types.

You create an Azure logic app named LA1.

You plan to use LA1 to automatically remediate security risks detected in Azure Security Center.

View the window

You need to test LA1 in Security Center.

What should you do? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Answer Area

Set the LA1 trigger to:

When an Azure Security Center Recommendation is created or triggered
When an Azure Security Center Alert is created or triggered
When a response to an Azure Security Center alert is triggered

Trigger the execution of LA1 from:

Recommendations
Workflow automation

Solution:

Answer Area

Set the LA1 trigger to:

When an Azure Security Center Recommendation is created or triggered
When an Azure Security Center Alert is created or triggered
When a response to an Azure Security Center alert is triggered

Trigger the execution of LA1 from:

Recommendations
Workflow automation

Does this meet the goal?

- A. Yes
- B. No

Answer: A

NEW QUESTION 4

- (Topic 4)

You have a custom Microsoft Sentinel workbook named Workbooks.

You need to add a grid to Workbook1. The solution must ensure that the grid contains a maximum of 100 rows.

What should you do?

- A. In the query editor interface, configure Settings.
- B. In the query editor interface, select Advanced Editor
- C. In the grid query, include the project operator.
- D. In the grid query, include the take operator.

Answer: B

NEW QUESTION 5

- (Topic 4)

You are investigating an incident in Azure Sentinel that contains more than 127 alerts. You discover eight alerts in the incident that require further investigation.

You need to escalate the alerts to another Azure Sentinel administrator. What should you do to provide the alerts to the administrator?

- A. Create a Microsoft incident creation rule
- B. Share the incident URL
- C. Create a scheduled query rule
- D. Assign the incident

Answer: D

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/sentinel/investigate-cases>

NEW QUESTION 6

HOTSPOT - (Topic 4)

You deploy Azure Sentinel.

You need to implement connectors in Azure Sentinel to monitor Microsoft Teams and Linux virtual machines in Azure. The solution must minimize administrative effort.

Which data connector type should you use for each workload? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Microsoft Teams:

	▼
Custom	
Office 365	
Security Events	
Syslog	

Linux virtual machines in Azure:

	▼
Custom	
Office 365	
Security Events	
Syslog	

Solution:

Microsoft Teams:

	▼
Custom	
Office 365	
Security Events	
Syslog	

Linux virtual machines in Azure:

	▼
Custom	
Office 365	
Security Events	
Syslog	

Does this meet the goal?

- A. Yes
- B. No

Answer: A

NEW QUESTION 7

- (Topic 4)

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.

Answer: D

Explanation:

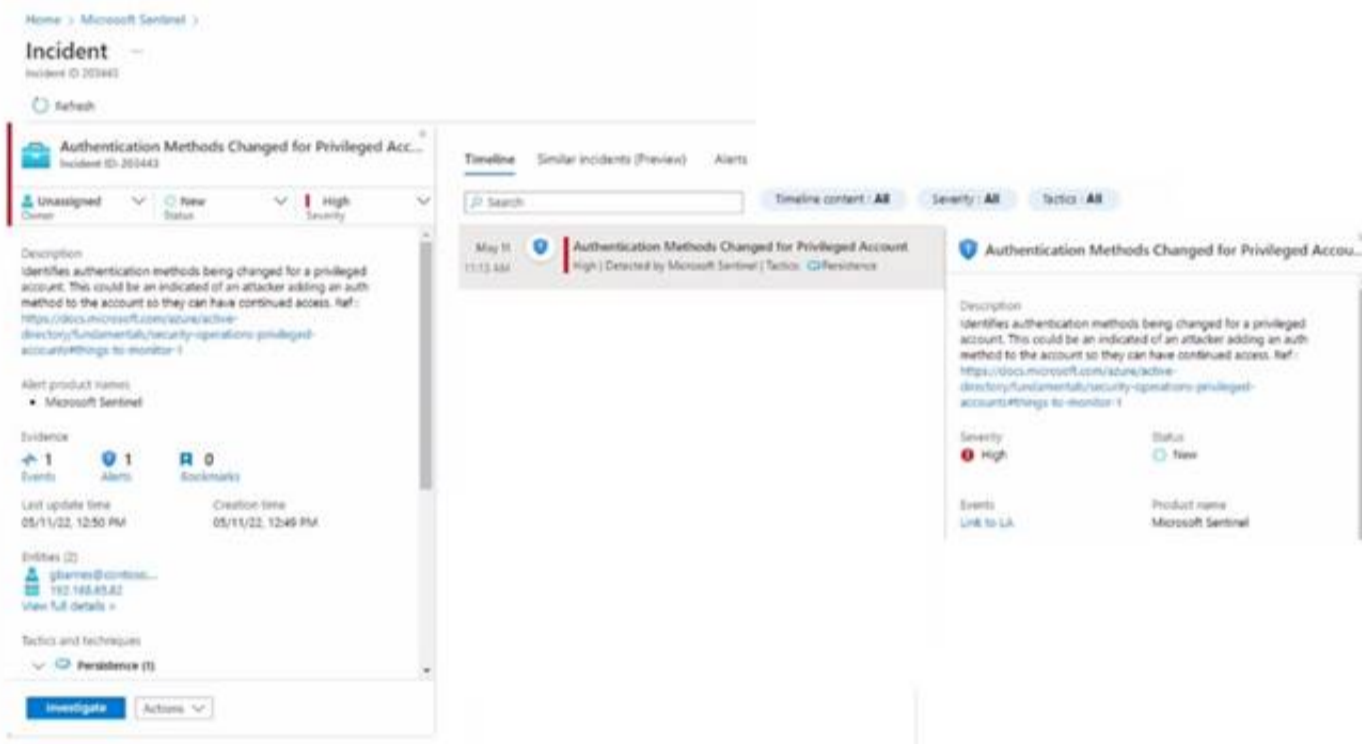
<https://docs.microsoft.com/en-us/azure/sentinel/playbook-triggers-actions> <https://docs.microsoft.com/en-us/azure/sentinel/tutorial-respond-threats-playbook>

