

Microsoft

Exam Questions SC-200

Microsoft Security Operations Analyst



NEW QUESTION 1

HOTSPOT - (Topic 1)

You need to recommend remediation actions for the Azure Defender alerts for Fabrikam.

What should you recommend for each threat? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Internal threat:

- Add resource locks to the key vault.
- Modify the access policy settings for the key vault.
- Modify the role-based access control (RBAC) settings for the key vault.

External threat:

- Implement Azure Firewall.
- Modify the Key Vault firewall settings.
- Modify the network security groups (NSGs).

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

Internal threat:

- Add resource locks to the key vault.
- Modify the access policy settings for the key vault.
- Modify the role-based access control (RBAC) settings for the key vault.

External threat:

- Implement Azure Firewall.
- Modify the Key Vault firewall settings.
- Modify the network security groups (NSGs).

NEW QUESTION 2

HOTSPOT - (Topic 1)

You need to create an advanced hunting query to investigate the executive team issue.

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

NOTE: Each correct selection is worth one point.

```


CloudAppEvents
DeviceFileEvents
DeviceProcessEvents

| where TimeStamp > ago(2d)

| summarize activityCount =  by FolderPath, FileName,
ActionType, AccountDisplayName

| where activityCount > 5
    
```

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

```

| where TimeStamp > ago(2d)
| summarize activityCount = avg(ActionType, AccountDisplayName) by FolderPath, FileName,
| where activityCount > 5
    
```

NEW QUESTION 3

- (Topic 1)

You need to remediate active attacks to meet the technical requirements. What should you include in the solution?

- A. Azure Automation runbooks
- B. Azure Logic Apps
- C. Azure FunctionsD Azure Sentinel livestreams

Answer: B

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/sentinel/automate-responses-with-playbooks>

NEW QUESTION 4

- (Topic 1)

You need to recommend a solution to meet the technical requirements for the Azure virtual machines. What should you include in the recommendation?

- A. just-in-time (JIT) access
- B. Azure Defender
- C. Azure Firewall
- D. Azure Application Gateway

Answer: B

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/security-center/azure-defender>

NEW QUESTION 5

DRAG DROP - (Topic 2)

You need to configure DC1 to meet the business requirements.

Which four 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
Provide domain administrator credentials to the litware.com Active Directory domain.	
Create an instance of Microsoft Defender for Identity.	
Provide global administrator credentials to the litware.com Azure AD tenant.	⬅️ ⬆️
Install the sensor on DC1.	➡️ ⬇️
Install the standalone sensor on DC1.	

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Text Description automatically generated with medium confidence

Step 1: log in to <https://portal.atp.azure.com> as a global admin

Step 2: Create the instance
 Step 3. Connect the instance to Active Directory Step 4. Download and install the sensor.

NEW QUESTION 6

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.

Actions	Answer Area
Add a bookmark and map an entity.	
From Azure Monitor, run a Log Analytics query.	
Add the query to favorites.	⬅️
Select a query result.	➡️
From the Azure Sentinel workspace, run a Log Analytics query.	⬆️
	⬆️

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Actions	Answer Area
Add a bookmark and map an entity.	From the Azure Sentinel workspace, run a Log Analytics query.
From Azure Monitor, run a Log Analytics query.	Select a query result.
Add the query to favorites.	Add a bookmark and map an entity.
Select a query result.	
From the Azure Sentinel workspace, run a Log Analytics query.	

NEW QUESTION 7

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: ▼

Default workspace created by Azure Security Center
LA1

Windows security events to collect: ▼

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 8

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 9

- (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 10

- (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 10

- (Topic 3)
 You need to ensure that the processing of incidents generated by rulequery1 meets the Microsoft Sentinel requirements.
 What should you create first?

- A. a playbook with an incident trigger
- B. a playbook with an entity trigger
- C. an Azure Automation rule
- D. a playbook with an alert trigger

Answer: A

NEW QUESTION 14

- (Topic 3)
 You need to implement the Defender for Cloud requirements. Which subscription-level role should you assign to Group1?

- A. Security Admin
- B. Owner
- C. Security Assessment Contributor
- D. Contributor

Answer: B

NEW QUESTION 16

HOTSPOT - (Topic 3)
 You need to implement the ASIM query for DNS requests. The solution must meet the Microsoft Sentinel requirements. How should you configure the query? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Answer Area

ASIM parser: 

- _Im_Dns
- _Im_Dns_InfobloxNIOS
- imDns

Filter: 

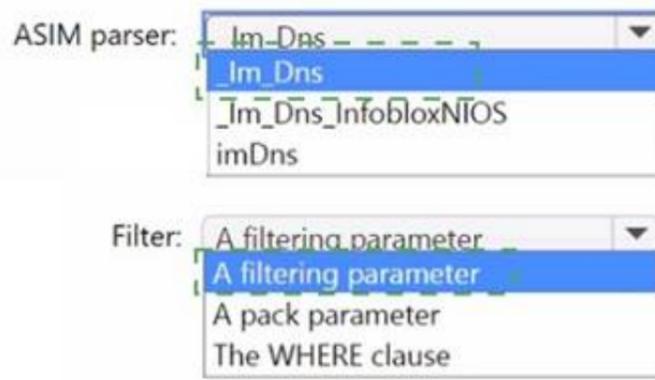
- A filtering parameter
- A pack parameter
- The WHERE clause

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area



NEW QUESTION 18

- (Topic 3)

You need to implement the scheduled rule for incident generation based on rulequery1. What should you configure first?

- A. entity mapping
- B. custom details
- C. event grouping
- D. alert details

Answer: D

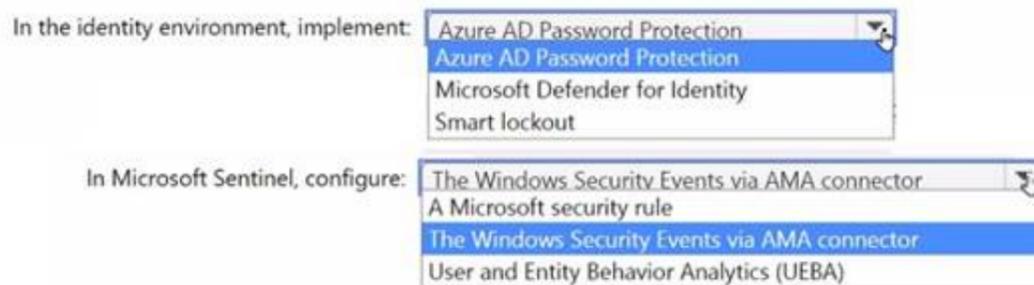
NEW QUESTION 19

HOTSPOT - (Topic 3)

You need to monitor the password resets. The solution must meet the Microsoft 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

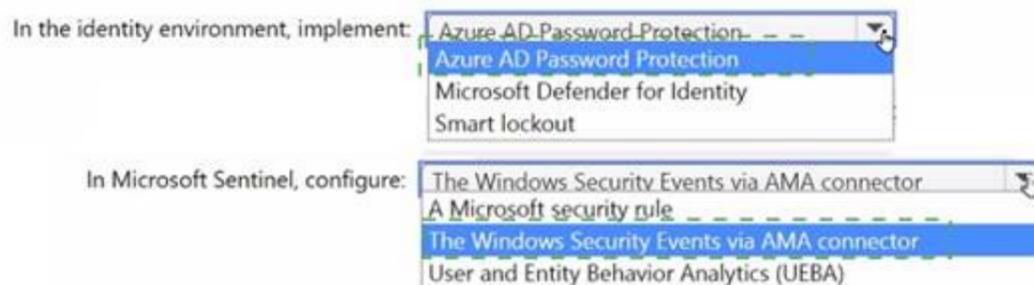


- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area



NEW QUESTION 24

- (Topic 4)

Your company uses Azure Sentinel.

