Microsoft.SC-200.v2026-06-19.q282

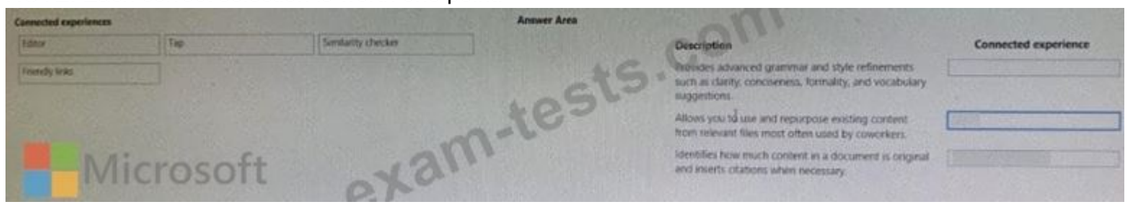
Exam Code:	SC-200
Exam Name:	Microsoft Security Operations Analyst
Certification Provider:	Microsoft
Free Question Number:	282
Version:	v2026-06-19
# of views:	141
# of Questions views:	2820
https://www.exam-tests.com/SC-200-exam/Microsoft.SC-200.v2026-06-19.q282.html	

NEW QUESTION: 1
You have an Azure subscription that contains a Microsoft Sentinel workspace named WS1.
You create a hunting query that detects a new attack vector. The attack vector maps to a tactic listed in the MITRE ATT&CK database.
You need to ensure that an incident is created in WS1 when the new attack vector is detected.
What should you configure?
A. a Fusion rule
B. a query bookmark
C. a scheduled query rule
D. a hunting livestream session
Answer: C (LEAVE A REPLY)
In Microsoft Sentinel, to automatically generate incidents when a specific pattern or behavior is detected by a query, you must create a scheduled analytics rule.
A scheduled query rule:
* Runs a KQL query on a defined schedule (e.g., every hour).
* Triggers an alert and incident when the query returns results.
* Can map detections to MITRE ATT&CK tactics and techniques, aligning with the requirement for attack vector mapping.
Other options explained:
* Fusion rule - Uses built-in machine learning for correlation, not custom KQL logic.
* Query bookmark - Saves hunting results but does not trigger incidents.
* Hunting livestream session - Used for live monitoring, not alert generation.
# Correct answer: C. a scheduled query rule

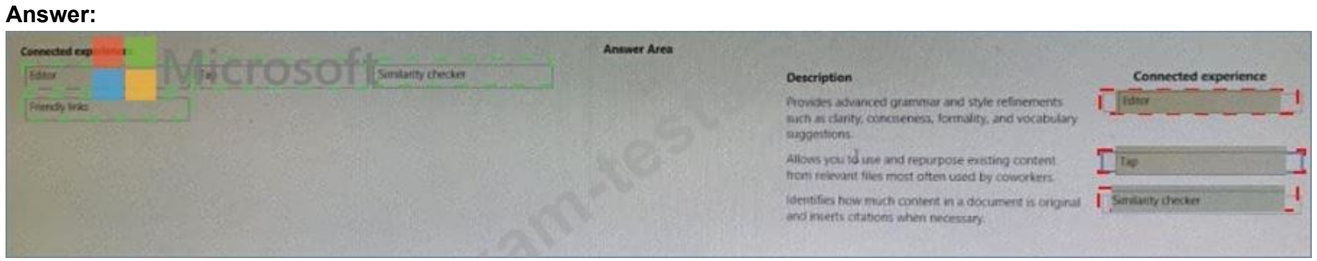
NEW QUESTION: 2
You have a Microsoft 365 E5 subscription that contains a device named Device1.
From the Microsoft Defender portal, you discover that an alert was triggered for Device1.
From the Device inventory page, you isolate Device1.
You need to collect a list of installed programs on Device1.
What should you do?

A. Run an advanced hunting query against the DeviceTvmSoftwareInventory table.
B. Initiate an automated investigation and view the results in the Action center.
C. Initiate a live response session and run the processes command.
D. Run an advanced hunting query against the DeviceProcessEvents table.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 3
A company wants to analyze by using Microsoft 365 Apps.
You need to describe the connected experiences the company can use.
Which connected experiences should you describe? To answer, drag the appropriate connected experiences to the correct description. Each connected experience may be used once, more than once, or not at all. You may need to drag the split between panes or scroll to view content.
NOTE: Each correct selection is worth one point.



Answer:



Explanation:

NEW QUESTION: 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 hav e 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 Mi crosoft Defender for Identity integration with Active Directory.
From the Microsoft Defender for identity portal, you need to configure several accounts for attackers to exploit.

Solution: You add each account as a Sensitive account.
Does this meet the goal?
A. Yes
B. No
Answer: A (LEAVE A REPLY)
In Microsoft Defender for Identity , marking accounts as Sensitive instructs the system to monitor those accounts more closely for suspicious activity or lateral movement attempts.
The question describes the goal as configuring several accounts that attackers might exploit. Microsoft Defender for Identity documentation explicitly says:
"Accounts designated as Sensitive are prioritized for monitoring and detection to identify potential compromise attempts." Thus, adding the accounts as Sensitive accounts achieves the goal.
Correct Answer: A. Yes

NEW QUESTION: 5
You need to configure Microsoft Cloud App Security to generate alerts and trigger remediation actions in response to external sharing of confidential files.
Which two actions should you perform in the Cloud App Security portal? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.
A. From Settings, select Information Protection, select Azure Information Protection, and then select Only scan files for Azure Information Protection classification labels and content inspection warnings from this tenant
B. Select Investigate files, and then filter App to Office 365.
C. Select Investigate files, and then select New policy from search
D. From Settings, select Information Protection, select Azure Information Protection, and then select Automatically scan new files for Azure Information Protection classification labels and content inspection warnings
E. From Settings, select Information Protection, select Files, and then enable file monitoring.
F. Select Investigate files, and then filter File Type to Document.
Answer: D,E (LEAVE A REPLY)
Reference:
https://docs.microsoft.com/en-us/cloud-app-security/tutorial-dlp
https://docs.microsoft.com/en-us/cloud-app-security/azip-integration

NEW QUESTION: 6
Hotspot Question
You have a Microsoft 365 E5 subscription that uses Microsoft Defender XDR.
You have a Microsoft Sentinel workspace.
Microsoft Sentinel connectors are configured as shown in the following table.

Connector	Collected log
Microsoft Entra ID	• Audit logs • Microsoft Graph activity logs
Microsoft 365	• Microsoft Exchange Online • Microsoft SharePoint Online • Microsoft Teams

You use Microsoft Sentinel to investigate suspicious Microsoft Graph API activity related to Conditional Access policies.
You need to search for the following activities:
- Downloads of the Conditional Access policies by using PowerShell
- Updates to the Conditional Access policies by using the Microsoft

Entra admin center

Which tables should you query for each activity? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

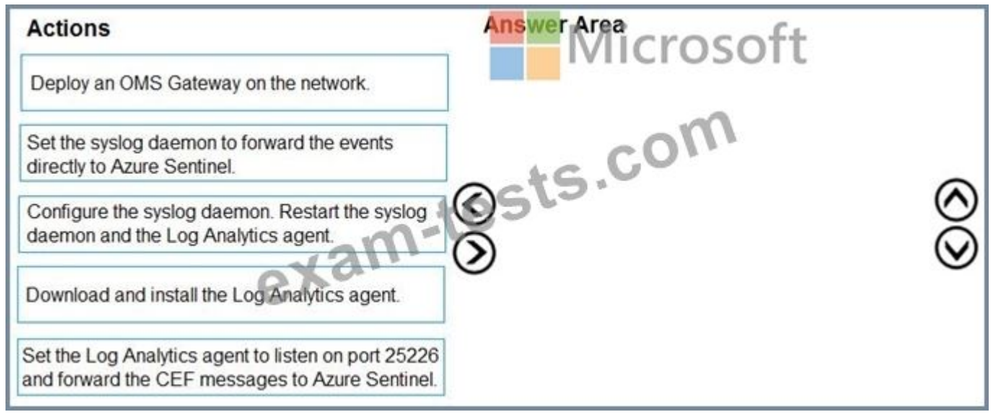
Answer:

NEW QUESTION: 7

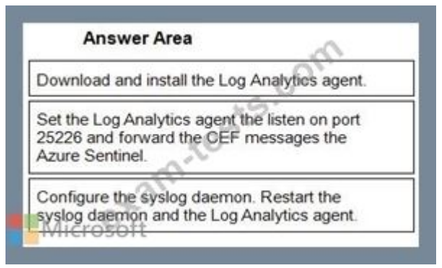
You plan to connect an external solution that will send Common Event Format (CEF) messages to Azure Sentinel.

You need to deploy the log forwarder.

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

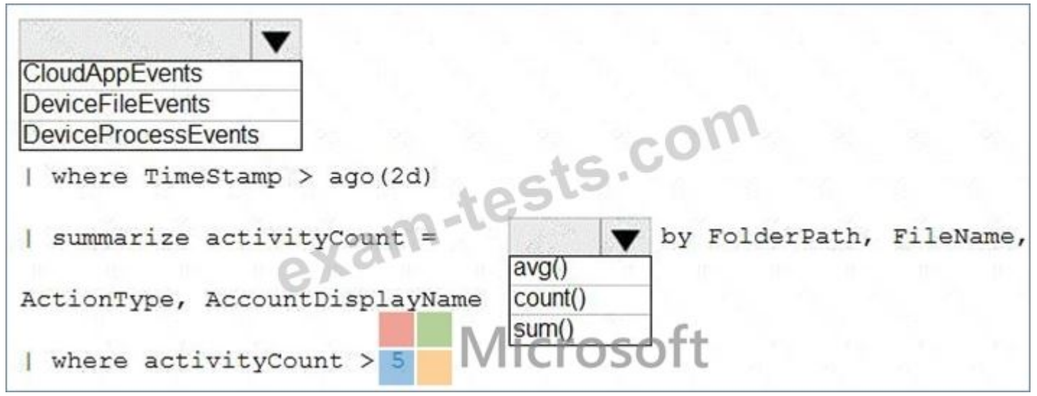


Answer:

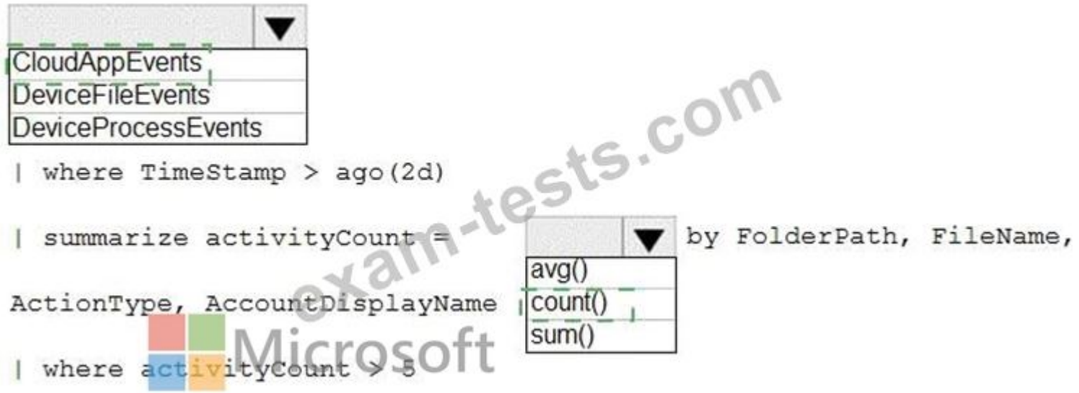


1 - Download and install the Log Analytics agent.
2 - Set the Log Analytics agent the listen on port 25226 and forward the CEF messages the Azure Sentinel.
3 - Configure the syslog daemon. Restart the syslog daemon and the Log Analytics agent.
Reference:
https://docs.microsoft.com/en-us/azure/sentinel/connect-cef-agent?tabs=rsyslog

