Microsoft

Exam Questions SC-200

Microsoft Security Operations Analyst

NEW QUESTION 1
- (Topic 1)
You need to complete the query for failed sign-ins to meet the technical requirements. Where can you find the column name to complete the where clause?

A. Security alerts in Azure Security Center
B. Activity log in Azure
C. Azure Advisor
D. the query windows of the Log Analytics workspace

Answer: D

NEW QUESTION 2
DRAG DROP - (Topic 2)
You need to add notes to the events to meet the Azure Sentinel requirements.
Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of action to the answer area and arrange them in the correct order.

A. Mastered
B. Not Mastered

Answer: A

Explanation:

NEW QUESTION 3
HOTSPOT - (Topic 2)
You need to implement Microsoft Defender for Cloud to meet the Microsoft Defender for Cloud requirements and the business requirements. 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.

Answer Area

Log Analytics workspace to use:	▼
A new Log Analytics workspace in the East US Azure region
Default workspace created by Azure Security Center
LA1

Windows security events to collect:	▼
All Events
Common
Minimal

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

Log Analytics workspace to use:	▼
A new Log Analytics workspace in the East US Azure region
Default workspace created by Azure Security Center
LA1 _

Windows security events to collect:	▼
All Events_
Common_
Minimal

NEW QUESTION 4
HOTSPOT - (Topic 2)
You need to create the analytics rule to meet the Azure Sentinel requirements. What should you do? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Answer Area

Create the rule of type:	▼
Fusion
Microsoft incident creation
Scheduled

Configure the playbook to include:	▼
Diagnostics settings
A service principal
A trigger

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

Create the rule of type: ▼
Fusion
Microsoft incident creation
Scheduled

Configure the playbook to include: ▼
Diagnostics settings
A service principal
A trigger

NEW QUESTION 5
- (Topic 2)
You need to restrict cloud apps running on CLIENT1 to meet the Microsoft Defender for Endpoint requirements.
Which two configurations should you modify? Each correct answer present part of the
solution.
NOTE: Each correct selection is worth one point.

A. the Onboarding settings from Device management in Microsoft Defender Security Center
B. Cloud App Security anomaly detection policies
C. Advanced features from Settings in Microsoft Defender Security Center
D. the Cloud Discovery settings in Cloud App Security

Answer: CD

Explanation:
All Cloud App Security unsanctioned apps must be blocked on the Windows 10 computers by using Microsoft Defender for Endpoint.
Reference:
https://docs.microsoft.com/en-us/cloud-app-security/mde-govern

NEW QUESTION 6
- (Topic 2)
You need to implement the Azure Information Protection requirements. What should you configure first?

A. Device health and compliance reports settings in Microsoft Defender Security Center
B. scanner clusters in Azure Information Protection from the Azure portal
C. content scan jobs in Azure Information Protection from the Azure portal
D. Advanced features from Settings in Microsoft Defender Security Center

Answer: D

Explanation:
https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender- atp/information- protection-in-windows-overview

NEW QUESTION 7
- (Topic 3)
You need to ensure that the Group1 members can meet the Microsoft Sentinel requirements.
Which role should you assign to Group1?

A. Microsoft Sentinel Automation Contributor
B. Logic App Contributor
C. Automation Operator
D. Microsoft Sentinel Playbook Operator

Answer: D

NEW QUESTION 8
HOTSPOT - (Topic 3)
You need to implement the Microsoft Sentinel NRT rule for monitoring the designated break glass account. The solution must meet the Microsoft Sentinel
requirements.
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

SigninLogs

join	kind=inner	GetWatchlist	('breakglass_account')
join		_GetWatchlist	
lookup		extenal_table	
union		materialized_view	

on $left.UserPrincipalName == $right.SearchKey

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

SigninLogs

join	kind=inner	_GetWatchlist_	('breakglass_account')
join		_GetWatchlist	
lookup		extenal_table	
union		materialized_view	

on $left.UserPrincipalName == $right.SearchKey

NEW QUESTION 9
- (Topic 4)
You use Azure Sentinel.
You need to receive an immediate alert whenever Azure Storage account keys are enumerated. Which two actions should you perform? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

A. Create a livestream
B. Add a data connector
C. Create an analytics rule
D. Create a hunting query.
E. Create a bookmark.

Answer: BC

Explanation:
B: To add a data connector, you would use the Azure Sentinel data connectors feature to connect to your Azure subscription and to configure log data collection for Azure Storage account key enumeration events.
C: After adding the data connector, you need to create an analytics rule to analyze the log data from the Azure storage connector, looking for the specific event of Azure storage account keys enumeration. This rule will trigger an alert when it detects the specific event, allowing you to take immediate action.

NEW QUESTION 10
- (Topic 4)
You have a Microsoft 365 subscription that contains 1,000 Windows 10 devices. The devices have Microsoft Office 365 installed.
You need to mitigate the following device threats:
? Microsoft Excel macros that download scripts from untrusted websites
? Users that open executable attachments in Microsoft Outlook
? Outlook rules and forms exploits
What should you use?