A new security analyst reports that she cannot assign and dismiss incidents in Azure Sentinel. You need to resolve the issue for the analyst. The solution must use the principle of least privilege. Which role should you assign to the analyst?

- A. Azure Sentinel Responder
- B. Logic App Contributor
- C. Azure Sentinel Contributor
- D. Azure Sentinel Reader

Answer: A

Explanation:

Reference:

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

NEW QUESTION 26

- (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:

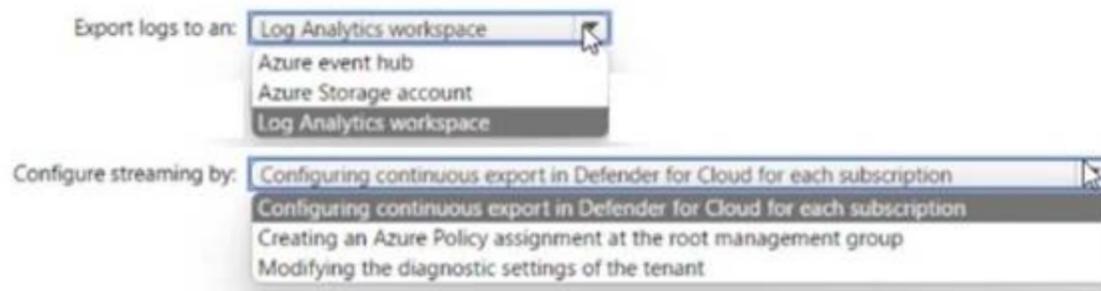
<https://docs.microsoft.com/en-us/azure/security-center/security-center-provide-security-contact-details>

NEW QUESTION 28

HOTSPOT - (Topic 4)

You have 100 Azure subscriptions that have enhanced security features in Microsoft Defender for Cloud enabled. All the subscriptions are linked to a single Azure AD tenant. You need to stream the Defender for Cloud logs to a syslog server. The solution must minimize administrative effort. What should you do? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point

Answer Area

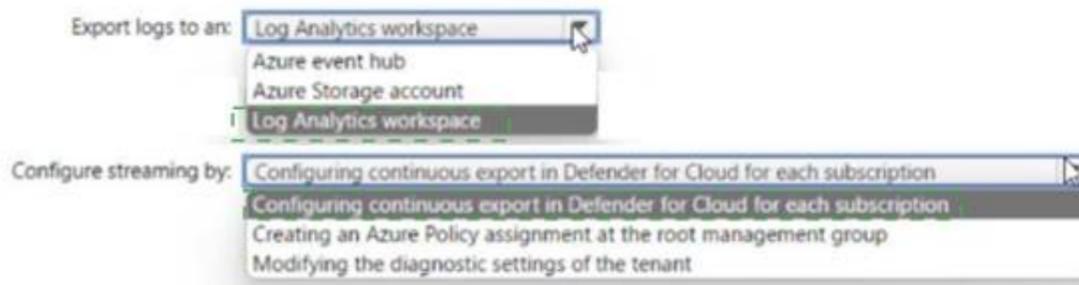


- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area



NEW QUESTION 33

- (Topic 4)

You have a custom analytics rule to detect threats in Azure Sentinel.

You discover that the analytics rule stopped running. The rule was disabled, and the rule name has a prefix of AUTO DISABLED.

What is a possible cause of the issue?

- A. There are connectivity issues between the data sources and Log Analytics.
- B. The number of alerts exceeded 10,000 within two minutes.
- C. The rule query takes too long to run and times out.
- D. Permissions to one of the data sources of the rule query were modified.

Answer: D

Explanation:

Reference:

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

NEW QUESTION 37

- (Topic 4)

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 DIP alert management dashboard of the Microsoft Purview compliance portal?

- A. the Details tab of the alert
- B. Management log

- C. the Sensitive Info Types tab of the alert
- D. the Events tab of the alert

Answer: B

NEW QUESTION 42

- (Topic 4)

You have an Azure subscription that contains a Microsoft Sentinel workspace. The workspace contains a Microsoft Defender for Cloud data connector. You need to customize which details will be included when an alert is created for a specific event. What should you do?

- A. Modify the properties of the connector.
- B. Create a Data Collection Rule (DCR).
- C. Create a scheduled query rule.
- D. Enable User and Entity Behavior Analytics (UEBA)

Answer: D

NEW QUESTION 46

DRAG DROP - (Topic 4)

You have an Azure subscription that contains 100 Linux virtual machines.

You need to configure Microsoft Sentinel to collect event logs from the virtual machines. 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.

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

NEW QUESTION 47

- (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 52

- (Topic 4)

You have a Microsoft Sentinel workspace named Workspace1 and 200 custom Advanced Security Information Model (ASIM) parsers based on the DNS schema. You need to make the 200 parsers available in Workspace1. The solution must minimize administrative effort. What should you do first?

- A. Copy the parsers to the Azure Monitor Logs page.
- B. Create a JSON file based on the DNS template.
- C. Create an XML file based on the DNS template.
- D. Create a YAML file based on the DNS template.

Answer: A

NEW QUESTION 56

HOTSPOT - (Topic 4)

You have a Microsoft 365 E5 subscription that contains two users named User1 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[0].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 actions:

- 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.	<input type="radio"/>	<input type="radio"/>
The query will identify the creation of User3.	<input type="radio"/>	<input type="radio"/>
The query will identify the creation of User5.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

Statements	Yes	No
The query will identify the role assignment of User2.	<input type="radio"/>	<input checked="" type="radio"/>
The query will identify the creation of User3.	<input checked="" type="radio"/>	<input type="radio"/>
The query will identify the creation of User5.	<input checked="" type="radio"/>	<input type="radio"/>

NEW QUESTION 58

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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

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

NEW QUESTION 62

- (Topic 4)

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

You have an Amazon Web Services (AWS) subscription. The subscription contains multiple virtual machines that run Windows Server.

You need to enable Microsoft Defender for Servers on the virtual machines.

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

- A. From Defender for Cloud, enable agentless scanning.
- B. Install the Azure Virtual Machine Agent (VM Agent) on each virtual machine.
- C. Onboard the virtual machines to Microsoft Defender for Endpoint.
- D. From Defender for Cloud, configure auto-provisioning.
- E. From Defender for Cloud, configure the AWS connector.

Answer: BC

NEW QUESTION 64

- (Topic 4)

You have two Azure subscriptions that use Microsoft Defender for Cloud.

You need to ensure that specific Defender for Cloud security alerts are suppressed at the root management group level. The solution must minimize administrative effort.

What should you do in the Azure portal?