NEW QUESTION 8

HOTSPOT - (Topic 4)

You have a Microsoft Sentinel workspace.

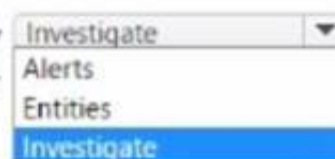
A Microsoft Sentinel incident is generated as shown in the following exhibit.



Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.
 NOTE: Each correct selection is worth one point.

Answer Area

A map of the entities connected to the alert can be viewed by selecting [answer choice].



A list of the activities performed during the investigation can be viewed by selecting [answer choice].



Solution:

Answer Area

A map of the entities connected to the alert can be viewed by selecting [answer choice].



A list of the activities performed during the investigation can be viewed by selecting [answer choice].



Does this meet the goal?

- A. Yes
- B. No

Answer: A

NEW QUESTION 9

- (Topic 4)

Your company has a single office in Istanbul and a Microsoft 365 subscription.

The company plans to use conditional access policies to enforce multi-factor authentication (MFA).

You need to enforce MFA for all users who work remotely. What should you include in the solution?

- A. a fraud alert
- B. a user risk policy
- C. a named location
- D. a sign-in user policy

Answer: C

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/location-condition>

NEW QUESTION 10

DRAG DROP - (Topic 4)

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

- 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.