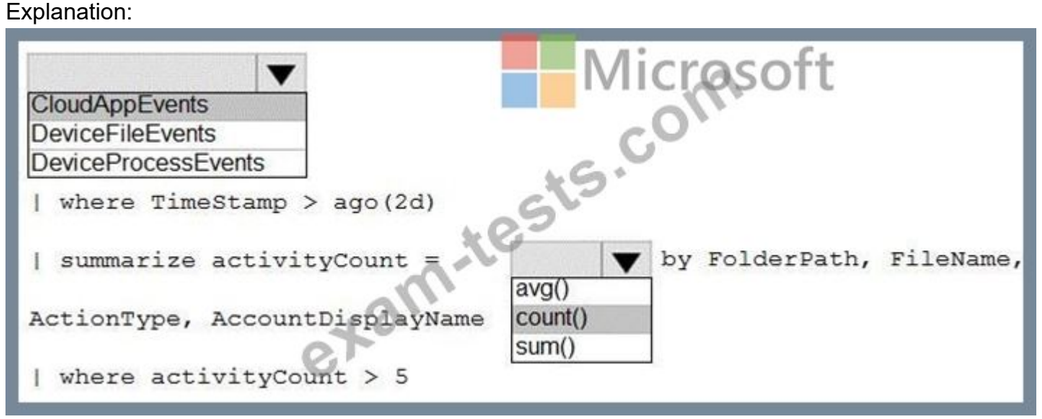
NEW QUESTION: 8
You need to create an advanced hunting query to investigate the executive team issue.
How should you complete the query? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



Answer:



Explanation:



NEW QUESTION: 9

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.

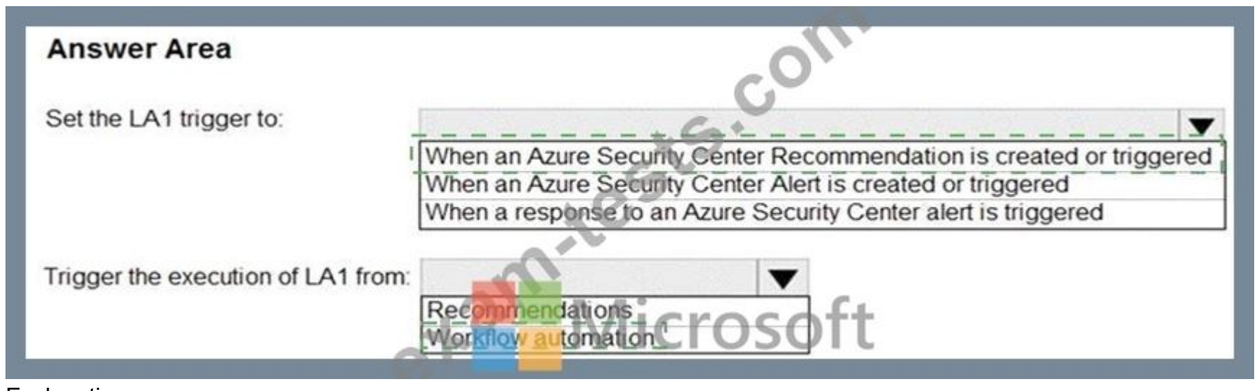
View the window

You need to test LA1 in Security Center.

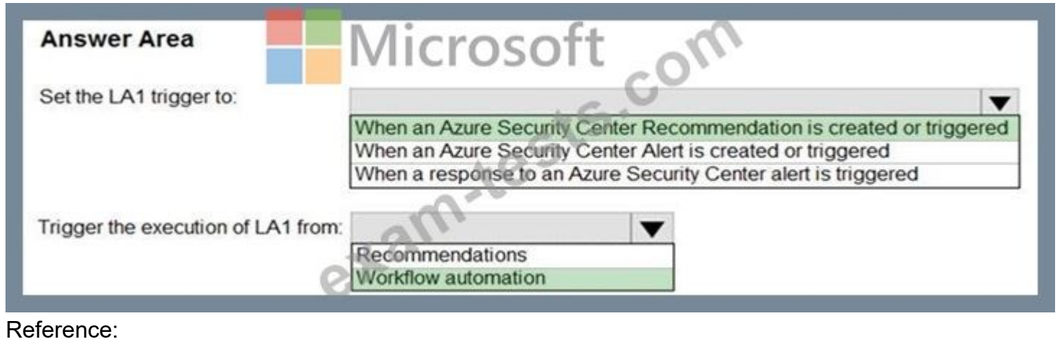
What should you do? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer:



Explanation

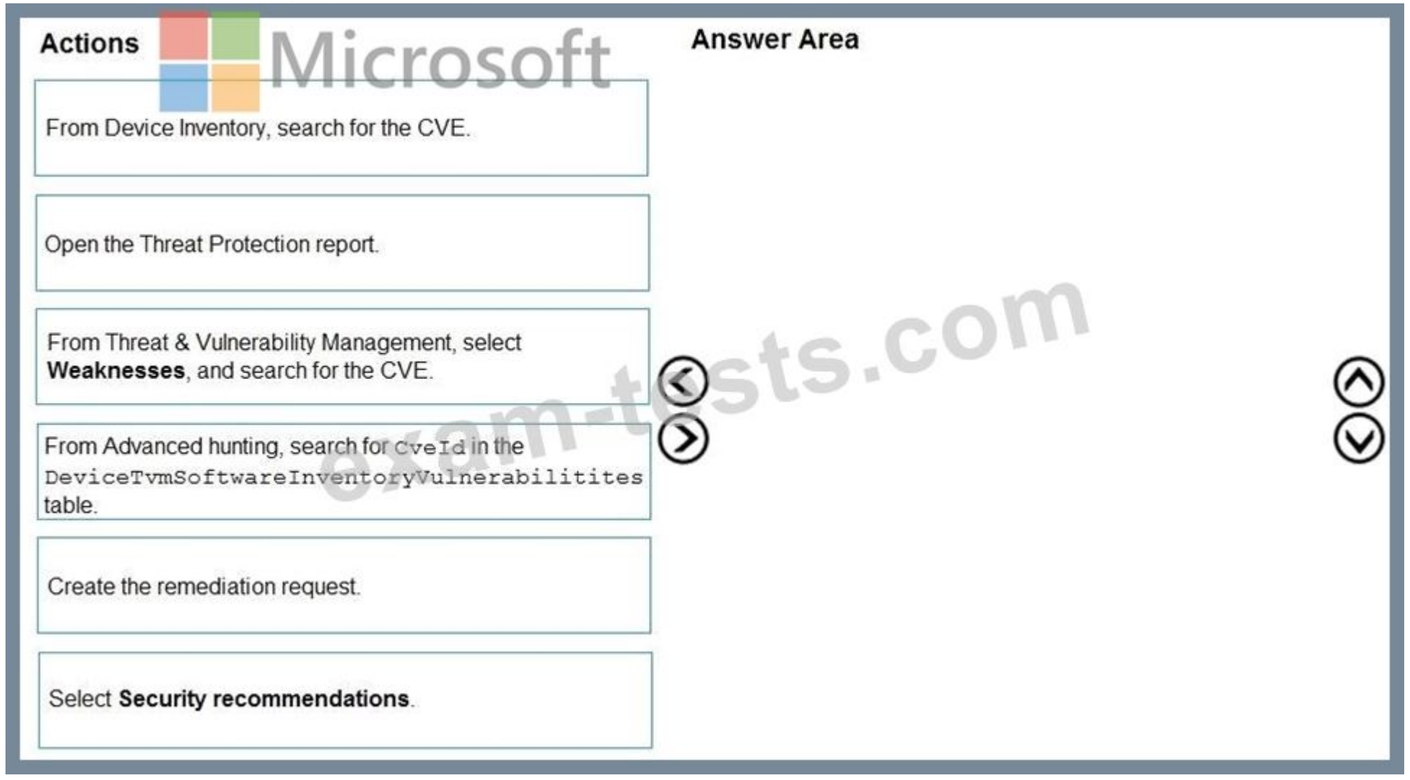


Reference:

https://docs.microsoft.com/en-us/azure/security-center/workflow-automation#create-a-logic-app-and-define-whe

NEW QUESTION: 10

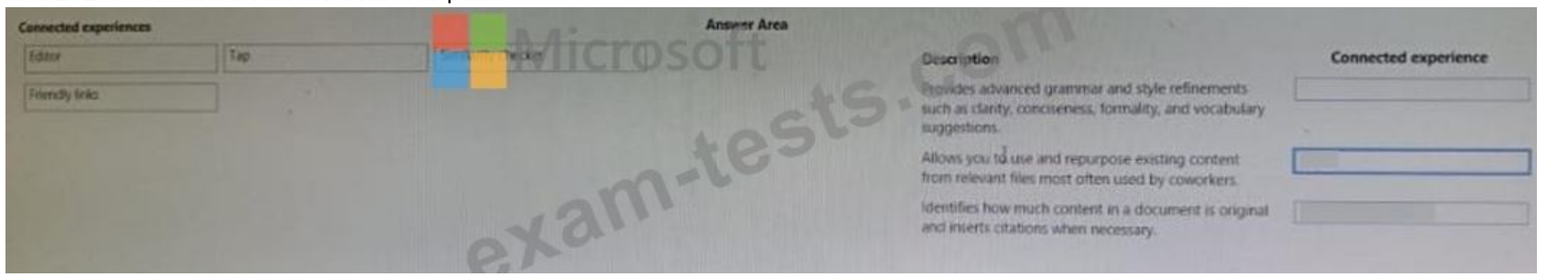
You are informed of a new common vulnerabilities and exposures (CVE) vulnerability that affects your environment.
You need to use Microsoft Defender Security Center to request remediation from the team responsible for the affected systems if there is a documented active exploit available.
Which three 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.