- A. Create an Azure Policy assignment.
- B. Modify the Workload protections settings in Defender for Cloud.
- C. Create an alert rule in Azure Monitor.
- D. Modify the alert settings in Defender for Cloud.

Answer: D

Explanation:

You can use alerts suppression rules to suppress false positives or other unwanted security alerts from Defender for Cloud.

Note: To create a rule directly in the Azure portal:

* 1. From Defender for Cloud's security alerts page:

Select the specific alert you don't want to see anymore, and from the details pane, select Take action.

Or, select the suppression rules link at the top of the page, and from the suppression rules page select Create new suppression rule:

* 2. In the new suppression rule pane, enter the details of your new rule.

Your rule can dismiss the alert on all resources so you don't get any alerts like this one in the future.

Your rule can dismiss the alert on specific criteria - when it relates to a specific IP address, process name, user account, Azure resource, or location.

* 3. Enter details of the rule.

* 4. Save the rule.

Reference: <https://docs.microsoft.com/en-us/azure/defender-for-cloud/alerts-suppression-rules>

NEW QUESTION 67

- (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 70

DRAG DROP - (Topic 4)

You need to use an Azure Sentinel analytics rule to search for specific criteria in Amazon Web Services (AWS) logs and to generate incidents.

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.

a Microsoft 365 E5

Actions

Answer Area

- Create a rule by using the Changes to Amazon VPC settings rule template
- From Analytics in Azure Sentinel, create a Microsoft incident creation rule
- Add the Amazon Web Services connector
- Set the alert logic
- From Analytics in Azure Sentinel, create a custom analytics rule that uses a scheduled query
- Select a Microsoft security service
- Add the Syslog connector



- A. Mastered
- B. Not Mastered

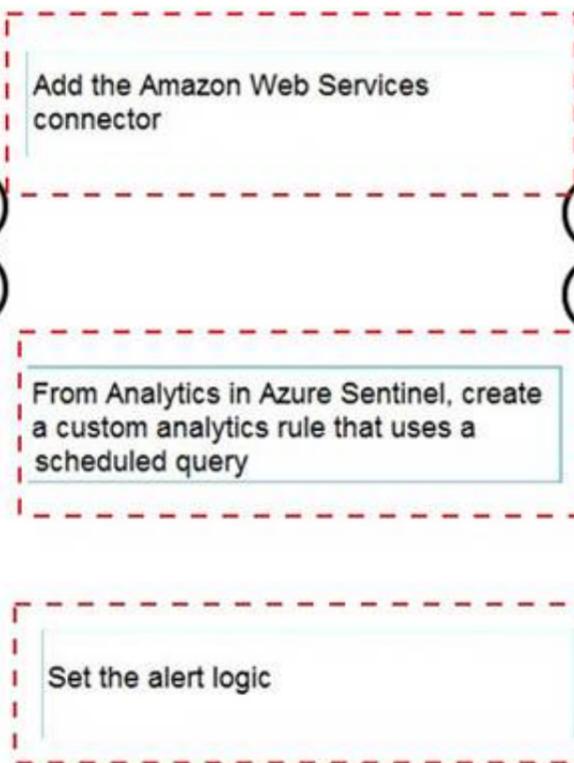
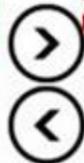
Answer: A

Explanation:

Actions

Answer Area

- Create a rule by using the Changes to Amazon VPC settings rule template
- From Analytics in Azure Sentinel, create a Microsoft incident creation rule
- Add the Amazon Web Services connector
- Set the alert logic
- From Analytics in Azure Sentinel, create a custom analytics rule that uses a scheduled query
- Select a Microsoft security service
- Add the Syslog connector



NEW QUESTION 72

- (Topic 4)

You have a Microsoft Sentinel workspace.

You need to prevent a built-in Advance Security information Model (ASIM) parse from being updated automatically.

What are two ways to achieve this goal? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

- A. Redeploy the built-in parse and specify a CallerContext parameter of any and a SourceSpecificParse parameter of any.
- B. Create a hunting query that references the built-in parse.
- C. Redeploy the built-in parse and specify a CallerContext parameter of built-in.
- D. Build a custom unify parse and include the build- parse version
- E. Create an analytics rule that includes the built-in parse

Answer: AD

NEW QUESTION 77

- (Topic 4)

You have an Azure subscription that uses Microsoft Defender for Cloud and contains a resource group named RG1. RG1. You need to configure just in time (JIT) VM access for the virtual machines in RG1. The solution must meet the following

- Limit the maximum request time to two hours.
- Limit protocol access to Remote Desktop Protocol (RDP) only.
- Minimize administrative effort. What should you use?

- A. Azure AD Privileged Identity Management (PIM)
- B. Azure Policy
- C. Azure Front Door
- D. Azure Bastion

Answer: A

NEW QUESTION 78

- (Topic 4)

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

Answer: D

NEW QUESTION 80

- (Topic 4)

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 Microsoft Defender for Cloud.
- C. Create a Microsoft Cloud App Security connector.
- D. Create an Azure AD Identity Protection connector.

Answer: AB

Explanation:

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, you should perform the following two actions:

? Create an Azure AD Identity Protection connector. This will allow you to monitor suspicious activities in your Azure AD tenant and detect malicious sign-ins.

? Create a custom rule based on the Office 365 connector templates. This will allow you to monitor and detect anomalous activities in the Microsoft 365 subscription. Reference: <https://docs.microsoft.com/en-us/azure/sentinel/fusion-rules>

NEW QUESTION 84

- (Topic 4)

You plan to create a custom Azure Sentinel query that will provide a visual representation of the security alerts generated by Azure Security Center. You need to create a query that will be used to display a bar graph. What should you include in the query?

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

Answer: B

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/azure-monitor/visualize/workbooks-chart-visualizations>

NEW QUESTION 89

- (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 93

HOTSPOT - (Topic 4)

You have an Azure subscription that contains a guest user named User1 and a Microsoft Sentinel workspace named workspace1. You need to ensure that User1 can triage Microsoft Sentinel incidents in workspace1. 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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

NEW QUESTION 98

- (Topic 4)

You are responsible for responding to Azure Defender for Key Vault alerts.

During an investigation of an alert, you discover unauthorized attempts to access a key vault from a Tor exit node.

What should you configure to mitigate the threat?

- A. Key Vault firewalls and virtual networks
- B. Azure Active Directory (Azure AD) permissions
- C. role-based access control (RBAC) for the key vault
- D. the access policy settings of the key vault

Answer: A

Explanation:

Reference:
<https://docs.microsoft.com/en-us/azure/key-vault/general/network-security>

NEW QUESTION 102

- (Topic 4)

You have a Microsoft Sentinel workspace named Workspace1.

You need to exclude a built-in, source-specific Advanced Security information Model (ASIM) parse from a built-in unified ASIM parser. What should you create in Workspace1?

- A. a watch list
- B. an analytic rule
- C. a hunting query
- D. a workbook

Answer: A

NEW QUESTION 106

- (Topic 4)

You create an Azure subscription.

You enable Azure Defender for the subscription.

You need to use Azure Defender to protect on-premises computers. What should you do on the on-premises computers?

- A. Install the Log Analytics agent.
- B. Install the Dependency agent.
- C. Configure the Hybrid Runbook Worker role.
- D. Install the Connected Machine agent.