➤

➤

➤

➤

➤

Answer Area

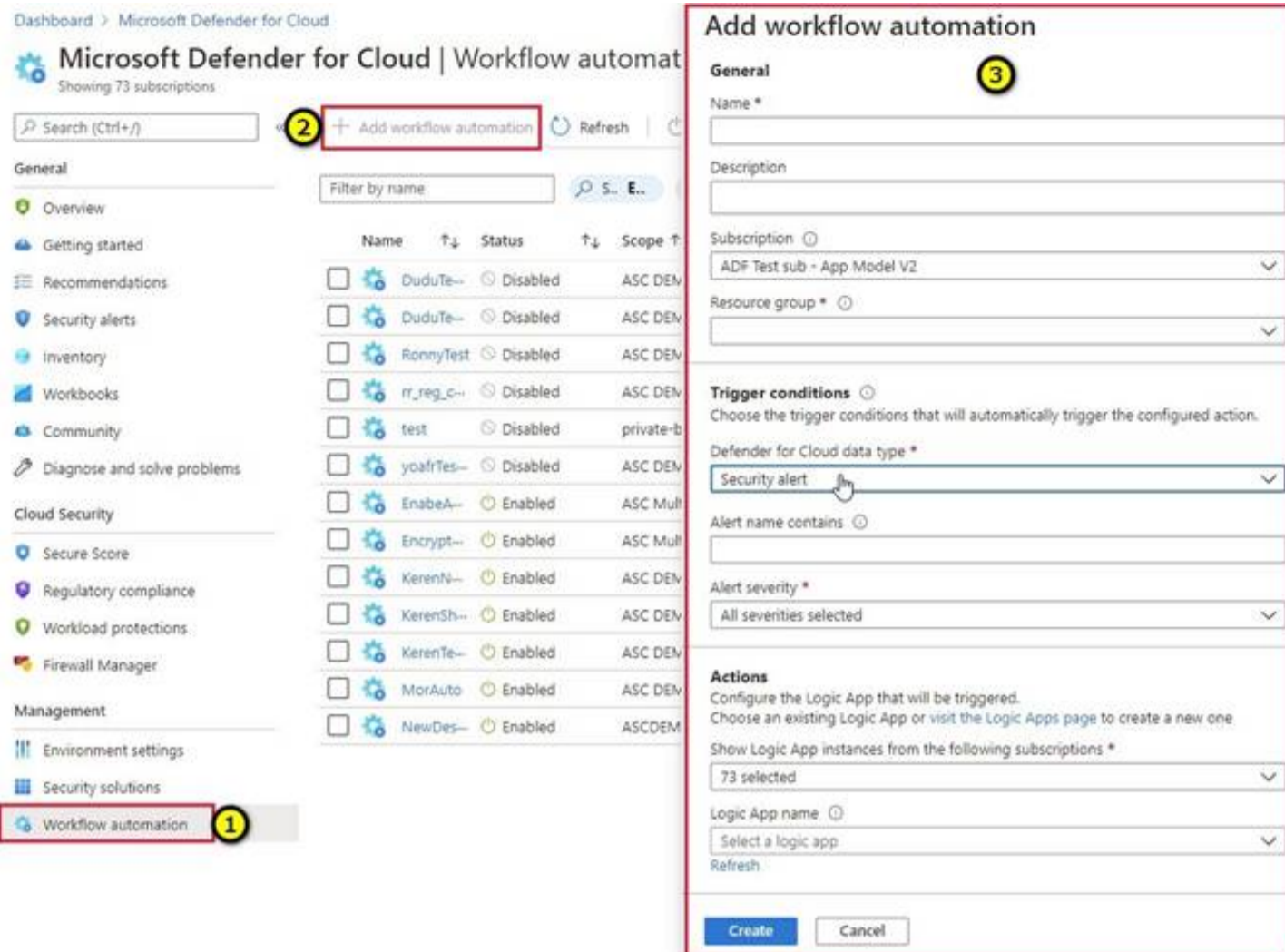
Solution:

Step 1: From Logic App Designer, create a logic app.

Create a logic app and define when it should automatically run

* 1. From Defender for Cloud's sidebar, select Workflow automation.

* 2. To define a new workflow, click Add workflow automation. The options pane for your new automation opens.



Here you can enter:

A name and description for the automation.

The triggers that will initiate this automatic workflow. For example, you might want your Logic App to run when a security alert that contains "SQL" is generated.

The Logic App that will run when your trigger conditions are met.

* 3. From the Actions section, select visit the Logic Apps page to begin the Logic App creation process.