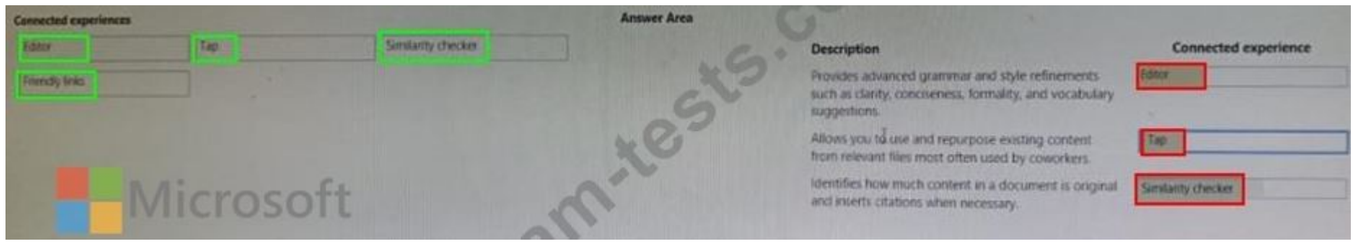
Answer:

1 - From Threat & Vulnerability Management, select Weaknesses, and search for the CVE.
2 - Select Security recommendations
3 - Create the remediation request.
Reference:
https://techcommunity.microsoft.com/t5/core-infrastructure-and-security/microsoft-defender-atp-remediate-apps-using-mem/ba-p/1599271

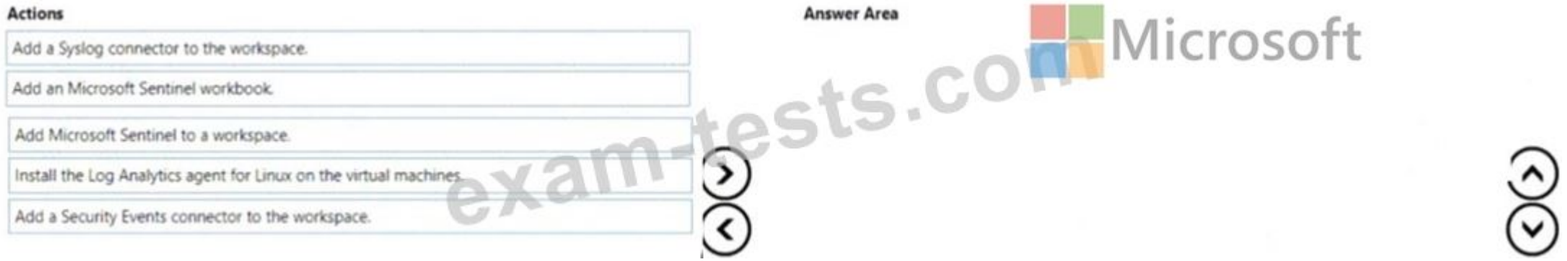
NEW QUESTION: 11
A company wants to analyze by using Microsoft 365 Apps.
You need to describe the connected experiences the company can use.
Which connected experiences should you describe? To answer, drag the appropriate connected experiences to the correct description. Each connected experience may be used once, more than once, or not at all. You may need to drag the split between panes or scroll to view content.
NOTE: Each correct selection is worth one point.



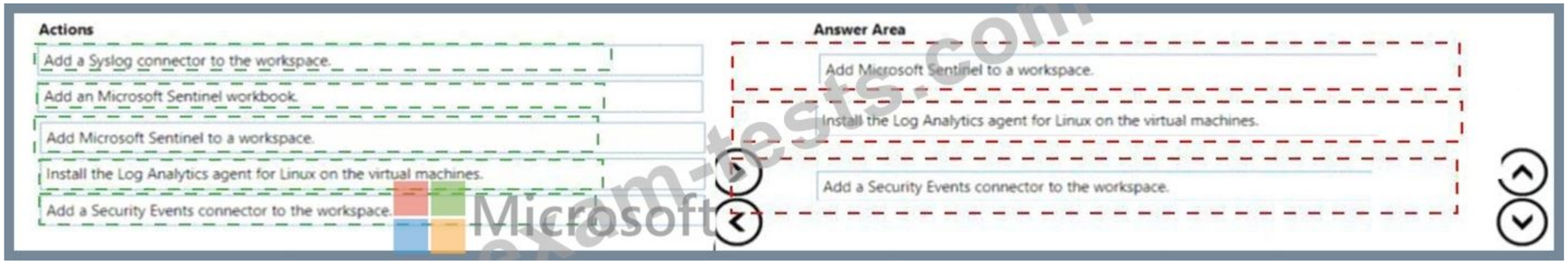
Answer:



NEW QUESTION: 12
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.



Answer:



Explanation:

NEW QUESTION: 13

Hotspot Question

You have a Microsoft 365 subscription.

You plan to use Microsoft Defender XDR to hunt for email-related threats.

You need to identify sign-ins performed by users within 30 minutes of the users receiving a known malicious email.

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

```
[alias | let | set]  MaliciousEmails=EmailEvents
| where ThreatTypes has "Malware"
| project TimeEmail = Timestamp, Subject, SenderFromAddress, AccountName = tostring(
    [parse | split | substring] (RecipientEmailAddress, "@")[0]); MaliciousEmails
| join ( IdentityLogonEvents
| project LogonTime = Timestamp, AccountName, DeviceName ) on AccountName
| where (LogonTime - TimeEmail) between (0min.. 30min)
```


Answer:

Answer Area

```
[let]  MaliciousEmails=EmailEvents
where ThreatTypes has "Malware"
project TimeEmail = Timestamp, Subject, SenderFromAddress, AccountName = tostring(
    [split] (RecipientEmailAddress, "@")[0]); MaliciousEmails
join ( IdentityLogonEvents
project LogonTime = Timestamp, AccountName , DeviceName ) on AccountName
where (LogonTime - TimeEmail) between (0min.. 30min)
```


NEW QUESTION: 14

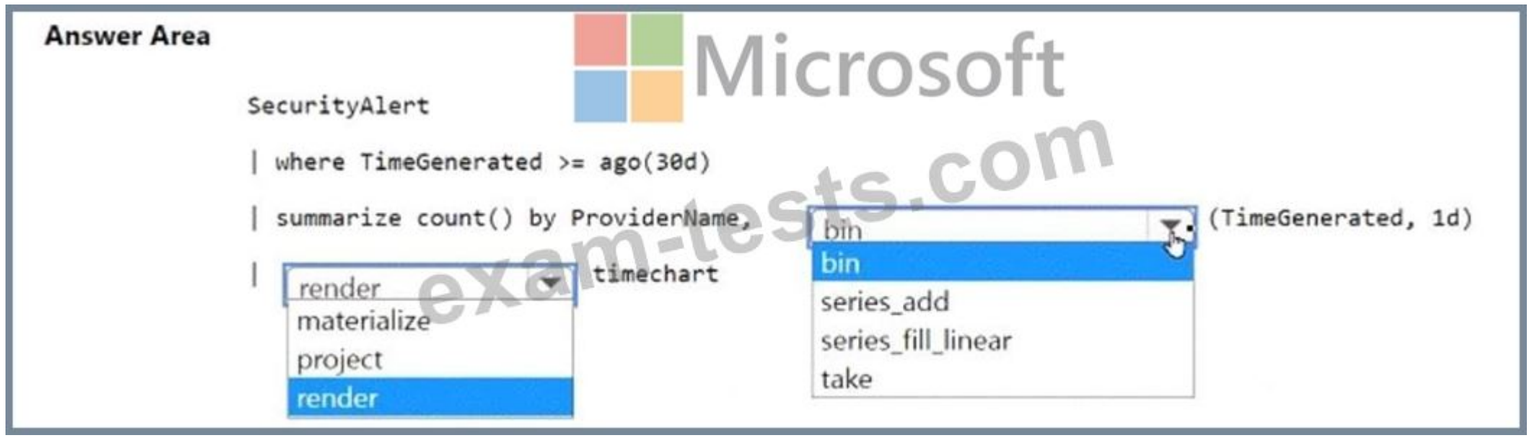
You have an Microsoft Sentinel workspace named SW1.

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

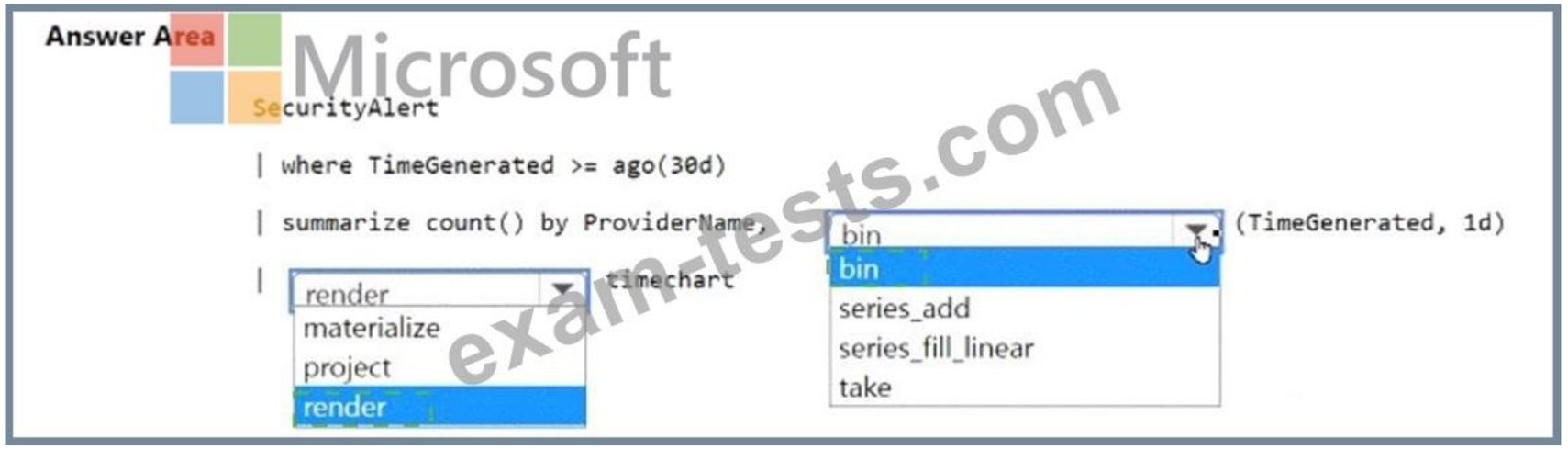
You need to create a query that will identify the number of security alerts per day for each provider.