A. Microsoft Defender Antivirus
B. attack surface reduction rules in Microsoft Defender for Endpoint
C. Windows Defender Firewall
D. adaptive application control in Azure Defender

Answer: B

Explanation:

Reference:
https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/overview-attack-surface-reduction?view=o365-worldwide

NEW QUESTION 10
- (Topic 4)
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 Azure Sentinel.
You need to create an incident in Azure Sentinel when a sign-in to an Azure virtual machine from a malicious IP address is detected.
Solution: You create a livestream from a query. Does this meet the goal?

A. Yes
B. No

Answer: B

Explanation:

Reference:
https://docs.microsoft.com/en-us/azure/sentinel/connect-azure-security-center

NEW QUESTION 12
DRAG DROP - (Topic 4)
You have an Azure subscription that contains the users shown in the following table.

Name	Role
User1	Security administrator
User2	Security reader
User3	Contributor

You need to delegate the following tasks:
• Enable Microsoft Defender for Servers on virtual machines.
• Review security recommendations and enable server vulnerability scans. The solution must use the principle of least privilege.
Which user should perform each task? To answer, drag the appropriate users to the correct tasks. Each user 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.

Users	Answer Area	
User1	Enable Microsoft Defender for Servers on virtual machines:	
User2	Review security recommendations and enable server vulnerability scans:	
User3		

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Users	Answer Area	
User1	Enable Microsoft Defender for Servers on virtual machines:	User1
User2	Review security recommendations and enable server vulnerability scans:	User2
User3		

NEW QUESTION 17
HOTSPOT - (Topic 4)
You have an Azure Storage account that will be accessed by multiple Azure Function apps during the development of an application.
You need to hide Azure Defender alerts for the storage account.
Which entity type and field should you use in a suppression rule? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Entity type:

IP address
Azure Resource
Host
User account

Field:

Name
Resource Id
Address
Command line

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Entity type:

IP address
Azure Resource
Host
User account

Field:

Name
Resource Id
Address
Command line

NEW QUESTION 18
HOTSPOT - (Topic 4)
You have a Microsoft Sentinel workspace that contains a custom workbook.
You need to query the number of daily security alerts. The solution must meet the following requirements:
• Identify alerts that occurred during the last 30 days.
• Display the results in a timechart.
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

```
SecurityAlert
| where TimeGenerated >= ago(30d)
|  [ lookup / project / summarize ▼ ]  count() by ProviderName,  [ bin / make series / range ▼ ]  (TimeGenerated, 1d)
| render timechart
```

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

```
SecurityAlert
| where TimeGenerated >= ago(30d)
|  [ lookup / project / summarize ▼ ]  count() by ProviderName,  [ bin / make series / range ▼ ]  (TimeGenerated, 1d)
| render timechart
```

NEW QUESTION 23
HOTSPOT - (Topic 4)
You have a Microsoft 365 E5 subscription that uses Microsoft Teams.
You need to perform a content search of Teams chats for a user by using the Microsoft Purview compliance portal. The solution must minimize the scope of the search.
How should you configure the content search? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Answer Area

Locations: [Exchange mailboxes ▼]
- Exchange mailboxes
- Exchange public folders
- SharePoint sites

Keywords: [Kind ▼]
- Category
- ItemClass
- Kind

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

Locations: [Exchange mailboxes ▼]
- Exchange mailboxes
- Exchange public folders
- SharePoint sites

Keywords: [Kind ▼]
- Category
- ItemClass
- Kind

NEW QUESTION 28
HOTSPOT - (Topic 4)
You have a Microsoft 365 E5 subscription that contains two users named User! and User2. You have the hunting query shown in the following exhibit.

```
1  AuditLogs
2  | where TimeGenerated >ago(7d)
3  | where OperationName == "Add user"
4  | project AddedTime - TimeGenerated, user - tostring(TargetResources[@].userPrincipalName)
5  | join (AzureActivity
6  | where OperationName == "Create role assignment"
7  | project OperationName, RoleAssignmentTime - TimeGenerated, user - Caller) on user
8  | project-away user1
9
```

The users perform the following anions:
• User1 assigns User2 the Global administrator role.
• User1 creates a new user named User3 and assigns the user a Microsoft Teams license.
• User2 creates a new user named User4 and assigns the user the Security reader role.
• User2 creates a new user named User5 and assigns the user the Security operator role. For each of the following statements, select Yes if the statement is true. Otherwise, select
No.
NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
The query will identify the role assignment of User2.	○	○
The query will identify the creation of User3.	○	○
The query will identify the creation of User5.	○	○

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

Statements	Yes	No
The query will identify the role assignment of User2.	○	[○]
The query will identify the creation of User3.	[○]	○
The query will identify the creation of User5.	[○]	○

NEW QUESTION 29
- (Topic 4)
You have the following environment:
? Azure Sentinel
? A Microsoft 365 subscription
? Microsoft Defender for Identity
? An Azure Active Directory (Azure AD) tenant
You configure Azure Sentinel to collect security logs from all the Active Directory member servers and domain controllers.
You deploy Microsoft Defender for Identity by using standalone sensors.
You need to ensure that you can detect when sensitive groups are modified in Active Directory.
Which two actions should you perform? Each correct answer presents part of the solution. NOTE: Each correct selection is worth one point.