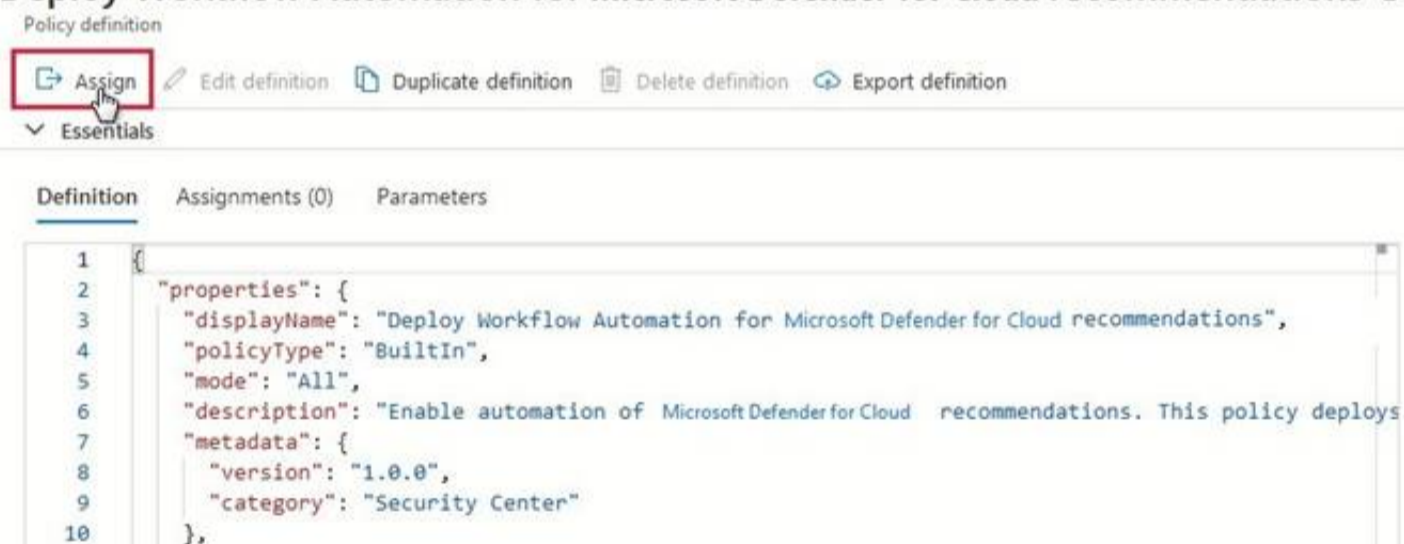
* 4. Etc.

Step 2: From Logic App Designer, run a trigger. Manually trigger a Logic App

You can also run Logic Apps manually when viewing any security alert or recommendation.

Step 3: From Workflow automation in Defender for cloud, add a workflow automation. Configure workflow automation at scale using the supplied policies
 Automating your organization's monitoring and incident response processes can greatly improve the time it takes to investigate and mitigate security incidents.

Deploy Workflow Automation for Microsoft Defender for Cloud recommendations



Does this meet the goal?

- A. Yes
- B. No

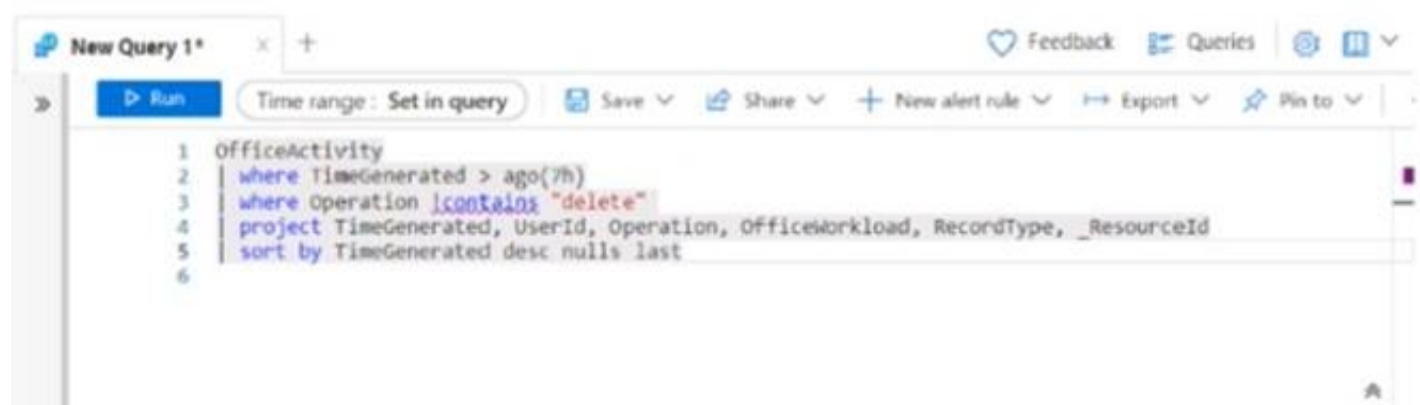
Answer: A

NEW QUESTION 11

- (Topic 4)

You have a Microsoft Sentinel workspace.

You have a query named Query1 as shown in the following exhibit.



You plan to create a custom parser named Parser 1. You need to use Query1 in Parser1. What should you do first?

- A. Remove line 2.
- B. In line 4. remove the TimeGenerated predicate.
- C. Remove line 5.
- D. In line 3, replace the 'contains operator with the !has operator.