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:

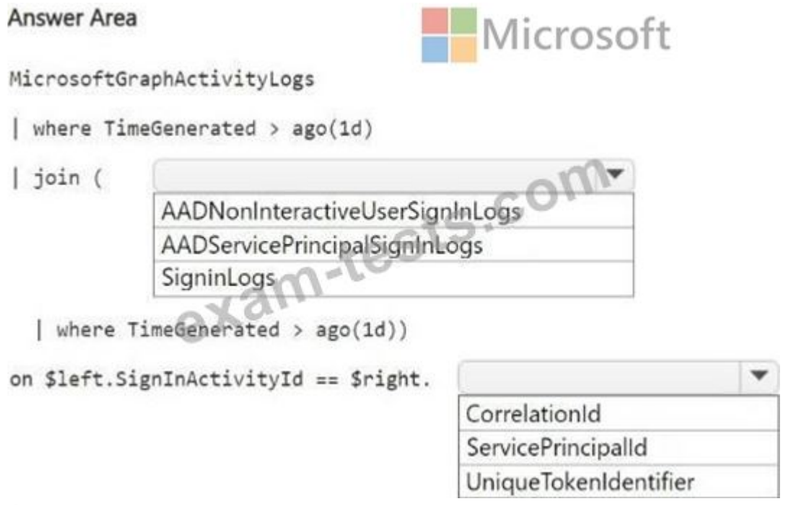


Explanation:

Answer Area

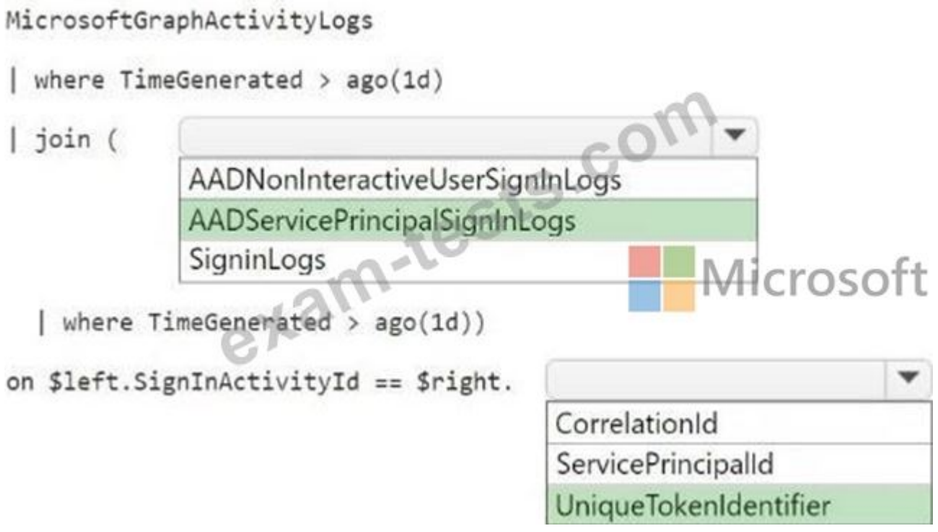
NEW QUESTION: 15
Hotspot Question
You have an Azure subscription name Sub1 that is linked to a Microsoft Entra tenant named contoso.com. Sub1 contains a Log Analytics workspace named Workspace1. All the logs from contoso.com are streamed to Workspace1.
You have a Microsoft 365 E5 subscription.
You need to query Workspace1 for the following:
- HTTP requests to the Microsoft Graph service of contoso.com
- Third-party app sign-in activities that use certificates or secrets
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



Answer:

Answer Area



NEW QUESTION: 16
You plan to review Microsoft Defender for Cloud alerts by using a third-party security information and event management (SIEM) solution.
You need to locate alerts that indicate the use of the Privilege Escalation MITRE ATT&CK tactic.
Which JSON key should you search?
A. Intent
B. Description
C. ExtendedProperies
D. Entities
Answer: (SHOW ANSWER)
Defender for Cloud alerts include a kill chain intent field that maps to MITRE ATT&CK tactics (for example, PrivilegeEscalation, Persistence, CredentialAccess). In the alert JSON this is exposed as intent; searching that key lets you filter for alerts where the tactic is Privilege Escalation.

NEW QUESTION: 17
Case Study 4 - Litware Inc
Overview
Adatum Corporation is a United States-based financial services company that has regional offices in New York, Chicago, and San Francisco.
Existing Environment

Identity Environment

The on-premises network contains an Active Directory Domain Services (AD DS) forest named corp.adatum.com that syncs with an Azure AD tenant named adatum.com. All user and group management tasks are performed in corp.adatum.com. The corp.adatum.com domain contains a group named Group1 that syncs with adatum.com.

Licensing Status

All the users at Adatum are assigned a Microsoft 365 ES license and an Azure Active Directory Premium P2 license.

Cloud Environment

The cloud environment contains a Microsoft 365 subscription, an Azure subscription linked to the adatum.com tenant, and the resources shown in the following table.

Name	Type	Description
Sentinel1	Microsoft Sentinel workspace	Includes a custom hunting query named HuntingQuery1
Server2	Azure virtual machine	Runs Windows Server 2022

On-premises Environment

The on-premises network contains the resources shown in the following table.

Name	Type	Description
Server1	Server	Runs Windows Server 2019 Has Azure Arc-enabled and the Azure Monitor agent installed
Webapp1	Web service	An on-premises, public-facing HTTP/HTTPS web service that generates JSON output in response to GET HTTP requests
Infoblox1	Infoblox DNS service	A third-party DNS service appliance linked to Sentinel1 by using a data connector

Requirements

Planned changes

Adatum plans to perform the following changes:

- Implement a query named rulequery1 that will include the following KQL query.

```
AzureActivity
| where ResourceProviderValue == "MICROSOFT.CLOUDSHELL"
| where ActivityStatusValue == "Start"
| extend
    Account_0_Name = tostring(split(Caller, '@', 0)[0]),
    Account_0_UPNSuffix = tostring(split(Caller, '@', 1)[0])
| project Account_0_Name, Account_0_UPNSuffix, CallerIpAddress, TimeGenerated
```

- Implement a Microsoft Sentinel scheduled rule that generates incidents based on rulequery1.

Microsoft Defender for Cloud Requirements

Adatum identifies the following Microsoft Defender for Cloud requirements:

- The members of Group1 must be able to enable Defender for Cloud plans and apply regulatory compliance initiatives.
- Microsoft Defender for Servers Plan 2 must be enabled on all the Azure virtual machines.
- Server2 must be excluded from agentless scanning.

Microsoft Sentinel Requirements

Adatum identifies the following Microsoft Sentinel requirements:

- Implement an Advanced Security Information Model (ASIM) query that will return a count of DNS requests that results in an NXDOMAIN response from Infoblox1.
- Ensure that multiple alerts generated by rulequery1 in response to a single user launching Azure Cloud Shell multiple times are consolidated as a single incident.
- Implement the Windows Security Events via AMA connector for Microsoft Sentinel and configure it to monitor the Security event log of Server1.
- Ensure that incidents generated by rulequery1 are closed automatically if Azure Cloud Shell is launched by the company's SecOps team.

- Implement a custom Microsoft Sentinel workbook named Workbook1 that will include a query to dynamically retrieve data from Webapp1.
- Implement a Microsoft Sentinel near-real-time (NRT) analytics rule that detects sign-ins to a designated break glass account.
- Ensure that HuntingQuery1 runs automatically when the Hunting page of Microsoft Sentinel in the Azure portal is accessed.
- Ensure that higher than normal volumes of password resets for corp.adatum.com user accounts are detected.
- Minimize the overhead associated with queries that use ASIM parsers.
- Ensure that the Group1 members can create and edit playbooks.
- Use built-in ASIM parsers whenever possible.

Business Requirements

Adatum identifies the following business requirements:

- Follow the principle of least privilege whenever possible.
- Minimize administrative effort whenever possible.

You need to implement the Defender for Cloud requirements.

Which subscription-level role should you assign to Group1?

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

Answer: (SHOW ANSWER)

Only Owner can enable defender for cloud plans and apply regulatory compliance initiatives at subscription level.

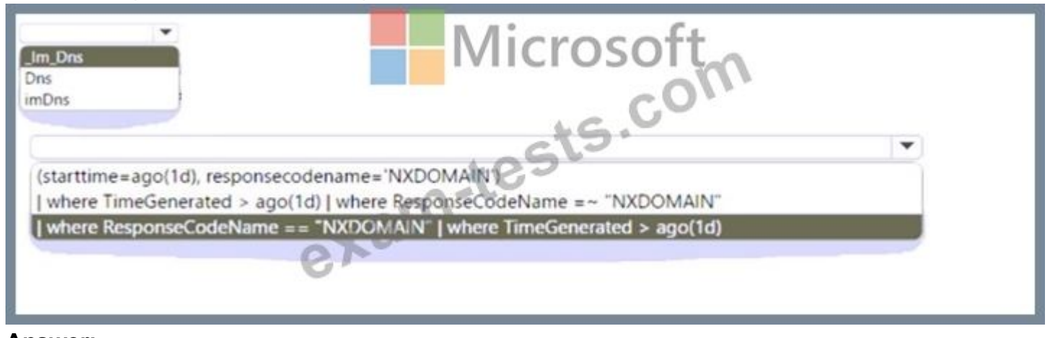
NEW QUESTION: 18

You have a Microsoft Sentinel workspace named Workspaces

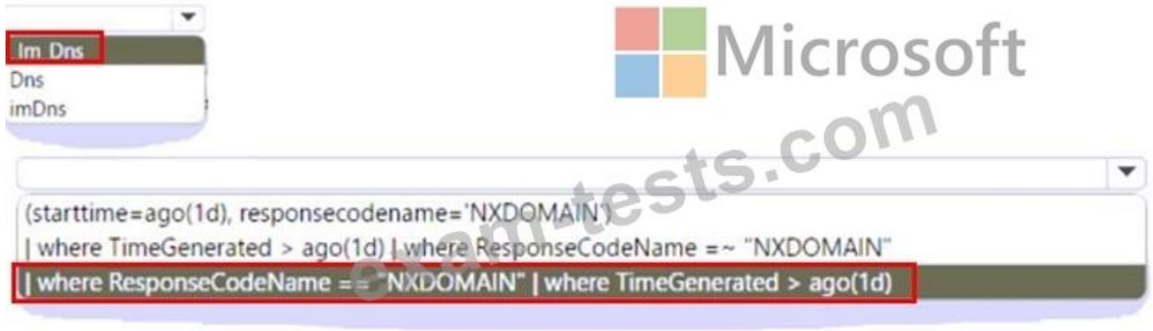
You configure Workspace1 to collect DNS events and deploy the Advanced Security information Model (ASIM) unifying parser for the DNS schema.

You need to query the ASIM DNS schema to list all the DNS events from the last 24 hours that have a response code of 'NXDOMAIN' and were aggregated by the source IP address in 15-minute intervals. The solution must maximize query performance.

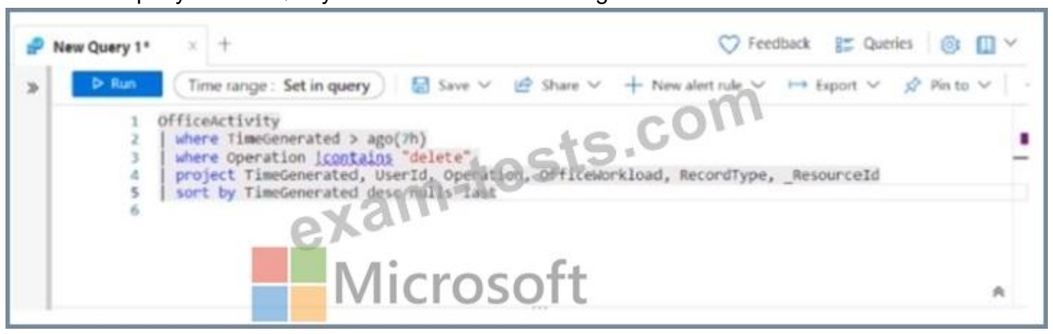
How should you complete the query? To answer, select the appropriate options in the answer area NOTE: Each correct selection is worth one point.