A. Configure the Advanced Audit Policy Configuration settings for the domain controllers.
B. Modify the permissions of the Domain Controllers organizational unit (OU).
C. Configure auditing in the Microsoft 365 compliance center.
D. Configure Windows Event Forwarding on the domain controllers.

Answer: AD

Explanation:
Reference:
https://docs.microsoft.com/en-us/defender-for-identity/configure-windows-event-collection https://docs.microsoft.com/en-us/defender-for-identity/configure-event-collection

NEW QUESTION 30
- (Topic 4)
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

Answer: B

NEW QUESTION 33
- (Topic 4)
You create a hunting query in Azure Sentinel.
You need to receive a notification in the Azure portal as soon as the hunting query detects a match on the query. The solution must minimize effort.
What should you use?

A. a playbook
B. a notebook
C. a livestream
D. a bookmark

Answer: C

Explanation:
Use livestream to run a specific query constantly, presenting results as they come in.
Reference:
https://docs.microsoft.com/en-us/azure/sentinel/hunting

NEW QUESTION 36
- (Topic 4)
Your company deploys the following services:
? Microsoft Defender for Identity
? Microsoft Defender for Endpoint
? Microsoft Defender for Office 365
You need to provide a security analyst with the ability to use the Microsoft 365 security center. The analyst must be able to approve and reject pending actions generated by Microsoft Defender for Endpoint. The solution must use the principle of least privilege.
Which two roles should assign to the analyst? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

A. the Compliance Data Administrator in Azure Active Directory (Azure AD)
B. the Active remediation actions role in Microsoft Defender for Endpoint
C. the Security Administrator role in Azure Active Directory (Azure AD)
D. the Security Reader role in Azure Active Directory (Azure AD)

Answer: BD

Explanation:
Reference:
https://docs.microsoft.com/en-us/microsoft-365/security/defender- endpoint/rbac?view=o365-worldwide

NEW QUESTION 38
- (Topic 4)
You need to minimize the effort required to investigate the Microsoft Defender for Identity false positive alerts. What should you review?

A. the status update time
B. the alert status
C. the certainty of the source computer
D. the resolution method of the source computer

Answer: B

NEW QUESTION 41
- (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 44
HOTSPOT - (Topic 4)
You have an Azure subscription that is linked to a hybrid Azure AD tenant and contains a Microsoft Sentinel workspace named Sentinel1.
You need to enable User and Entity Behavior Analytics (UEBA) for Sentinel 1 and configure UEBA to use data collected from Active Directory Domain Services (AD OS).
What should you do? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Answer Area

To the AD DS domain controllers, deploy:
| The Azure Connected Machine agent ▼ |
| Microsoft Defender for Identity sensors |
| **The Azure Connected Machine agent** |
| The Azure Monitor agent |
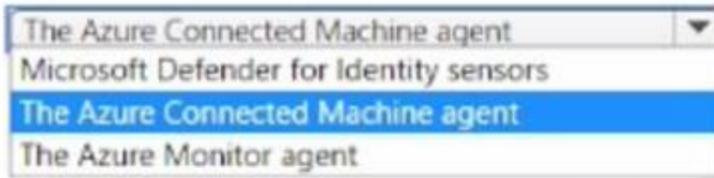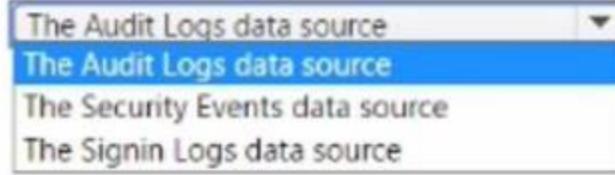
For Sentinel1, configure:
| The Audit Logs data source ▼ |
| **The Audit Logs data source** |
| The Security Events data source |
| The Signin Logs data source |

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

To the AD DS domain controllers, deploy:
| The Azure Connected Machine agent ▼ |
| Microsoft Defender for Identity sensors |
| **The Azure Connected Machine agent** |
| The Azure Monitor agent |
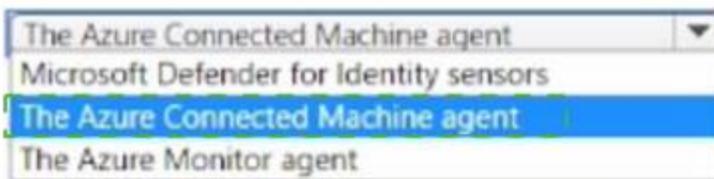
For Sentinel1, configure:
| The Audit Logs data source ▼ |
| **The Audit Logs data source** |
| The Security Events data source |
| The Signin Logs data source |
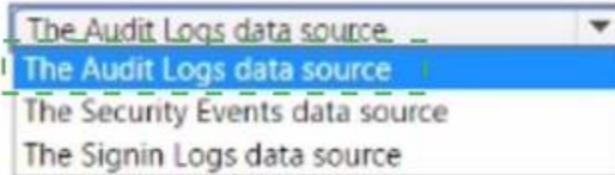
NEW QUESTION 49
- (Topic 4)
You have an Azure subscription that uses Microsoft Defender for Cloud and contains a storage account named storage1. You receive an alert that there was an unusually high volume of delete operations on the blobs in storage1. You need to identify which blobs were deleted. What should you review?