Answer: A

Explanation:

This can be confirmed by referring to the official Microsoft documentation on creating custom log queries in Azure Sentinel, which states that the “has” operator should not be used in the query, and that it is unnecessary.

Reference: <https://docs.microsoft.com/en-us/azure/sentinel/query-custom-logs>

NEW QUESTION 12

- (Topic 4)

You need to configure Microsoft Cloud App Security to generate alerts and trigger remediation actions in response to external sharing of confidential files. Which two actions should you perform in the Cloud App Security portal? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

- A. From Settings, select Information Protection, select Azure Information Protection, and then select Only scan files for Azure Information Protection classification labels and content inspection warnings from this tenant
- B. Select Investigate files, and then filter App to Office 365.
- C. Select Investigate files, and then select New policy from search
- D. From Settings, select Information Protection, select Azure Information Protection, and then select Automatically scan new files for Azure Information Protection classification labels and content inspection warnings
- E. From Settings, select Information Protection, select Files, and then enable file monitoring.
- F. Select Investigate files, and then filter File Type to Document.

Answer: DE

Explanation:

Reference:

<https://docs.microsoft.com/en-us/cloud-app-security/tutorial-dlp> <https://docs.microsoft.com/en-us/cloud-app-security/azip-integration>

NEW QUESTION 13

- (Topic 4)

You need to meet the Microsoft Sentinel requirements for App1. What should you configure for App1?

- A. an API connection
- B. a trigger
- C. an connector
- D. authorization

Answer: B

NEW QUESTION 14

HOTSPOT - (Topic 4)

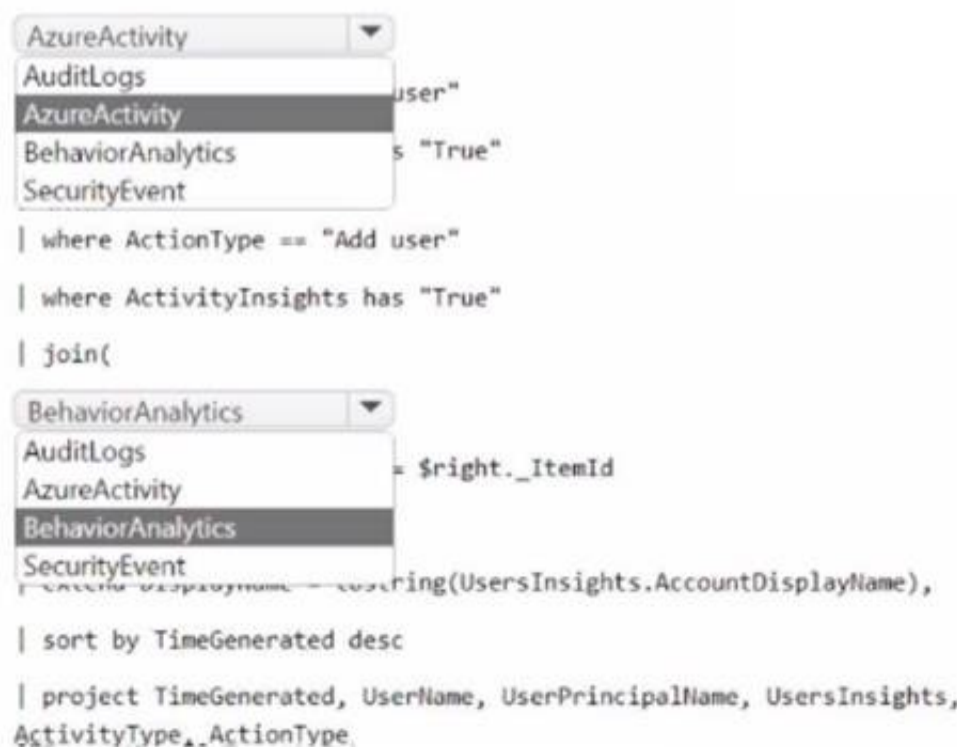
You have a Microsoft Sentinel workspace named sws1.

You need to create a query that will detect when a user creates an unusually large numbers of Azure AD user accounts.

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

NOTE: Each correct selection is worth one point.