Answer: A

Explanation:

Security Center collects data from your Azure virtual machines (VMs), virtual machine scale sets, IaaS containers, and non-Azure (including on-premises) machines to monitor for security vulnerabilities and threats.

Data is collected using:

The Log Analytics agent, which reads various security-related configurations and event logs from the machine and copies the data to your workspace for analysis. Examples of such data are: operating system type and version, operating system logs (Windows event logs), running processes, machine name, IP addresses, and logged in user.

Security extensions, such as the Azure Policy Add-on for Kubernetes, which can also provide data to Security Center regarding specialized resource types.

Reference:

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

NEW QUESTION 110

- (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 enable Azure Arc and onboard the virtual machines to Azure Arc. 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 111

- (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 115

- (Topic 4)

You have an Azure Sentinel deployment in the East US Azure region.

You create a Log Analytics workspace named LogsWest in the West US Azure region. You need to ensure that you can use scheduled analytics rules in the existing Azure

Sentinel deployment to generate alerts based on queries to LogsWest. What should you do first?

- A. Deploy Azure Data Catalog to the West US Azure region.
- B. Modify the workspace settings of the existing Azure Sentinel deployment
- C. Add Microsoft Sentinel to a workspace.
- D. Create a data connector in Azure Sentinel.

Answer: C

Explanation:

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

NEW QUESTION 119

HOTSPOT - (Topic 4)

You have an Microsoft Sentinel workspace named SW1.

You plan to create a custom workbook that will include a time chart.

You need to create a query that will identify the number of security alerts per day for each provider.

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)
| summarize count() by ProviderName,
```

timechart

- render
- materialize
- project
- render

(TimeGenerated, 1d)

- bin
- bin
- series_add
- series_fill_linear
- take

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

SecurityAlert

```
| where TimeGenerated >= ago(30d)
| summarize count() by ProviderName,
```

timechart

- render
- materialize
- project
- render

(TimeGenerated, 1d)

- bin
- bin
- series_add
- series_fill_linear
- take

NEW QUESTION 124

DRAG DROP - (Topic 4)

You have an Azure Sentinel deployment.

You need to query for all suspicious credential access activities.

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

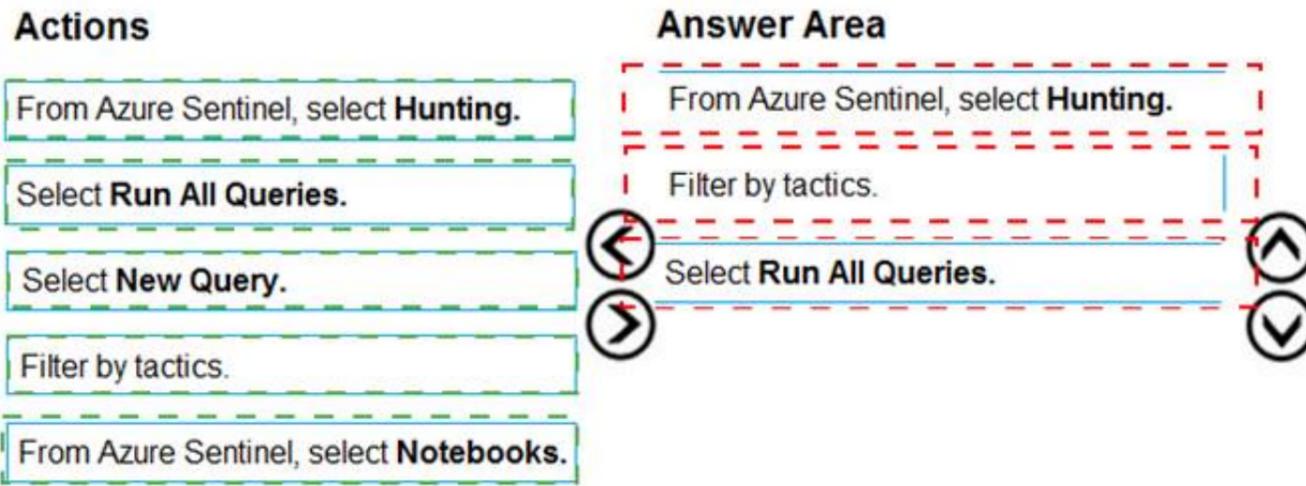
- From Azure Sentinel, select **Hunting**.
- Select **Run All Queries**.
- Select **New Query**.
- Filter by tactics.
- From Azure Sentinel, select **Notebooks**.



- A. Mastered
- B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 125

HOTSPOT - (Topic 4)

You have a Microsoft Sentinel workspace.

You need to create a KQL query that will identify successful sign-ins from multiple countries during the last three hours.

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

NOTE: Each correct selection is worth one point

```
let timeframe = ago(3h);
let threshold = 5;
imAuthentication
| where TimeGenerated > timeframe
| where EventType=='Logon' and EventResult=='Success'
| where isnotempty(SrcGeoCountry)
| summarize StartTime = min(TimeGenerated), EndTime = max(TimeGenerated), Vendors=make_set(EventVendor), Products=make_set(EventProduct), '
NumOfCountries = dcount( DstGeoCountry ) by TargetUserId, TargetUserPrincipalName, TargetUserType
| where NumOfCountries >= threshold
```

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