Answer:

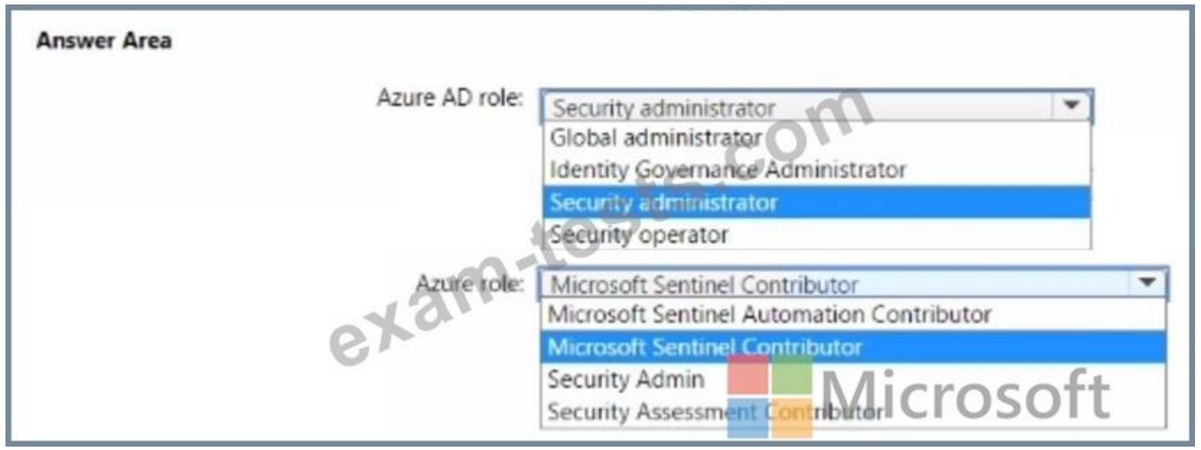


NEW QUESTION: 19
You have a Microsoft Sentinel workspace.
You have a query named Query1 as shown in the following exhibit.



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 (LEAVE A REPLY)
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: 20
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:

NEW QUESTION: 21

Hotspot Question

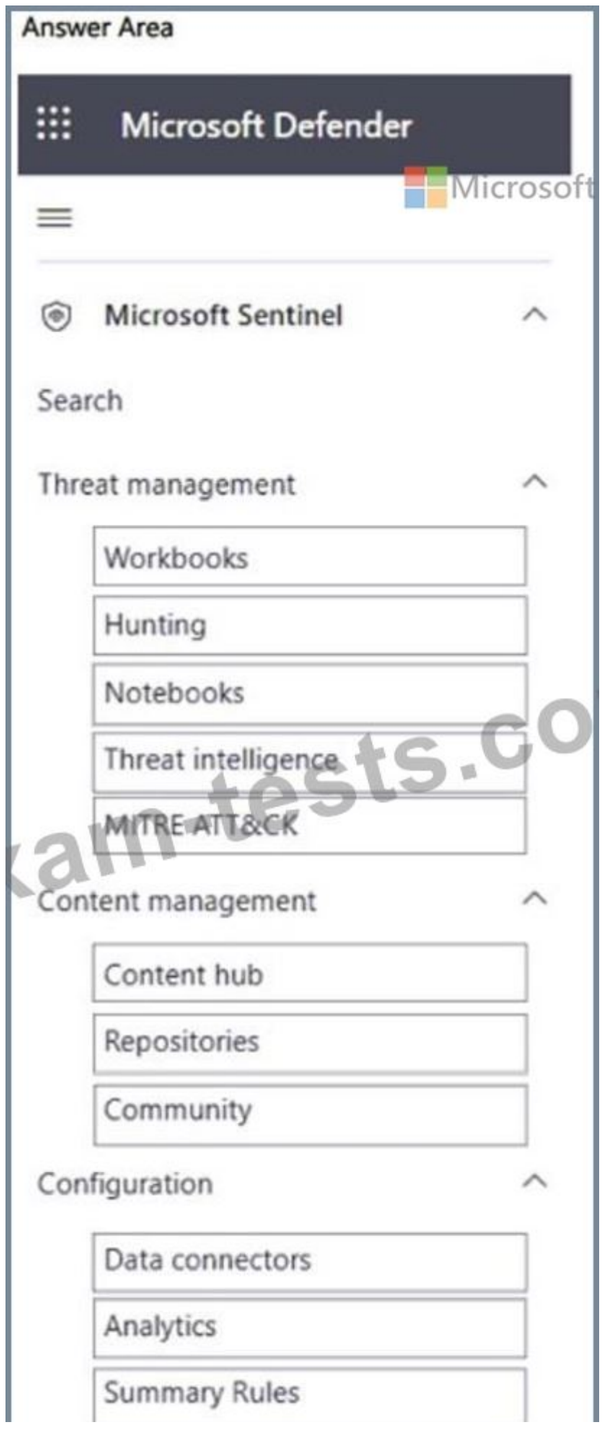
You have a Microsoft 365 E5 subscription.

You need to configure Microsoft Sentinel to collect logs from Microsoft Entra.

Which two nodes should you use in the Microsoft Defender portal? To answer, select the appropriate nodes in the answer area.

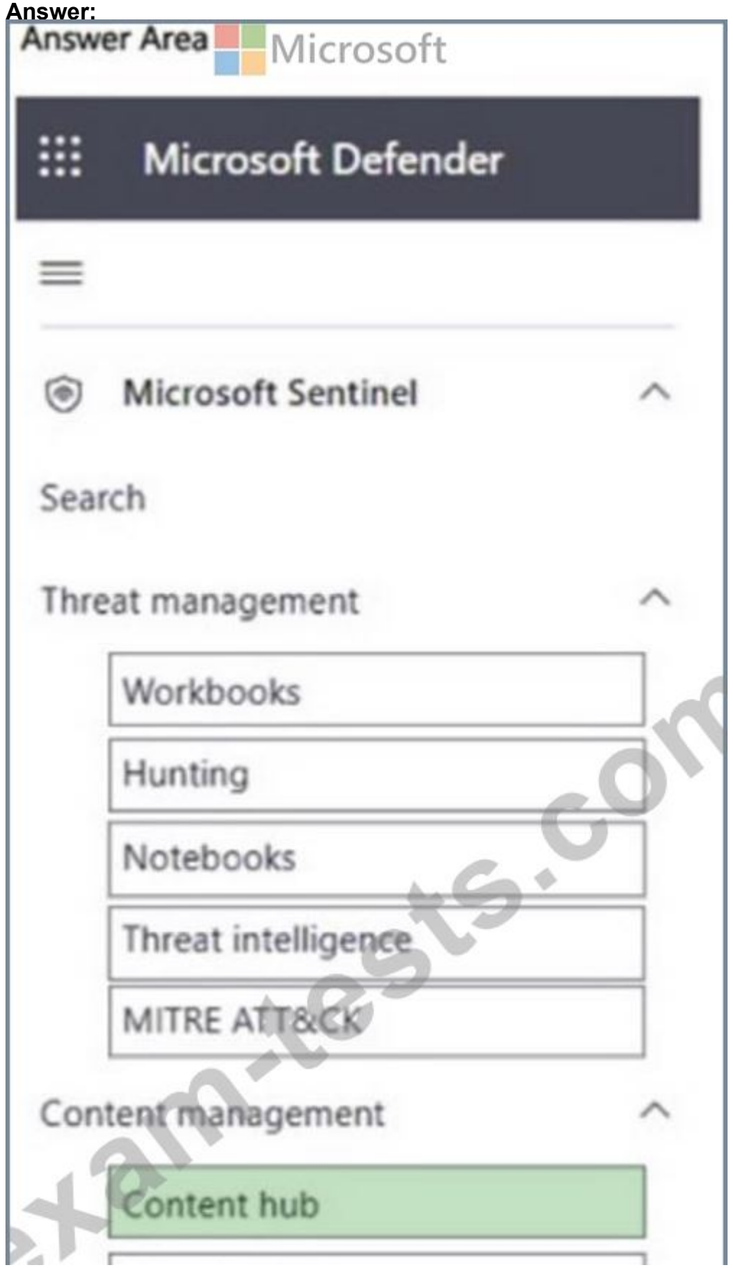
NOTE: Each correct answer is worth one point.

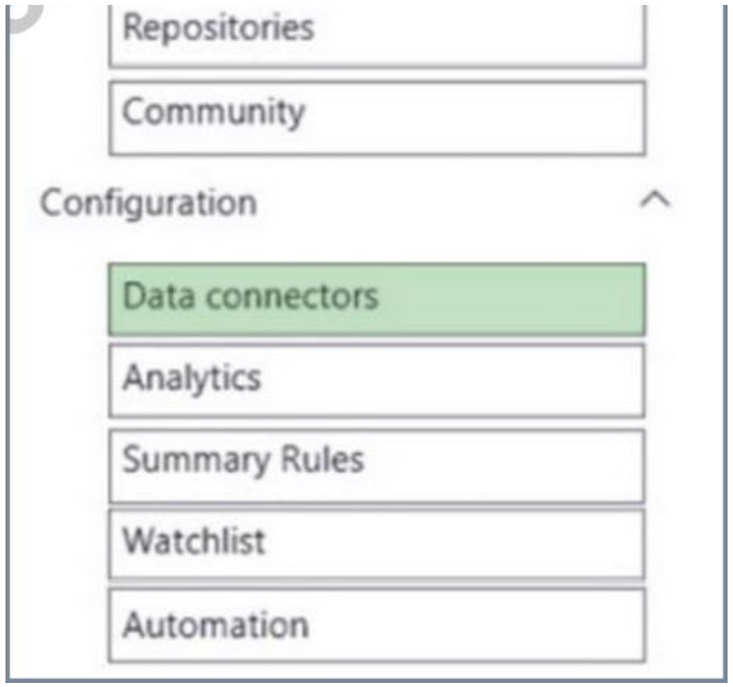
Answer Area




Watchlist
Automation

Answer:


Answer Area
Microsoft
Microsoft Defender
Microsoft Sentinel
Search
Threat management
Workbooks
Hunting
Notebooks
Threat intelligence
MITRE ATT&CK
Content management
Content hub



NEW QUESTION: 22

Hotspot Question

You have a custom detection rule that includes the following KQL query.

```
AlertInfo
| where Severity == "High"
| distinct AlertId
| join AlertEvidence on AlertId
| where EntityType in ("User", "Mailbox")
| where EvidenceRole == "Impacted"
| summarize by Timestamp, AlertId, AccountName, AccountObjectId,
EntityType, DeviceId, SHA256
| join EmailEvents on $left.AccountObjectId == $right.RecipientObjectId
| where DeliveryAction == "Delivered"
| summarize by Timestamp, AlertId, ReportId, RecipientObjectId,
RecipientEmailAddtess, EntityType, DeviceId, SHA256
```


For each of the following statements, select Yes if True. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Answer:

Explanation:

https://learn.microsoft.com/en-us/microsoft-365/security/defender/custom-detection-rules?view=o365-worldwide#4-specify-actions

Hotspot Question

NEW QUESTION: 23

You have a Microsoft Sentinel workspace named Workspace1 that contains a table named CommonSecurityLog.

You ingest logs into CommonSecurityLog. CommonSecurityLog has an average log ingestion time of five minutes.

You need to create an analytics rule that has a lookback period of seven minutes and uses the data in the CommonSecurityLog table. The solution must meet the following requirements:

- Prevent the same event from being processed twice.
- Minimize the number of missed events due to log ingestion delays.

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

NOTE: Each correct selection is worth one point.