A. the activity logs of storage1
B. the Azure Storage Analytics logs
C. the alert details
D. the related entities of the alert

Answer: A

Explanation:
 To identify which blobs were deleted, you should review the activity logs of the storage account. The activity logs contain information about all the operations that have taken place in the storage account, including delete operations. These logs can be accessed in the Azure portal by navigating to the storage account, selecting "Activity log" under the "Monitoring" section, and filtering by the appropriate time range. You can also use Azure Monitor and Log Analytics to query and analyze the activity logs data. References:
? https://docs.microsoft.com/en-us/azure/storage/common/storage-activity-logs
? https://docs.microsoft.com/en-us/azure/azure-monitor/platform/activity-log-azure- storage

NEW QUESTION 53
- (Topic 4)
You have an Azure subscription that uses Microsoft Defender for Cloud and contains a storage account named storage1. You receive an alert that there was an unusually high volume of delete operations on the blobs in storage1.
You need to identify which blobs were deleted. What should you review?

A. the Azure Storage Analytics logs
B. the activity logs of storage1
C. the alert details
D. the related entities of the alert

Answer: B

NEW QUESTION 58
- (Topic 4)
Your company uses line-of-business apps that contain Microsoft Office VBA macros.
You plan to enable protection against downloading and running additional payloads from the Office VBA macros as additional child processes.
You need to identify which Office VBA macros might be affected.
Which two commands can you run to achieve the goal? Each correct answer presents a complete solution.
NOTE: Each correct selection is worth one point.

A. `Add-MpPreference -AttackSurfaceReductionRules_Ids D4F940AB -401B -4EFC -AADC -AD5F3C50688A -AttackSurfaceReductionRules_Actions Enabled`

B. `Set-MpPreference -AttackSurfaceReductionRules_Ids D4F940AB -401B -4EFC -AADC -AD5F3C50688A -AttackSurfaceReductionRules_Actions AuditMode`

C. `Add-MpPreference -AttackSurfaceReductionRules_Ids D4F940AB -401B -4EFC -AADC -AD5F3C50688A -AttackSurfaceReductionRules_Actions AuditMode`

D. `Set-MpPreference -AttackSurfaceReductionRules_Ids D4F940AB -401B -4EFC -AADC -AD5F3C50688A -AttackSurfaceReductionRules_Actions Enabled`

A. Option A
B. Option B
C. Option C
D. Option D

Answer: BC

Explanation:
 Reference:
https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/attack-surface- reduction

NEW QUESTION 59
- (Topic 4)
You create an Azure subscription named sub1.
In sub1, you create a Log Analytics workspace named workspace1.
You enable Azure Security Center and configure Security Center to use workspace1.
You need to ensure that Security Center processes events from the Azure virtual machines that report to workspace1.
What should you do?

A. In workspace1, install a solution.
B. In sub1, register a provider.
C. From Security Center, create a Workflow automation.
D. In workspace1, create a workbook.

Answer: A

Explanation:
 Reference:
https://docs.microsoft.com/en-us/azure/security-center/security-center-enable-data- collection

NEW QUESTION 60
- (Topic 4)
You have a Microsoft Sentinel workspace.
You receive multiple alerts for failed sign in attempts to an account. You identify that the alerts are false positives.
You need to prevent additional failed sign-in alerts from being generated for the account. The solution must meet the following requirements.
• Ensure that failed sign-in alerts are generated for other accounts.
• Minimize administrative effort What should do?

A. Create an automation rule.
B. Create a watchlist.
C. Modify the analytics rule.
D. Add an activity template to the entity behavior.

Answer: A

Explanation:
 An automation rule will allow you to specify which alerts should be suppressed, ensuring that failed sign-in alerts are generated for other accounts while minimizing administrative effort. To create an automation rule, navigate to the Automation Rules page in the Microsoft Sentinel workspace and configure the rule parameters to suppress the false positive alerts.

NEW QUESTION 63
- (Topic 4)
You have 50 Microsoft Sentinel workspaces.
You need to view all the incidents from all the workspaces on a single page in the Azure portal. The solution must minimize administrative effort.
Which page should you use in the Azure portal?