```
let timeframe = ago(3h);
let threshold = 5;
imAuthentication
| where TimeGenerated > timeframe
| where EventType=='Logon' and EventResult=='Success'
| where isnotempty(SrcGeoCountry)
| summarize StartTime = min(TimeGenerated), EndTime = max(TimeGenerated), Vendors=make_set(EventVendor), Products=make_set(EventProduct), '
NumOfCountries = dcount( DstGeoCountry ) by TargetUserId, TargetUserPrincipalName, TargetUserType
| where NumOfCountries >= threshold
```

NEW QUESTION 128

- (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 131

DRAG DROP - (Topic 4)
 DRAG DROP

You create a new Azure subscription and start collecting logs for Azure Monitor.

You need to configure Azure Security Center to detect possible threats related to sign-ins from suspicious IP addresses to Azure virtual machines. The solution must validate the configuration.

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

Actions	Answer Area
Change the alert severity threshold for emails to Medium .	
Copy an executable file on a virtual machine and rename the file as ASC_AlertTest_662jfi039N.exe.	
Enable Azure Defender for the subscription.	⬅️ ⬆️
Change the alert severity threshold for emails to Low .	➡️ ⬇️
Run the executable file and specify the appropriate arguments.	
Rename the executable file as AlertTest.exe.	

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Actions	Answer Area
Change the alert severity threshold for emails to Medium .	
Copy an executable file on a virtual machine and rename the file as ASC_AlertTest_662jfi039N.exe.	Enable Azure Defender for the subscription.
Enable Azure Defender for the subscription.	Copy an executable file on a virtual machine and rename the file as ASC_AlertTest_662jfi039N.exe.
Change the alert severity threshold for emails to Low .	Run the executable file and specify the appropriate arguments.
Run the executable file and specify the appropriate arguments.	
Rename the executable file as AlertTest.exe.	

NEW QUESTION 133

- (Topic 4)

You need to identify which mean time metrics to use to meet the Microsoft Sentinel requirements. Which workbook should you use?

- A. Analytics Efficiency
- B. Security Operations Efficiency
- C. Event Analyzer
- D. Investigation insights

Answer: C

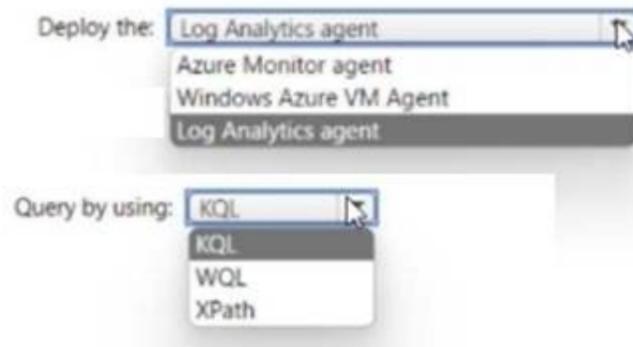
NEW QUESTION 138

HOTSPOT - (Topic 4)

You need to meet the Microsoft Sentinel requirements for collecting Windows Security event logs. What should you do? To answer, select the appropriate options

in the answer area. NOTE Each correct selection is worth one point.

Answer Area

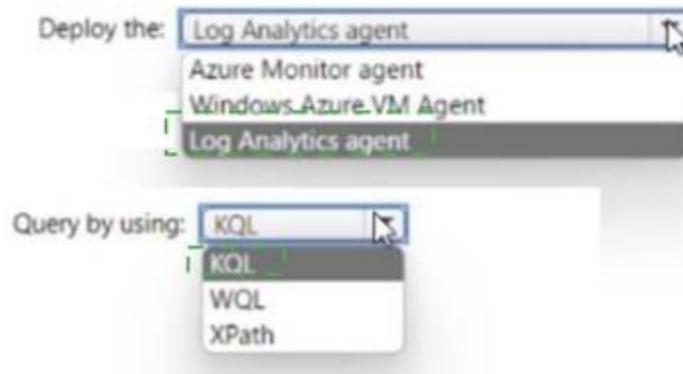


- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area



NEW QUESTION 143

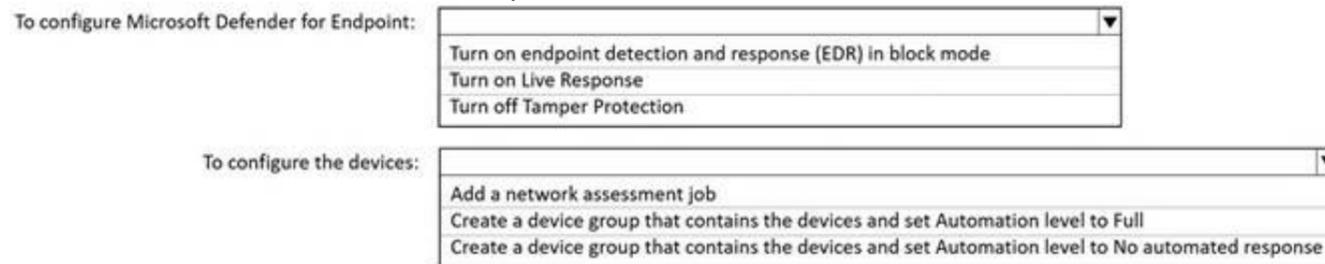
HOTSPOT - (Topic 4)

You have a Microsoft 365 E5 subscription that contains 200 Windows 10 devices enrolled in Microsoft Defender for Endpoint.

You need to ensure that users can access the devices by using a remote shell connection directly from the Microsoft 365 Defender portal. The solution must use the principle of least privilege.

What should you do in the Microsoft 365 Defender portal? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.



- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Box 1: Turn on Live Response

Live response is a capability that gives you instantaneous access to a device by using a remote shell connection. This gives you the power to do in-depth investigative work and take immediate response actions.

Box: 2 : Add a network assessment job

Network assessment jobs allow you to choose network devices to be scanned regularly and added to the device inventory.

NEW QUESTION 145

- (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 147

- (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 148

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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

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.

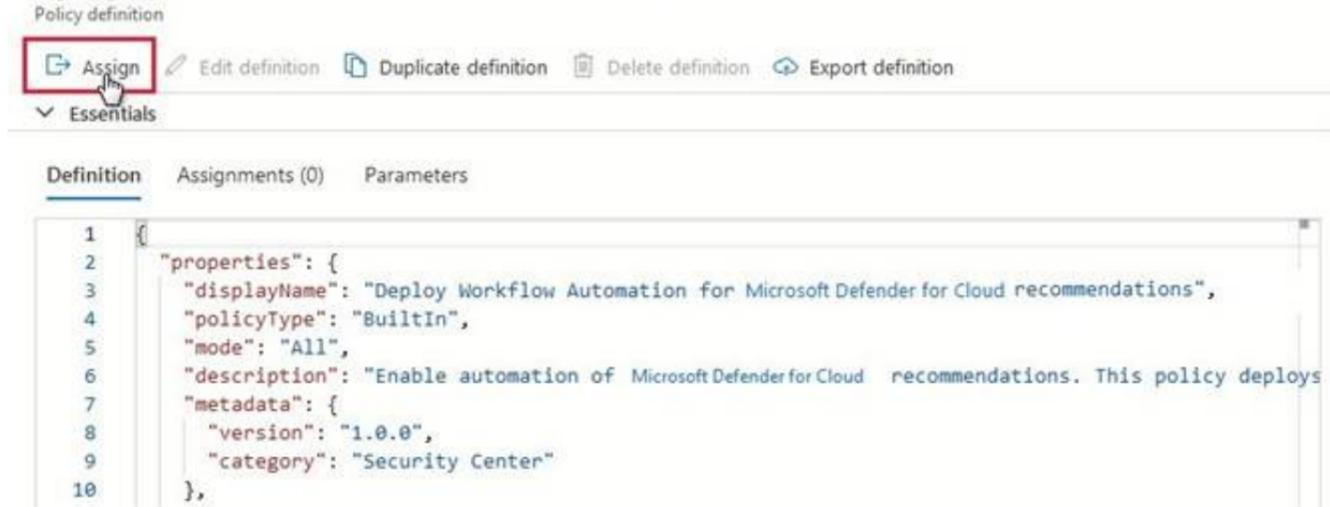
- * 3. From the Actions section, select visit the Logic Apps page to begin the Logic App creation process.
- * 4. Etc.

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



NEW QUESTION 153

DRAG DROP - (Topic 4)

Your company deploys Azure Sentinel.

You plan to delegate the administration of Azure Sentinel to various groups. You need to delegate the following tasks:

? Create and run playbooks

? Create workbooks and analytic rules.

The solution must use the principle of least privilege.

Which role should you assign for each task? To answer, drag the appropriate roles to the correct tasks. 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.

Azure Sentinel Contributor	
Azure Sentinel Responder	Create and run playbooks: <input style="width: 150px; height: 20px;" type="text"/>
Azure Sentinel Reader	Create workbooks and analytic rules: <input style="width: 150px; height: 20px;" type="text"/>
Logic App Contributor	

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Azure Sentinel Contributor	
Azure Sentinel Responder	Create and run playbooks: Logic App Contributor
Azure Sentinel Reader	Create workbooks and analytic rules: Azure Sentinel Contributor
Logic App Contributor	

NEW QUESTION 156

- (Topic 4)

You need to ensure that you can run hunting queries to meet the Microsoft Sentinel requirements. Which type of workspace should you create?

- A. Azure Synapse AnarytKS
- B. AzureDalabricks
- C. Azure Machine Learning
- D. LogAnalytics

Answer: D

NEW QUESTION 159

DRAG DROP - (Topic 4)

You have the resources shown in the following table.

Name	Description
SW1	An Azure Sentinel workspace
CEF1	A Linux sever configured to forward Common Event Format (CEF) logs to SW1
Server1	A Linux server configured to send Common Event Format (CEF) logs to CEF1
Server2	A Linux server configured to send Syslog logs to CEF1

You need to prevent duplicate events from occurring in SW1.

What should you use for each action? To answer, drag the appropriate resources to the correct actions. Each resource 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.

Resources

Answer Area

SW1	From the Syslog configuration, remove the facilities that send CEF messages.	
CEF1		
Server1	From the Log Analytics agent, disable Syslog synchronization.	
Server2		

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Resources

Answer Area

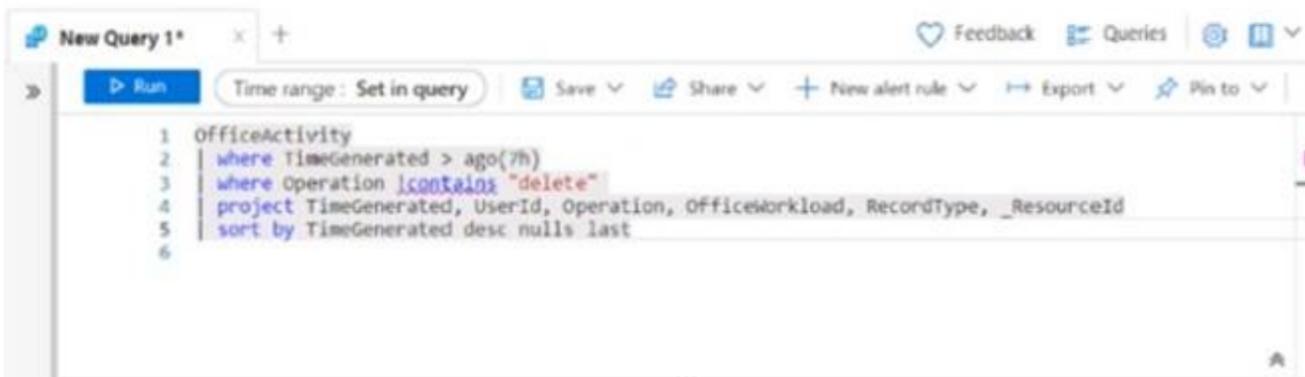
SW1	From the Syslog configuration, remove the facilities that send CEF messages.	Server1
CEF1		
Server1	From the Log Analytics agent, disable Syslog synchronization.	CEF1
Server2		

NEW QUESTION 163

- (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 167

- (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 170

- (Topic 4)

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

Answer: B

Explanation:

Reference:

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

NEW QUESTION 172

- (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 175

HOTSPOT - (Topic 4)

You have a Microsoft Sentinel workspace

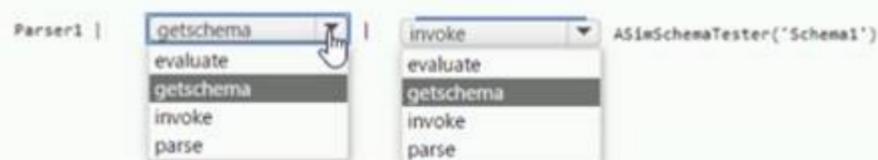
You develop a custom Advanced Security information Model (ASIM) parser named Parser1 that produces a schema named Schema1.

You need to validate Schema1.

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

NOTE: Each correct selection is worth one point.

Answer Area

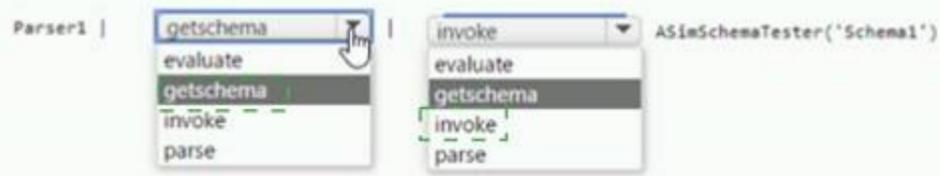


- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area



NEW QUESTION 179

- (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 183

- (Topic 4)

You have an Azure subscription that uses Microsoft Defender for Servers Plan 1 and contains a server named Server1.

You enable agentless scanning.

You need to prevent Server1 from being scanned. The solution must minimize administrative effort.

What should you do?

- A. Create an exclusion tag.
- B. Upgrade the subscription to Defender for Servers Plan 2.
- C. Create a governance rule.
- D. Create an exclusion group.

Answer: D

NEW QUESTION 187

HOTSPOT - (Topic 4)

You have the following KQL query.