Answer Area

```
let ingestion_delay= 5min;
let rule_look_back = 7min;
CommonSecurityLog
| where TimeGenerated >= ago [ ▼ ]
| where ingestion_time() > ago [ ▼ ]
```

- (ingestion_delay)
- (rule_look_back)
- (ingestion_delay + rule_look_back)

- (ingestion_delay)
- (rule_look_back)
- (ingestion_delay + rule_look_back)

Answer:

Answer Area

```
let ingestion_delay= 5min;
let rule_look_back = 1min;
CommonSecurityLog
| where TimeGenerated >= ago
```

- (ingestion_delay)
- (rule_look_back)
- (ingestion_delay + rule_look_back)

```
| where ingestion_time() > ago
```

- (ingestion_delay)
- (rule_look_back)
- (ingestion_delay + rule_look_back)

NEW QUESTION: 24
You have a Microsoft 365 subscription that uses Microsoft Defender XDR.
You are investigating an incident.
You need to review the incident tasks that were performed. The solution must include a query that will display the incidents in a workbook, and then display the tasks of each incident in another grid.
Which table should you target in the query?
A. SecurityIncident
B. SecurityEvent
C. SentinelAudit
D. SecurityAlert
Answer: (SHOW ANSWER)
The SecurityIncident table in Microsoft Sentinel contains information about incidents, including details such as incident ID, severity, status, and tasks.

NEW QUESTION: 25
You have a Microsoft 365 E5 subscription that uses Microsoft Defender XDR.
You have a Microsoft Sentinel workspace.
Microsoft Sentinel connectors are configured as shown in the following table.

Connector	Collected log
Microsoft Entra ID	• Audit logs • Microsoft Graph activity logs
Microsoft 365	• Microsoft Exchange Online • Microsoft SharePoint Online • Microsoft Teams

You use Microsoft Sentinel to investigate suspicious Microsoft Graph API activity related to Conditional Access policies. You need to search for the following activities:

* Downloads of the Conditional Access policies by using PowerShell

* Updates to the Conditional Access policies by using the Microsoft Entra admin center Which tables should you query for each activity? lo answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer:

Explanation:

NEW QUESTION: 26

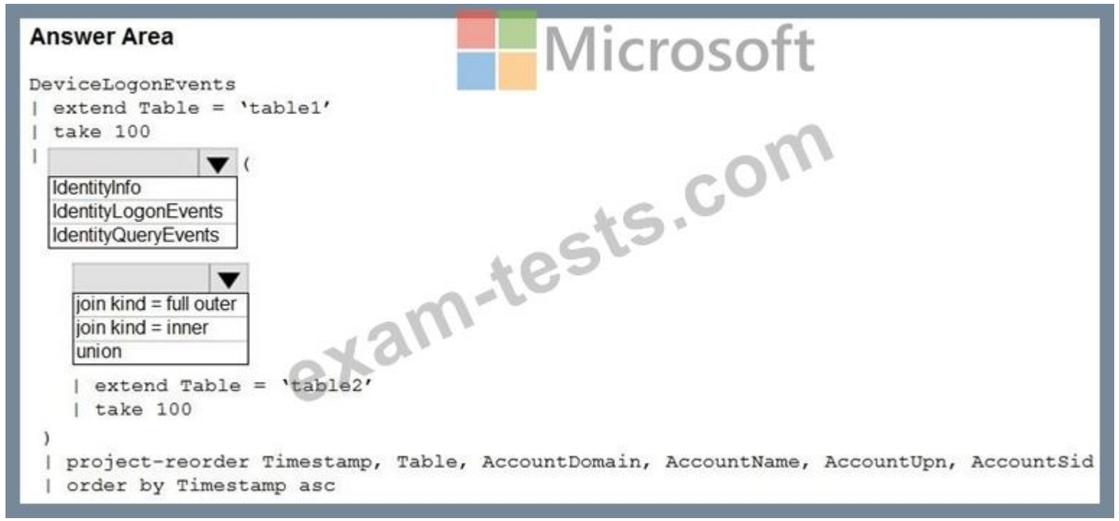
Hotspot Question

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

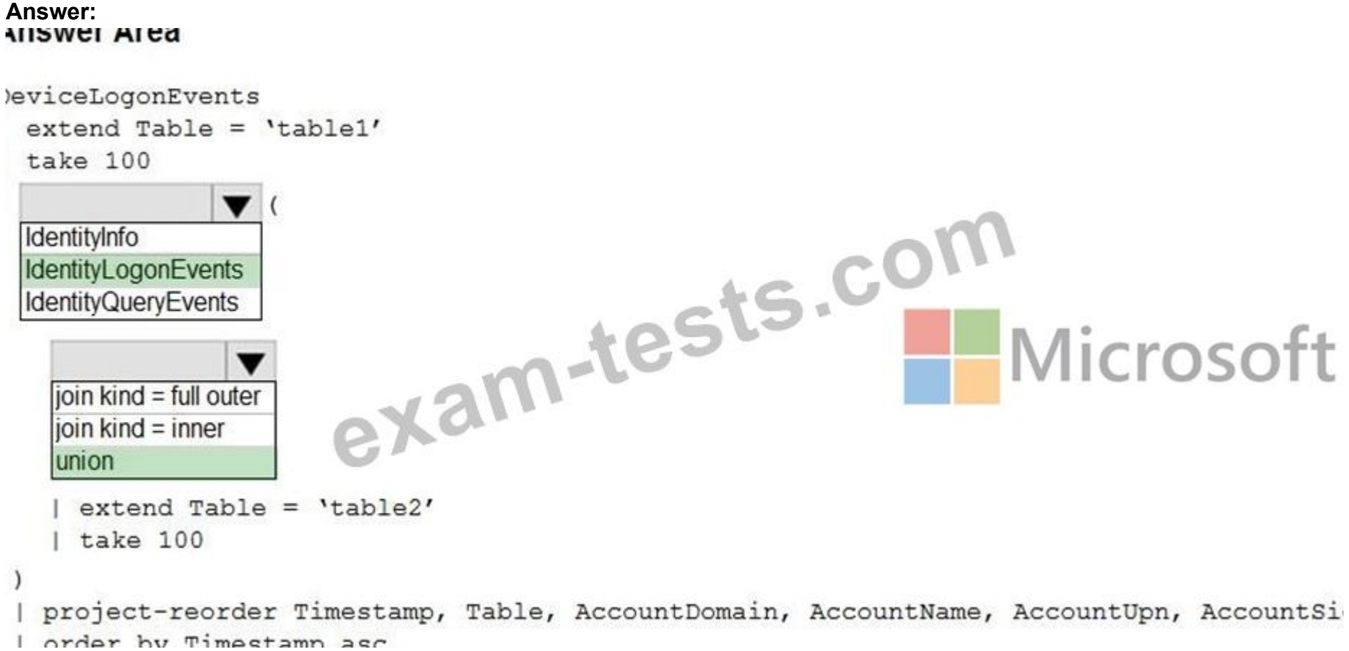
Your network contains an on-premises Active Directory Domain Services (AD DS) domain that syncs with Azure AD.

You need to identify the 100 most recent sign-in attempts recorded on devices and AD DS domain controllers.

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:



Explanation:

Box 1: IdentityLogonEvents

The final column requires "AccountUpn." Therefore, "IdentityInfo" would not be appropriate. Since it's about sign-in attempts to ADDS domain controllers, "IdentityLogonEvents" would be the suitable choice.

Box 2: union

We need to extract the latest 100 sign-in attempts from BOTH "Devices" AND "ADDS domain controllers." Using "union" would be optimal.

NEW QUESTION: 27

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

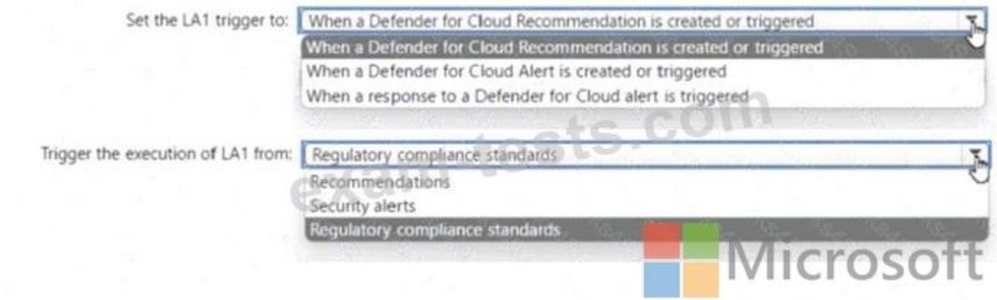
You create an Azure logic app named LA1.

You plan to use LA1 to automatically remediate security risks detected in Defenders for Cloud .

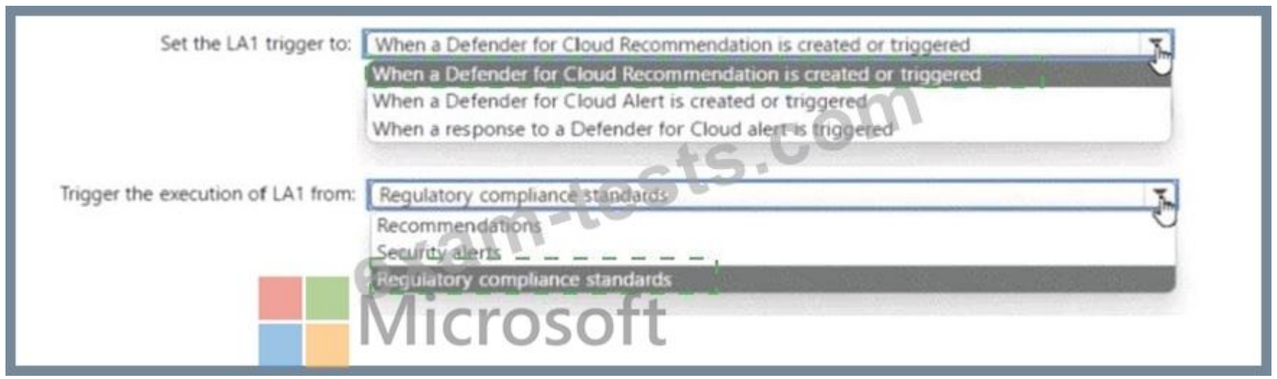
You need to test LA1 in Defender for Cloud .

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

NOTE: Each correct selection is worth one point.



Answer:



Explanation:

According to Microsoft Defender for Cloud automation documentation, Logic Apps can be integrated to automatically respond to recommendations or alerts. To test or automate remediation from Defender for Cloud , you must configure an automation workflow (Logic App) that triggers when a recommendation is created or updated.

Microsoft defines the available triggers for Defender for Cloud automation as follows:

* When a Defender for Cloud Recommendation is created or triggered - This event type initiates the Logic App whenever a new security recommendation appears or an existing one changes state. It's the proper trigger for remediation scenarios because recommendations typically indicate a detected security misconfiguration or risk requiring action.
* When a Defender for Cloud Alert is created or triggered - This applies to security alerts, not recommendations.
* When a response to a Defender for Cloud alert is triggered - Used for incident-response workflows, not for testing remediation logic.