A. Microsoft Sentinel - Incidents
B. Microsoft Sentinel - Workbooks
C. Microsoft Sentinel
D. Log Analytics workspaces

Answer: D

NEW QUESTION 65
- (Topic 4)

You have an Azure subscription that uses Microsoft Sentinel.
You need to minimize the administrative effort required to respond to the incidents and remediate the security threats detected by Microsoft Sentinel.
Which two features should you use? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

A. Microsoft Sentinel bookmarks
B. Azure Automation runbooks
C. Microsoft Sentinel automation rules
D. Microsoft Sentinel playbooks
E. Azure Functions apps

Answer: CE

Explanation:
Reference: https://docs.microsoft.com/en-us/azure/sentinel/tutorial-respond-threats- playbook?tabs=LAC

NEW QUESTION 68
- (Topic 4)
You have an Azure subscription that uses Microsoft Defender for Cloud and contains 100 virtual machines that run Windows Server.
You need to configure Defender for Cloud to collect event data from the virtual machines. The solution must minimize administrative effort and costs.
Which two actions should you perform? Each correct answer presents part of the solution. NOTE: Each correct selection is worth one point.

A. From the workspace created by Defender for Cloud, set the data collection level to Common
B. From the Microsoft Endpoint Manager admin center, enable automatic enrollment.
C. From the Azure portal, create an Azure Event Grid subscription.
D. From the workspace created by Defender for Cloud, set the data collection level to All Events
E. From Defender for Cloud in the Azure portal, enable automatic provisioning for the virtual machines.

Answer: DE

NEW QUESTION 69
- (Topic 4)
You have an Azure subscription that use Microsoft Defender for Cloud and contains a user named User1.
You need to ensure that User1 can modify Microsoft Defender for Cloud security policies. The solution must use the principle of least privilege.
Which role should you assign to User1?

A. Security operator
B. Security Admin
C. Owner
D. Contributor

Answer: B

NEW QUESTION 70
- (Topic 4)
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

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

NEW QUESTION 73
- (Topic 4)
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 use Azure Security Center.
You receive a security alert in Security Center.
You need to view recommendations to resolve the alert in Security Center.
Solution: From Security alerts, you select the alert, select Take Action, and then expand the Mitigate the threat section.
Does this meet the goal?

A. Yes
B. No

Answer: A

Explanation:
Reference:
https://docs.microsoft.com/en-us/azure/security-center/security-center-managing-and-responding-alerts

NEW QUESTION 78
- (Topic 4)
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 Azure Sentinel.
You need to create an incident in Azure Sentinel when a sign-in to an Azure virtual machine from a malicious IP address is detected.
Solution: You create a scheduled query rule for a data connector. Does this meet the goal?

A. Yes
B. No

Answer: B

Explanation:
Reference:
https://docs.microsoft.com/en-us/azure/sentinel/connect-azure-security-center

NEW QUESTION 80
- (Topic 4)
You have a Microsoft Sentinel workspace that uses the Microsoft 365 Defender data connector.
From Microsoft Sentinel, you investigate a Microsoft 365 incident.
You need to update the incident to include an alert generated by Microsoft Defender for Cloud Apps.
What should you use?

A. the entity side panel of the Timeline card in Microsoft Sentinel
B. the investigation graph on the Incidents page of Microsoft Sentinel
C. the Timeline tab on the Incidents page of Microsoft Sentinel
D. the Alerts page in the Microsoft 365 Defender portal

Answer: A

NEW QUESTION 81
- (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 83
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


```
AzureActivity          ▼
AuditLogs
AzureActivity          user"
BehaviorAnalytics      s "True"
SecurityEvent

| where ActionType == "Add user"

| where ActivityInsights has "True"

| join(

BehaviorAnalytics      ▼
AuditLogs
AzureActivity          = $right._ItemId
BehaviorAnalytics
SecurityEvent
                ring(UsersInsights.AccountDisplayName),

| sort by TimeGenerated desc

| project TimeGenerated, UserName, UserPrincipalName, UsersInsights,
ActivityType,_ActionType
```

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area
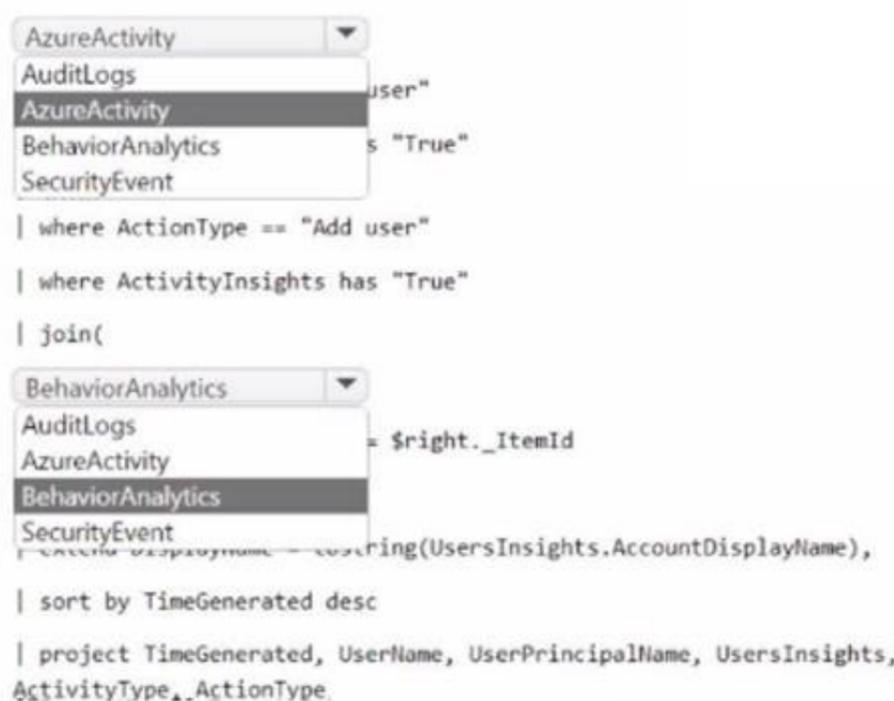
```
AzureActivity          ▼
  AuditLogs
  AzureActivity           user"
  BehaviorAnalytics     s "True"
  SecurityEvent

| where ActionType == "Add user"

| where ActivityInsights has "True"

| join(

BehaviorAnalytics      ▼
  AuditLogs
  AzureActivity          = $right._ItemId
  BehaviorAnalytics
  SecurityEvent
                  ...string(UsersInsights.AccountDisplayName),

| sort by TimeGenerated desc

| project TimeGenerated, UserName, UserPrincipalName, UsersInsights,
ActivityType,_ActionType
```