```
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.

The watchlist cannot be updated after it is created.

The `IPList` variable is set as the IP address entity.

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Statements

The `Username` field is set as the account entity.

Yes

No

The watchlist cannot be updated after it is created.

The `IPList` variable is set as the IP address entity.

NEW QUESTION 189

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 191

- (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 193

- (Topic 4)

You have five on-premises Linux servers.

You have an Azure subscription that uses Microsoft Defender for Cloud. You need to use Defender for Cloud to protect the Linux servers.

What should you install on the servers first?

- A. the Dependency agent
- B. the Log Analytics agent
- C. the Azure Connected Machine agent
- D. the Guest Configuration extension

Answer: B

Explanation:

Defender for Cloud depends on the Log Analytics agent. Use the Log Analytics agent if you need to:

- * Collect logs and performance data from Azure virtual machines or hybrid machines hosted outside of Azure
- * Etc.

Reference:

<https://docs.microsoft.com/en-us/azure/defender-for-cloud/os-coverage> <https://docs.microsoft.com/en-us/azure/azure-monitor/agents/agents-overview#log-analytics-agent>

NEW QUESTION 197

DRAG DROP - (Topic 4)

Your network contains an on-premises Active Directory Domain Services (AD DS) domain that syncs with an Azure AD tenant.

You have a Microsoft Sentinel workspace named Sentinel1.

You need to enable User and Entity Behavior Analytics (UEBA) for Sentinel1 and collect security events from the AD DS domain.

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.

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

NEW QUESTION 198

- (Topic 4)

You have a Microsoft Sentinel workspace named Workspaces

You need to exclude a built-in, source-specific Advanced Security Information Model (ASIM) parser from a built-in unified ASIM parser.

What should you create in Workspace1?

- A. a workbook
- B. a hunting query
- C. a watchlist
- D. an analytic rule

Answer: D

Explanation:

To exclude a built-in, source-specific Advanced Security Information Model (ASIM) parser from a built-in unified ASIM parser, you should create an analytic rule in the Microsoft Sentinel workspace. An analytic rule allows you to customize the behavior of the unified ASIM parser and exclude specific source-specific parsers from being used.