In the context of the question, the goal is to test automatic remediation for detected configuration issues (security risks). Those are surfaced as recommendations within Defender for Cloud, not as alerts.
Next, the execution source should be configured under:
* Trigger the execution of LA1 from: Recommendations
This ensures that Defender for Cloud will execute the Logic App (LA1) automatically when relevant recommendations are triggered, allowing immediate testing and validation of the remediation logic.
In summary:
To test the Logic App remediation workflow in Defender for Cloud, you must:
* Set the trigger type to "When a Defender for Cloud Recommendation is created or triggered" .
* Configure it to execute from "Recommendations" .
Thus, the verified correct answers are:
Set the LA1 trigger to: When a Defender for Cloud Recommendation is created or triggered
Trigger the execution of LA1 from: Recommendations

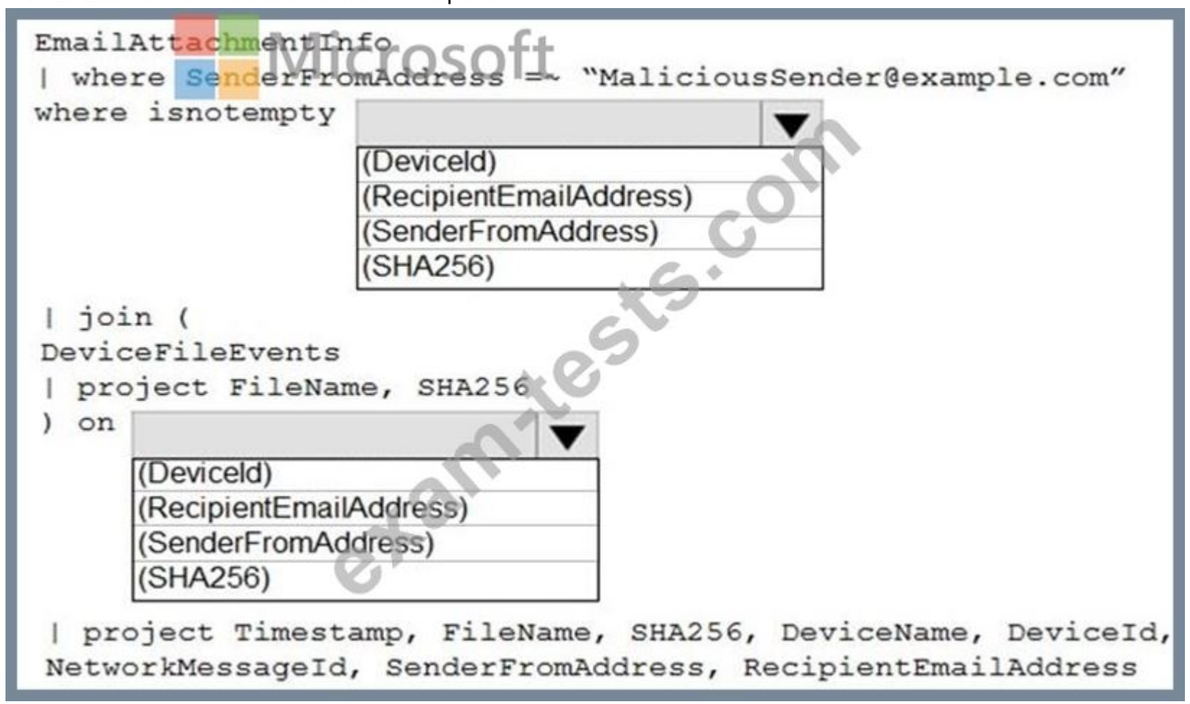
NEW QUESTION: 28
You are responsible for responding to Azure Defender for Key Vault alerts.
During an investigation of an alert, you discover unauthorized attempts to access a key vault from a Tor exit node.
What should you configure to mitigate the threat?
A. Key Vault firewalls and virtual networks
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 (LEAVE A REPLY)
Reference:
https://docs.microsoft.com/en-us/azure/key-vault/general/network-security

NEW QUESTION: 29
You have 500 on-premises Windows 11 devices that use Microsoft Defender for Endpoint You enable Network device discovery.
You need to create a hunting query that will identify discovered network devices and return the identity of the onboarded device that discovered each network device.
Which built-in function should you use?
A. next ()
B. SeenBy ()
C. current_cluster,endpoint()
D. DeviceFromIP ()
Answer: B (LEAVE A REPLY)

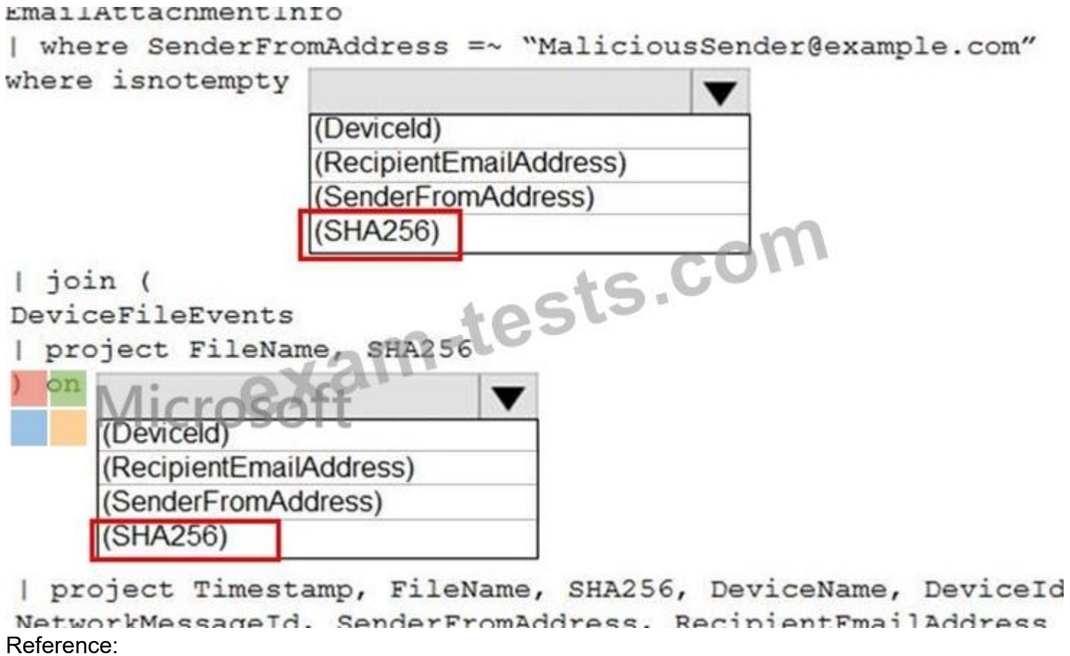
NEW QUESTION: 30
You have a Microsoft Sentinel workspace that contains the following incident.
Brute force attack against Azure Portal analytics rule has been triggered.
You need to identify the geolocation information that corresponds to the incident.
What should you do?
A. From Overview, review the 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 (LEAVE A REPLY)
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: 31
You have a Microsoft 365 E5 subscription that uses Microsoft Defender and an Azure subscription that uses Azure Sentinel.
You need to identify all the devices that contain files in emails sent by a known malicious email sender. The query will be based on the match of the SHA256 hash.
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:



Reference:
https://docs.microsoft.com/en-us/microsoft-365/security/defender/advanced-hunting-query-emails-devices?view=o365-worldwide

NEW QUESTION: 32
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. Enable User and Entity Behavior Analytics (UEBA)
B. Create a scheduled query rule.
C. Create a Data Collection Rule (DCR).
D. Modify the properties of the connector.
Answer: (SHOW ANSWER)

NEW QUESTION: 33
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 (LEAVE A REPLY)
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

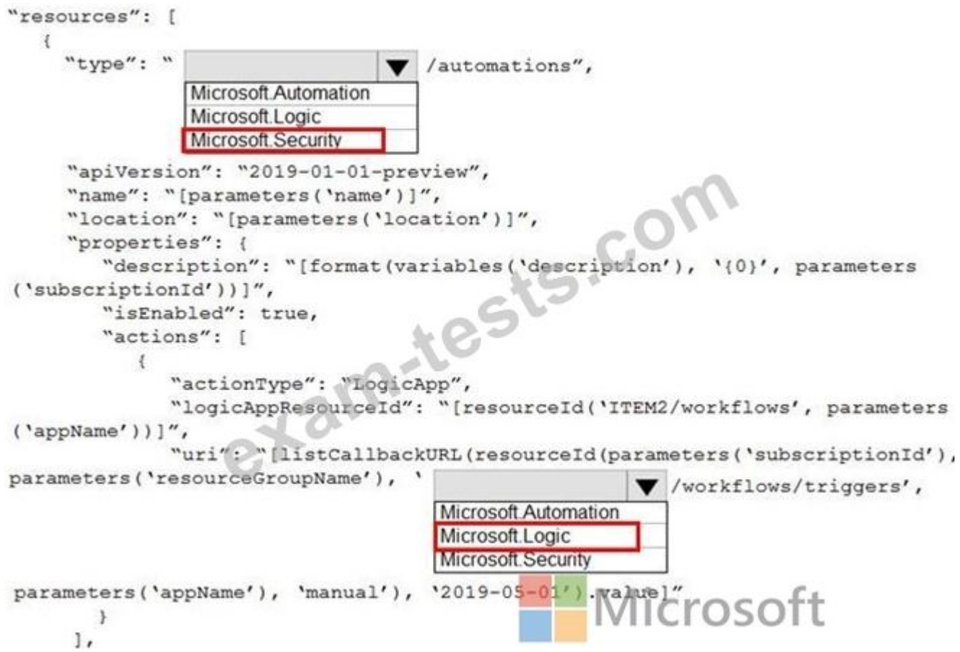
NEW QUESTION: 34
You need to use an Azure Resource Manager template to create a workflow automation that will trigger an automatic remediation when specific security alerts are received by Azure Security Center.
How should you complete the portion of the template that will provision the required Azure resources? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

```
"resources": [
  {
    "type": "                                    /automations",
    "apiVersion": "2019-01-01-preview",
    "name": "[parameters('name')]",
    "location": "[parameters('location')]",
    "properties": {
      "description": "[format(variables('description'), '{0}', parameters
['subscriptionId'))]",
      "isEnabled": true,
      "actions": [
        {
          "actionType": "LogicApp",
          "logicAppResourceId": "[resourceId('ITEM2/workflows', parameters
['appName'))]",
          "uri": "[listCallbackURL(resourceId(parameters('subscriptionId')
parameters('resourceGroupName'), '                    /workflows/triggers',
parameters('appName'), 'manual'), '2019-05-01').value]"
        }
```