NEW QUESTION 86
- (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 87
HOTSPOT - (Topic 4)
You need to implement Microsoft Sentinel queries for Contoso and Fabrikam to meet the technical requirements.
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.

Answer Area

Minimum number of Log Analytics workspaces required in the Azure subscription of Fabrikam:

```
1              ▼
0
1
2
3
```

Query element required to correlate data between tenants:

```
workspace      ▼
extend
project
workspace
```

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

Minimum number of Log Analytics workspaces required in the Azure subscription of Fabrikam:	1
	0
	1
	2
	3

Query element required to correlate data between tenants:	workspace
	extend
	project
	workspace
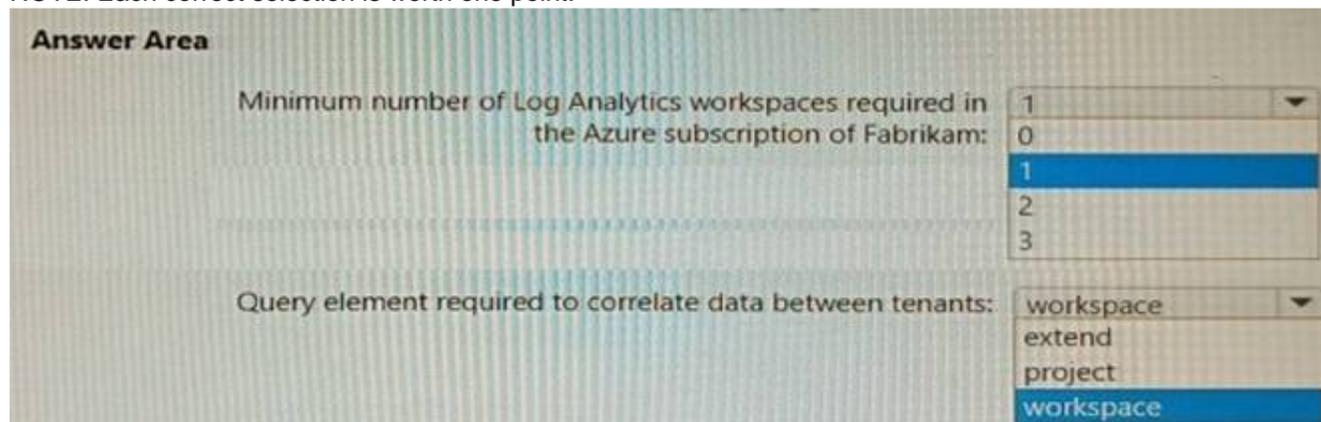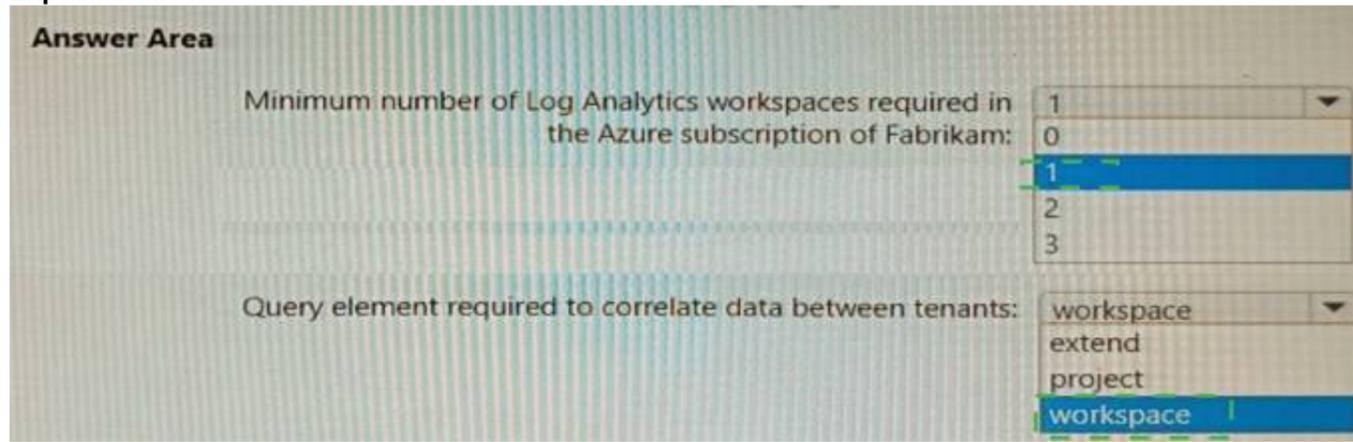
NEW QUESTION 89
- (Topic 4)
You are configuring Azure Sentinel.
You need to send a Microsoft Teams message to a channel whenever a sign-in from a suspicious IP address is detected.
Which two actions should you perform in Azure Sentinel? Each correct answer presents part of the solution.
NOTE: Each correct 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 93
HOTSPOT - (Topic 4)
Your network contains an on-premises Active Directory Domain Services (AD DS) domain that syncs with Azure AD.
You have a Microsoft 365 E5 subscription that uses Microsoft Defender 365.
You need to identify all the interactive authentication attempts by the users in the finance department of your company.
How should you complete the KQL query? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Answer Area

```
IdentityQueryEvents
  BehaviorAnalytics
  IdentityInfo
  IdentityQueryEvents
| where Department == 'Finance'
| project-rename objid = AccountObjectId
| join    AuditLogs                on $left.objid == $right.AccountObjectId
          AuditLogs
          IdentityLogonEvents
          SigninLogs
```
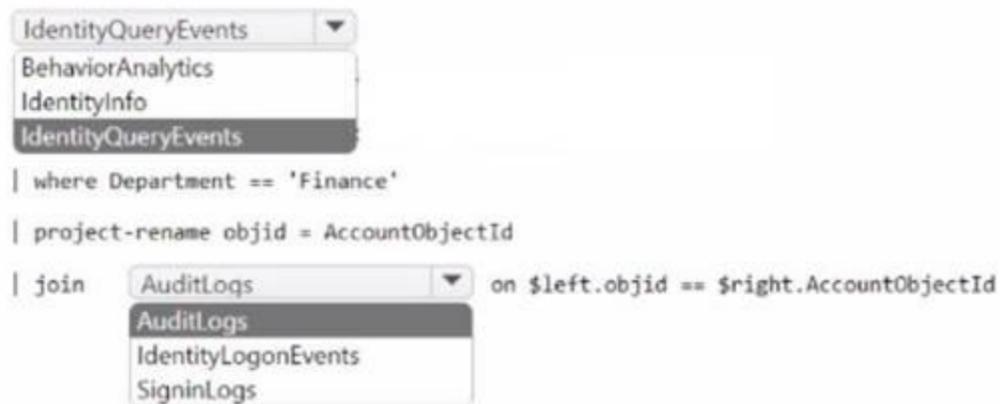
A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

```
IdentityQueryEvents        ▼
  BehaviorAnalytics
  IdentityInfo
  IdentityQueryEvents

| where Department == 'Finance'

| project-rename objid = AccountObjectId

| join   AuditLogs            ▼    on $left.objid == $right.AccountObjectId
           AuditLogs
           IdentityLogonEvents
           SigninLogs
```