Reference: <https://docs.microsoft.com/en-us/azure/sentinel/analytics-create-analytic-rule>

NEW QUESTION 201

- (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 204

DRAG DROP - (Topic 4)

You create a new Azure subscription and start collecting logs for Azure Monitor. You need to validate that Microsoft Defender for Cloud will trigger an alert when a malicious file is present on an Azure virtual machine running Windows Server. Which three actions should you perform in a sequence? To answer, move the appropriate actions from the list of action to the answer area and arrange them in the correct order. NOTE: More than one order of answer choices is correct. You will receive credit for any of the correct orders you select.

Actions		Answer Area
Enable Microsoft Defender for Cloud's enhanced security features for the subscription.		
Change the alert severity threshold for emails to Medium .		
Rename the executable file as AlertTest.exe.		
Change the alert severity threshold for emails to Low .		
Copy an executable file on a virtual machine and rename the file as ASC_AlertTest_662jfi039N.exe.		
Run the executable file and specify the appropriate arguments.		

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

To validate that Microsoft Defender for Cloud will trigger an alert when a malicious file is present on an Azure virtual machine running Windows Server, you should perform the following three actions in sequence:
 ? Copy an executable file on a virtual machine and rename the file as ASC_AlertTest_662jfi039N.exe
 ? Run the executable file and specify the appropriate arguments
 ? Enable Microsoft Defender for Cloud's enhanced security features for the subscription.
 These actions will simulate a malicious activity on the virtual machine and generate an alert in Defender for Cloud. You can then verify the alert details and response recommendations in the Azure portal. For more information, see Alert validation - Microsoft Defender for Cloud.

NEW QUESTION 208

- (Topic 4)

You have an Azure subscription that contains a virtual machine named VM1 and uses Azure Defender. Azure Defender has automatic provisioning enabled. You need to create a custom alert suppression rule that will suppress false positive alerts for suspicious use of PowerShell on VM1. What should you do first?

- A. From Azure Security Center, add a workflow automation.
- B. On VM1, run the Get-MPThreatCatalog cmdlet.
- C. On VM1 trigger a PowerShell alert.
- D. From Azure Security Center, export the alerts to a Log Analytics workspace.

Answer: C

Explanation:

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

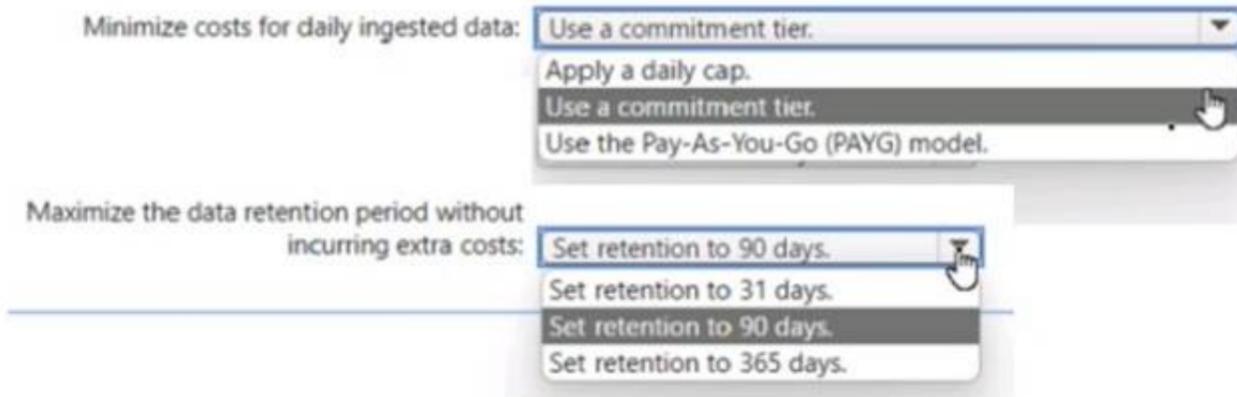
NEW QUESTION 209

HOTSPOT - (Topic 4)

You have an Azure subscription. You plan to implement an Microsoft Sentinel workspace. You anticipate that you will ingest 20 GB of security log data per day. You need to configure storage for the workspace. The solution must meet the following requirements:

- Minimize costs for daily ingested data.
- Maximize the data retention period without incurring extra costs.

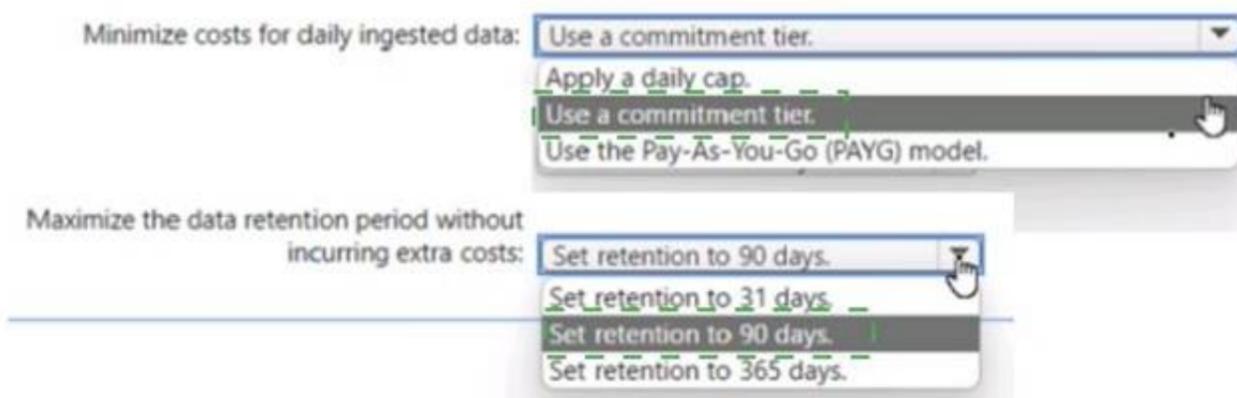
What should you do for each requirement? To answer, select the appropriate options in the answer area. NOTE Each correct selection is worth one point.



- A. Mastered
- B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 213

- (Topic 4)

You are configuring Azure Sentinel.

You need to send a Microsoft Teams message to a channel whenever an incident representing a sign-in risk event is activated in Azure Sentinel.

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

Answer: AB

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/sentinel/enable-entity-behavior-analytics> <https://docs.microsoft.com/en-us/azure/sentinel/automate-responses-with-playbooks>

NEW QUESTION 218

HOTSPOT - (Topic 4)

You have a Microsoft 365 E5 subscription that uses Microsoft Purview and contains a user named User1.

User1 shares a Microsoft Power BI report file from the Microsoft OneDrive folder of your company to an external user by using Microsoft Teams.

You need to identify which Power BI report file was shared.