Answer Area



The screenshot shows a query editor interface with two dropdown menus. The first dropdown menu is open, showing options: AzureActivity, AuditLogs, AzureActivity, BehaviorAnalytics, and SecurityEvent. The second dropdown menu is also open, showing options: BehaviorAnalytics, AuditLogs, AzureActivity, BehaviorAnalytics, and SecurityEvent. The query text below the dropdowns is as follows:

```

| where ActionType == "Add user"
| where ActivityInsights has "True"
| join(
BehaviorAnalytics
= $right._ItemId
) on (UsersInsights.AccountDisplayName),
| sort by TimeGenerated desc
| project TimeGenerated, Username, UserPrincipalName, UsersInsights,
ActivityType, ActionType

```

Solution:

Answer Area

```

AzureActivity
AuditLogs
AzureActivity
BehaviorAnalytics
SecurityEvent
| where ActionType == "Add user"
| where ActivityInsights has "True"
| join(
BehaviorAnalytics
AuditLogs
AzureActivity
BehaviorAnalytics
SecurityEvent
| where ActivityInsights has "True"
| sort by TimeGenerated desc
| project TimeGenerated, Username, UserPrincipalName, UsersInsights,
ActivityType, ActionType

```

Does this meet the goal?

- A. Yes
- B. No

Answer: A

NEW QUESTION 15

DRAG DROP - (Topic 4)

A company wants to analyze by using Microsoft 365 Apps.

You need to describe the connected experiences the company can use.

Which connected experiences should you describe? To answer, drag the appropriate connected experiences to the correct description. Each connected experience may be used once, more than once, or not at all. You may need to drag the split between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

Solution:

Does this meet the goal?

- A. Yes
- B. No

Answer: A

NEW QUESTION 16

- (Topic 4)

A security administrator receives email alerts from Azure Defender for activities such as potential malware uploaded to a storage account and potential successful brute force attacks.

The security administrator does NOT receive email alerts for activities such as antimalware action failed and suspicious network activity. The alerts appear in Azure Security Center.

You need to ensure that the security administrator receives email alerts for all the activities.

What should you configure in the Security Center settings?

- A. the severity level of email notifications
- B. a cloud connector
- C. the Azure Defender plans
- D. the integration settings for Threat detection

Answer: A

Explanation:

Reference:

<https://techcommunity.microsoft.com/t5/microsoft-365-defender/get-email-notifications-on-new-incidents-from-microsoft-365/ba-p/2012518>

NEW QUESTION 17

- (Topic 4)

You are configuring Azure Sentinel.

You need to send a Microsoft Teams message to a channel whenever a sign-in from a suspicious IP address is detected.

Which two actions should you perform in Azure Sentinel? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

- A. Add a playbook.
- B. Associate a playbook to an incident.
- C. Enable Entity behavior analytics.
- D. Create a workbook.
- E. Enable the Fusion rule.

Answer: AB

Explanation:

Reference:

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

NEW QUESTION 18

- (Topic 4)

Your company stores the data for every project in a different Azure subscription. All the subscriptions use the same Azure Active Directory (Azure AD) tenant.

Every project consists of multiple Azure virtual machines that run Windows Server. The Windows events of the virtual machines are stored in a Log Analytics workspace in each machine's respective subscription.

You deploy Azure Sentinel to a new Azure subscription.

You need to perform hunting queries in Azure Sentinel to search across all the Log Analytics workspaces of all the subscriptions.

Which two actions should you perform? Each correct answer presents part of the solution. NOTE: Each correct selection is worth one point.

- A. Add the Security Events connector to the Azure Sentinel workspace.
- B. Create a query that uses the workspace expression and the union operator.
- C. Use the alias statement.
- D. Create a query that uses the resource expression and the alias operator.
- E. Add the Azure Sentinel solution to each workspace.

Answer: BE

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/sentinel/extend-sentinel-across-workspaces-tenants>

NEW QUESTION 19

- (Topic 4)

You have an Azure subscription that contains an Microsoft Sentinel workspace.

You need to create a playbook that will run automatically in response to an Microsoft Sentinel alert.

What should you create first?

- A. a trigger in Azure Functions
- B. an Azure logic app
- C. a hunting query in Microsoft Sentinel
- D. an automation rule in Microsoft Sentinel

Answer: D

NEW QUESTION 20

- (Topic 4)

You receive a security bulletin about a potential attack that uses an image file.

You need to create an indicator of compromise (IoC) in Microsoft Defender for Endpoint to prevent the attack.

Which indicator type should you use?