NEW QUESTION 97
- (Topic 4)
You have a suppression rule in Azure Security Center for 10 virtual machines that are used for testing. The virtual machines run Windows Server.
You are troubleshooting an issue on the virtual machines.
In Security Center, you need to view the alerts generated by the virtual machines during the last five days.
What should you do?

A. Change the rule expiration date of the suppression rule.
B. Change the state of the suppression rule to Disabled.
C. Modify the filter for the Security alerts page.
D. View the Windows event logs on the virtual machines.

Answer: B

Explanation:
Reference:
https://docs.microsoft.com/en-us/azure/security-center/alerts-suppression-rules

NEW QUESTION 98
HOTSPOT - (Topic 4)
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.

```
Policy template type:      ▼
                      Access policy
                      Activity policy
                      Anomaly detection policy


Filter based on:           ▼
                      IP address tag
                      Source
                      User agent string
```

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Policy template type:

- Access policy
- Activity policy
- Anomaly detection policy

Filter based on:

- IP address tag
- Source
- User agent string

NEW QUESTION 102
- (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 105
- (Topic 4)
You create a custom analytics rule to detect threats in Azure Sentinel. You discover that the rule fails intermittently.
What are two possible causes of the failures? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

A. The rule query takes too long to run and times out.
B. The target workspace was deleted.
C. Permissions to the data sources of the rule query were modified.
D. There are connectivity issues between the data sources and Log Analytics

Answer: AD

NEW QUESTION 107
- (Topic 4)
You have a Microsoft 365 subscription that uses Microsoft 365 Defender. You need to identify all the entities affected by an incident.
Which tab should you use in the Microsoft 365 Defender portal?