How should you configure the search? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Activities:

- Copied file
- Downloaded files to computer
- Share file, folder, or site
- Shared Power BI report

Record type:

- MicrosoftTeams
- OneDrive
- PowerBiAudit
- Shared Power BI report

Workload:

- MicrosoftTeams
- OneDrive
- PowerBI
- SharePoint

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

To identify which Power BI report file was shared by User1, you should configure the search with the following parameters:

- ? Activities: Shared Power BI report
- ? Record Type: PowerBiAudit
- ? Workload: PowerBi

These parameters will filter the search results to show only the events where a Power BI report was shared by a user in your organization. You can then look for the event that has User1 as the user ID and an external user as the recipient. The event details will show the name and URL of the Power BI report file that was shared. For more information, see Search the audit log for events in Power BI and Search for content in the Microsoft Purview compliance portal.

NEW QUESTION 223

- (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 Regulatory compliance, you download the report.

Does this meet the goal?

- A. Yes
- B. No

Answer: B

Explanation:

Reference:

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

NEW QUESTION 225

- (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 229

- (Topic 4)

You have a Microsoft Sentinel playbook that is triggered by using the Azure Activity connector.

You need to create a new near-real-time (NRT) analytics rule that will use the playbook. What should you configure for the rule?

- A. the Incident automation settings
- B. entity mapping
- C. the query rule

D. the Alert automation settings

Answer: B

NEW QUESTION 230

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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

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

NEW QUESTION 234

- (Topic 4)

A company uses Azure Sentinel.

You need to create an automated threat response. What should you use?

- A. a data connector
- B. a playbook
- C. a workbook
- D. a Microsoft incident creation rule

Answer: B

Explanation:

Reference:

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

NEW QUESTION 239

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)
```

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

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"
```

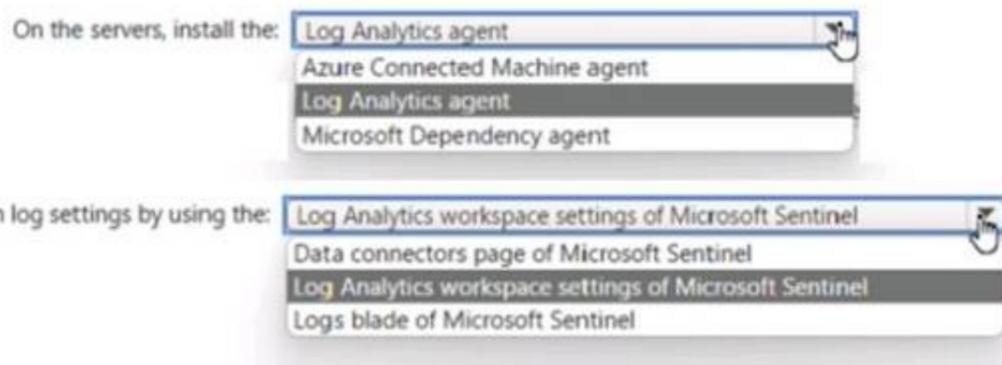
```
| join DeviceFileEvents on SHA256
| join kind=inner (DeviceFileEvents | where Timestamp > ago(1h)) on SHA256
| where Timestamp > ago(1h)
| where Timestamp < ago(1h)
```

NEW QUESTION 240

HOTSPOT - (Topic 4)

Your on-premises network contains 100 servers that run Windows Server. You have an Azure subscription that uses Microsoft Sentinel.

You need to upload custom logs from the on-premises servers to Microsoft Sentinel. What should you do? To answer, select the appropriate options in the answer area.



- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

To upload custom logs from the on-premises servers to Microsoft Sentinel, you should install the Log Analytics agent on each of the 100 servers. The Log Analytics agent is a lightweight agent that runs on the server and allows it to connect to the cloud-based Microsoft Defender Security Center. Once installed, the agent will allow the Microsoft Sentinel service to collect and analyze the custom log data from the servers.

NEW QUESTION 243

- (Topic 4)

You have an Azure subscription that uses Microsoft Sentinel.

You need to create a custom report that will visualise sign-in information over time.

What should you create first?

- A. a workbook
- B. a hunting query
- C. a notebook
- D. a playbook

Answer: A

Explanation:

A workbook is a data-driven interactive report in Microsoft Sentinel. You can use workbooks to create custom reports based on data from your Azure subscription.

Reference: <https://docs.microsoft.com/en-us/azure/sentinel/workbooks-overview>

NEW QUESTION 248

- (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 253

- (Topic 4)

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

You have a virtual machine named Server1 that runs Windows Server 2022 and is hosted in Amazon Web Services (AWS).

You need to collect logs and resolve vulnerabilities for Server1 by using Defender for Cloud.

What should you install first on Server1?

- A. the Microsoft Monitoring Agent
- B. the Azure Arc agent
- C. the Azure Monitor agent
- D. the Azure Pipelines agent

Answer: C

NEW QUESTION 254

- (Topic 4)

You have a Microsoft 365 E5 subscription that uses Microsoft 365 Defender.

You need to review new attack techniques discovered by Microsoft and identify vulnerable resources in the subscription. The solution must minimize administrative effort

Which blade should you use in the Microsoft 365 Defender portal?

- A. Advanced hunting
- B. Threat analytics
- C. Incidents & alerts
- D. Learning hub

Answer: B

Explanation:

To review new attack techniques discovered by Microsoft and identify vulnerable resources in the subscription, you should use the Threat Analytics blade in the Microsoft 365 Defender portal. The Threat Analytics blade provides insights into attack techniques, configuration vulnerabilities, and suspicious activities, and it can help you identify risks and prioritize threats in your environment. Reference: <https://docs.microsoft.com/en-us/microsoft-365/security/mtp/microsoft-365-defender-threat-analytics>

NEW QUESTION 255

- (Topic 4)

You are investigating a potential attack that deploys a new ransomware strain.

You plan to perform automated actions on a group of highly valuable machines that contain sensitive information.

You have three custom device groups.

You need to be able to temporarily group the machines to perform actions on the devices. Which three actions should you perform? Each correct answer presents part of the solution. NOTE: Each correct selection is worth one point.

- A. Add a tag to the device group.
- B. Add the device users to the admin role.
- C. Add a tag to the machines.

- D. Create a new device group that has a rank of 1.
- E. Create a new admin role.
- F. Create a new device group that has a rank of 4.

Answer: ACD

Explanation:

<https://docs.microsoft.com/en-us/learn/modules/deploy-microsoft-defender-for-endpoints-environment/4-manage-access>

NEW QUESTION 260

- (Topic 4)

You have a Microsoft 365 E5 subscription that uses Microsoft Defender for Endpoint

You need to identify any devices that triggered a malware alert and collect evidence related to the alert. The solution must ensure that you can use the results to initiate device isolation for the affected devices.

What should you use in the Microsoft 365 Defender portal?

- A. Incidents
- B. Investigations
- C. Advanced hunting
- D. Remediation

Answer: A

NEW QUESTION 263

- (Topic 4)

You have a third-party security information and event management (SIEM) solution.

You need to ensure that the SIEM solution can generate alerts for Azure Active Directory (Azure AD) sign-events in near real time.

What should you do to route events to the SIEM solution?

- A. Create an Azure Sentinel workspace that has a Security Events connector.
- B. Configure the Diagnostics settings in Azure AD to stream to an event hub.
- C. Create an Azure Sentinel workspace that has an Azure Active Directory connector.
- D. Configure the Diagnostics settings in Azure AD to archive to a storage account.

Answer: B

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/overview-monitoring>

NEW QUESTION 267

.....

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](#)