- A. a URL/domain indicator that has Action set to Alert only
- B. a URL/domain indicator that has Action set to Alert and block
- C. a file hash indicator that has Action set to Alert and block
- D. a certificate indicator that has Action set to Alert and block

Answer: C

Explanation:

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/indicator-file?view=o365-worldwide>

NEW QUESTION 21

- (Topic 4)

You have an Azure subscription that uses Microsoft Defender for Endpoint.

You need to ensure that you can allow or block a user-specified range of IP addresses and URLs.

What should you enable first in the advanced features from the Endpoints Settings in the Microsoft 365 Defender portal?

- A. endpoint detection and response (EDR) in block mode
- B. custom network indicators
- C. web content filtering
- D. Live response for servers

Answer: A

NEW QUESTION 22

HOTSPOT - (Topic 4)

You have an Azure subscription that uses Microsoft Sentinel and contains a user named User1.

You need to ensure that User1 can enable User and Entity Behavior Analytics (UEBA) for entity behavior in Azure AD. The solution must use The principle of least privilege.

Which roles should you assign to User1? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Azure AD role:

- Global administrator
- Identity Governance Administrator
- Security administrator**
- Security operator

Azure role:

- Microsoft Sentinel Automation Contributor
- Microsoft Sentinel Contributor**
- Security Admin
- Security Assessment Contributor

Solution:

Answer Area

Azure AD role:

- Global administrator
- Identity Governance Administrator
- Security administrator**
- Security operator

Azure role:

- Microsoft Sentinel Automation Contributor
- Microsoft Sentinel Contributor**
- Security Admin
- Security Assessment Contributor

Does this meet the goal?

- A. Yes
- B. No

Answer: A

NEW QUESTION 23

DRAG DROP - (Topic 4)

You have an Azure subscription.

You need to delegate permissions to meet the following requirements:

? Enable and disable Azure Defender.

? Apply security recommendations to resource.

The solution must use the principle of least privilege.

Which Azure Security Center role should you use for each requirement? To answer, drag the appropriate roles to the correct requirements. Each role may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

Roles

- Security Admin
- Resource Group Owner
- Subscription Contributor
- Subscription Owner

Answer Area

Enable and disable Azure Defender:

Apply security recommendations to a resource:

Solution:

Roles

- Security Admin
- Resource Group Owner
- Subscription Contributor
- Subscription Owner

Answer Area

Enable and disable Azure Defender:

Apply security recommendations to a resource:

Does this meet the goal?

- A. Yes
- B. No

Answer: A

NEW QUESTION 24

HOTSPOT - (Topic 4)

You have a Microsoft 365 E5 subscription.

You need to create a hunting query that will return every email that contains an attachment named Document.pdf. The query must meet the following requirements:

- Only show emails sent during the last hour.
- Optimize query performance.

How should you complete the query? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Answer Area

EmailAttachmentInfo

```

| join DeviceFileEvents on SHA256
| join kind=inner (DeviceFileEvents | where Timestamp > ago(1h)) on SHA256
| where Timestamp > ago(1h)
| where Timestamp < ago(1h)
```

| where Subject == "Document Attachment" and FileName == "Document.pdf"

```

| join DeviceFileEvents on SHA256
| join kind=inner (DeviceFileEvents | where Timestamp > ago(1h)) on SHA256
| where Timestamp > ago(1h)
| where Timestamp < ago(1h)
```

Solution:

Answer Area

EmailAttachmentInfo

```
| join DeviceFileEvents on SHA256
| join kind=inner (DeviceFileEvents | where Timestamp > ago(1h)) on SHA256
| where Timestamp > ago(1h)
| where Timestamp < ago(1h)

| where Subject == "Document Attachment" and FileName == "Document.pdf"
```

```
| join DeviceFileEvents on SHA256
| join kind=inner (DeviceFileEvents | where Timestamp > ago(1h)) on SHA256
| where Timestamp > ago(1h)
| where Timestamp < ago(1h)
```

Does this meet the goal?

- A. Yes
- B. No

Answer: A

NEW QUESTION 25

.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questions and Answers in PDF Format

SC-200 Practice Exam Features:

- * SC-200 Questions and Answers Updated Frequently
- * SC-200 Practice Questions Verified by Expert Senior Certified Staff
- * SC-200 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- * SC-200 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

100% Actual & Verified — Instant Download, Please Click
[Order The SC-200 Practice Test Here](#)