A. Investigations
B. Devices
C. Evidence and Response
D. Alerts

Answer: C

Explanation:
The Evidence and Response tab shows all the supported events and suspicious entities in the alerts in the incident.
Reference: https://docs.microsoft.com/en-us/microsoft-365/security/defender/investigate- incidents

NEW QUESTION 109
- (Topic 4)
You have an Azure subscription that uses Microsoft Sentinel and contains 100 Linux virtual machines.
You need to monitor the virtual machines by using Microsoft Sentinel. The solution must meet the fallowing requirements:
• Minimize administrative effort
• Minimize the parsing required to read log data What should you configure?

A. REST API integration
B. a SysJog connector
C. a Log Analytics Data Collector API
D. a Common Event Format (CEF) connector

Answer: B

NEW QUESTION 114
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 Used? To answer select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Answer Area

Azure AD role:	Security administrator ▼
	Global administrator
	Identity Governance Administrator
	Security administrator
	Security operator

Azure role:	Microsoft Sentinel Contributor ▼
	Microsoft Sentinel Automation Contributor
	Microsoft Sentinel Contributor
	Security Admin
	Security Assessment Contributor

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

Azure AD role:	Security administrator ▼
	Global administrator
	Identity Governance Administrator
	Security administrator
	Security operator

Azure role:	Microsoft Sentinel Contributor ▼
	Microsoft Sentinel Automation Contributor
	Microsoft Sentinel Contributor
	Security Admin
	Security Assessment Contributor

NEW QUESTION 118
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:	Role
Apply security recommendations to a resource:	Role

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Roles	Answer Area

Roles

Security Admin

Resource Group Owner

Subscription Contributor

Subscription Owner

Answer Area

Enable and disable Azure Defender: | Security Admin

Apply security recommendations to a resource: | Subscription Contributor

NEW QUESTION 122
- (Topic 4)
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 have Linux virtual machines on Amazon Web Services (AWS). You deploy Azure Defender and enable auto-provisioning.
You need to monitor the virtual machines by using Azure Defender.
Solution: You manually install the Log Analytics agent on the virtual machines. Does this meet the goal?

A. Yes
B. No

Answer: B

Explanation:
Reference:
https://docs.microsoft.com/en-us/azure/defender-for-cloud/quickstart-onboard- machines?pivots=azure-arc

NEW QUESTION 127
- (Topic 4)
You have a Microsoft Sentinel workspace that contains the following incident. Brute force attack against Azure Portal analytics rule has been triggered.
You need to identify the geolocation information that corresponds to the incident. What should you do?

A. From Overview, review the Potential malicious events map.
B. From Incidents, review the details of the iPCustomEntity entity associated with the incident.
C. From Incidents, review the details of the AccouncCuscomEntity entity associated with the incident.
D. From Investigation, review insights on the incident entity.

Answer: A

Explanation:
Potential malicious events: When traffic is detected from sources that are known to be malicious, Microsoft Sentinel alerts you on the map. If you see orange, it is inbound traffic: someone is trying to access your organization from a known malicious IP address. If you see Outbound (red) activity, it means that data from your network is being streamed out of your organization to a known malicious IP address.

NEW QUESTION 130
- (Topic 4)
Your company uses Azure Sentinel to manage alerts from more than 10,000 IoT devices.
A security manager at the company reports that tracking security threats is increasingly difficult due to the large number of incidents.
You need to recommend a solution to provide a custom visualization to simplify the investigation of threats and to infer threats by using machine learning.
What should you include in the recommendation?

A. built-in queries
B. livestream
C. notebooks
D. bookmarks

Answer: C

Explanation:
Reference:
https://docs.microsoft.com/en-us/azure/sentinel/notebooks

NEW QUESTION 133
- (Topic 4)
You use Azure Security Center.
You receive a security alert in Security Center.
You need to view recommendations to resolve the alert in Security Center. What should you do?

A. From Security alerts, select the alert, select Take Action, and then expand the Prevent future attacks section.
B. From Security alerts, select Take Action, and then expand the Mitigate the threat section.
C. From Regulatory compliance, download the report.
D. From Recommendations, download the CSV report.

Answer: B

Explanation:
Reference:
https://docs.microsoft.com/en-us/azure/security-center/security-center-managing-and- responding-alerts

NEW QUESTION 134
DRAG DROP - (Topic 4)
You have a Microsoft 365 E5 subscription that uses Microsoft Exchange Online. You need to identify phishing email messages.
Which three cmdlets should you run in sequence? To answer, move the appropriate cmdlets from the list of cmdlets to the answer area and arrange them in the correct order.

Cmdlets	Answer Area
Connect-IPPSSession	
Start-ComplianceSearch	
New-ComplianceSearch	
Connect-ExchangeOnline	
Search-UnifiedAuditLog	

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Cmdlets	Answer Area
Connect-IPPSSession	New-ComplianceSearch
Start-ComplianceSearch	Connect-ExchangeOnline
New-ComplianceSearch	Search-UnifiedAuditLog
Connect-ExchangeOnline	
Search-UnifiedAuditLog	

NEW QUESTION 136
......

Thank You for Trying Our Product

We offer two products:

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

2nd - Questons 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