Microsoft.Automation
Microsoft.Logic
Microsoft.Security

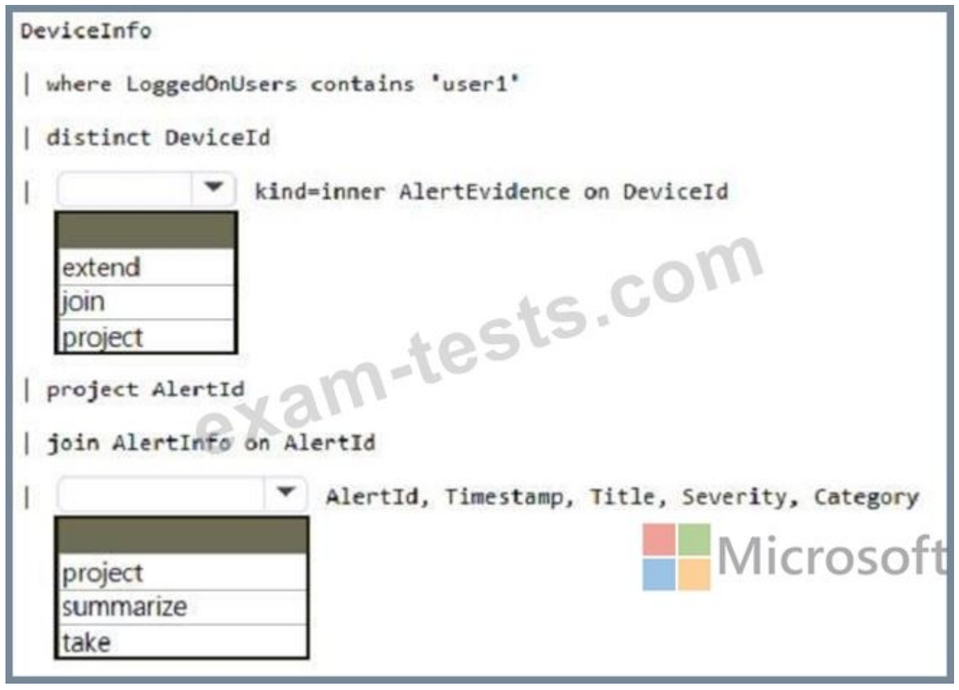
Microsoft.Automation
Microsoft.Logic
Microsoft.Security

Answer:

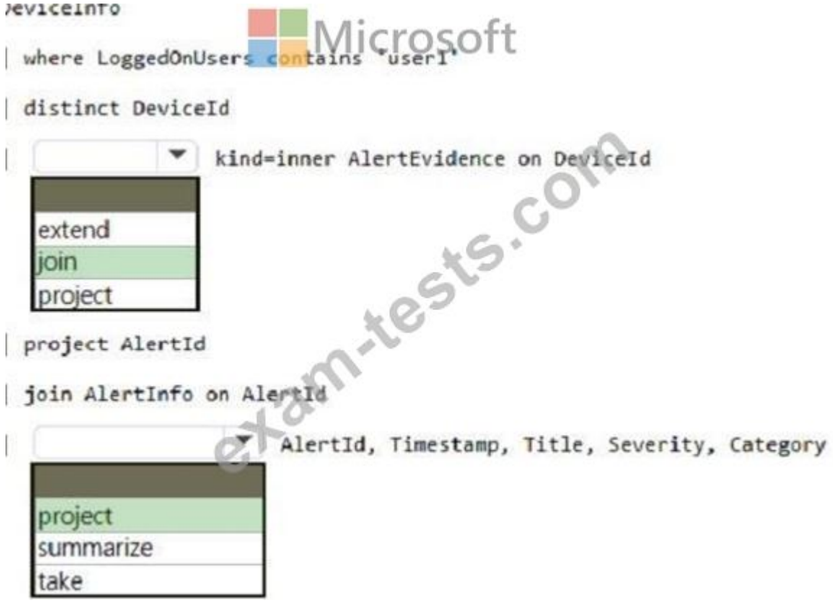


Reference:
https://docs.microsoft.com/en-us/azure/security-center/quickstart-automation-alert

NEW QUESTION: 35
Hotspot Question
You have a Microsoft 365 subscription that uses Microsoft 365 Defender and contains a user named User1.
You are notified that the account of User1 is compromised.
You need to review the alerts triggered on the devices to which User1 signed in.
How should you complete the query? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.



Answer:



Explanation:

Filtering the DeviceInfo table to only include rows where the LoggedOnUsers field contains the string "user1".

Removing duplicates based on the DeviceId field.

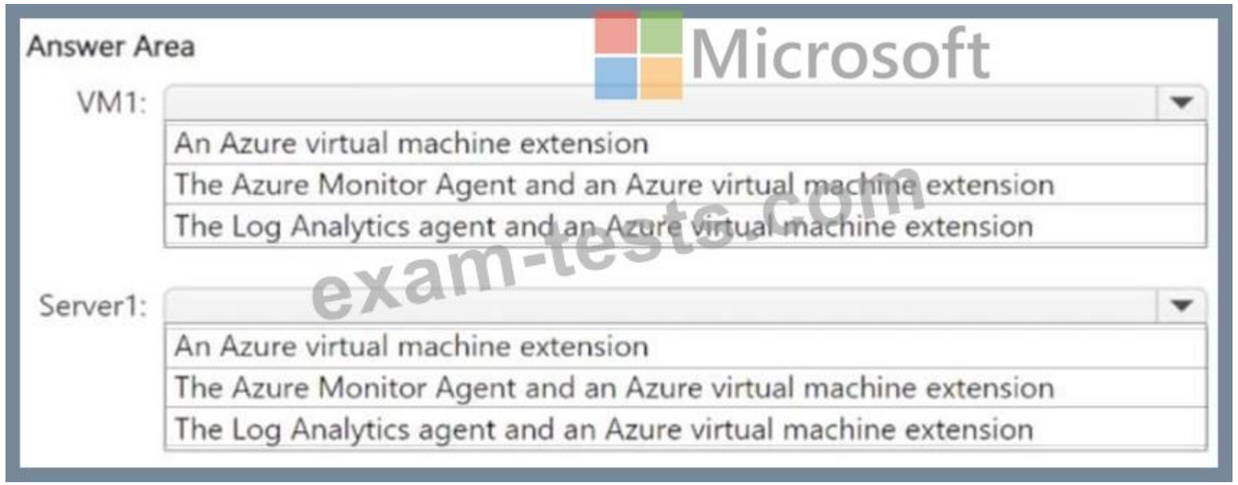
Joining the resulting set of devices with the AlertEvidence table based on the DeviceId field.
Projecting the AlertId field from the resulting set.
Joining the resulting set of alerts with the AlertInfo table based on the AlertId field.
Projecting the AlertId, Timestamp, Title, Severity, and Category fields from the resulting set of alerts.
This query retrieves a list of alerts that are related to devices where the user "user1" is logged on, and it includes the alert ID, timestamp, title, severity, and category for each alert. The "join" and "project" operations in the query are used to combine and filter the data from the various tables in the ATP data model.
Reference:
https://docs.microsoft.com/en-us/microsoft-365/security/defender/advanced-hunting-query-emails-devices?view=o365-worldwide

NEW QUESTION: 36
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: A,B (LEAVE A REPLY)
Explanation/Reference:
https://docs.microsoft.com/en-us/azure/sentinel/tutorial-respond-threats-playbook

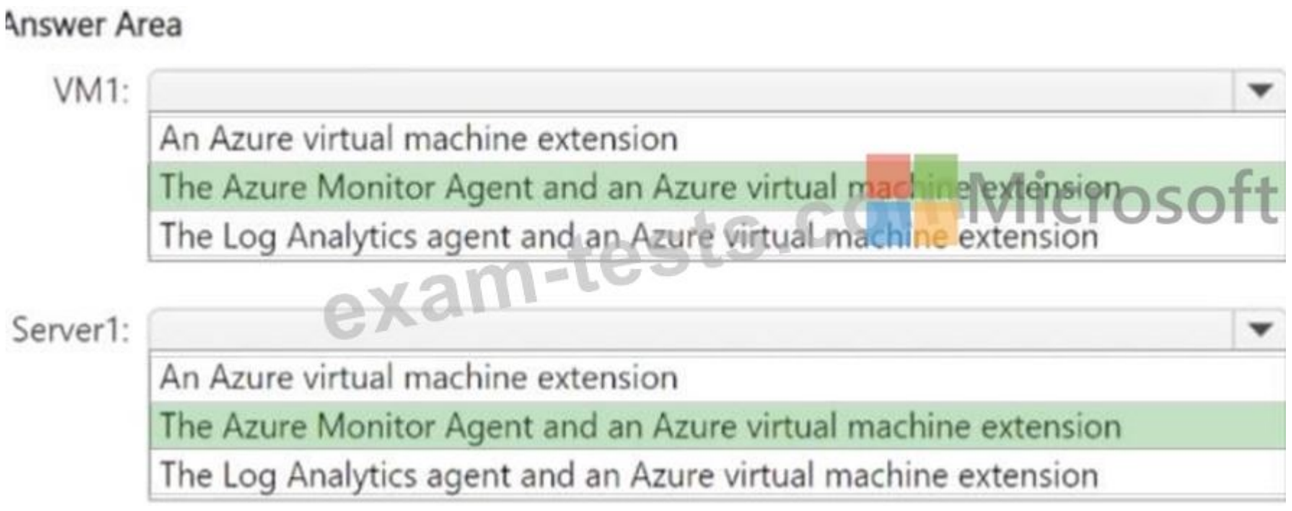
NEW QUESTION: 37
Hotspot Question
You have the resources shown in the following table.

Name	Type	Description
Server1	On-premises server	On-boarded to Azure Arc Runs Windows Server 2022 Has Microsoft SQL Server 2022 installed
VM1	SQL Server on Azure Virtual Machines	Runs Windows Server 2022 Has Microsoft SQL Server 2022 installed

You have an Azure subscription that uses Microsoft Defender for Cloud.
You need to use Defender for Cloud to protect VM1 and Server1. The solution must meet the following requirements:
- Support Advanced Threat Protection and vulnerability assessment.
- Register each SQL Server 2022 instance as a SQL virtual machine.
- Minimize implementation and administrative effort.
What should you deploy to each server? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



Answer:

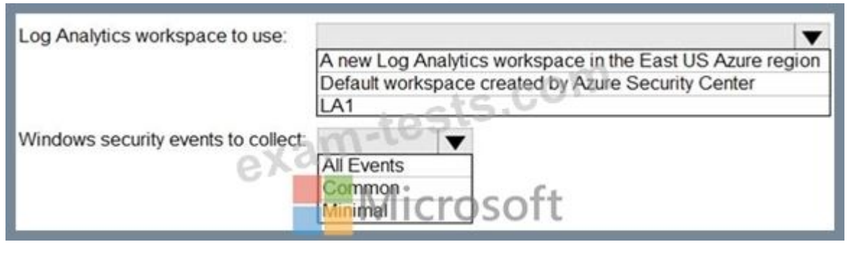


NEW QUESTION: 38

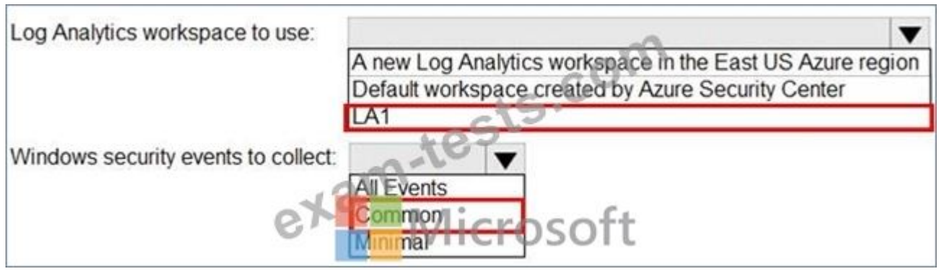
You need to implement Azure Defender to meet the Azure Defender requirements and the business requirements.

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.

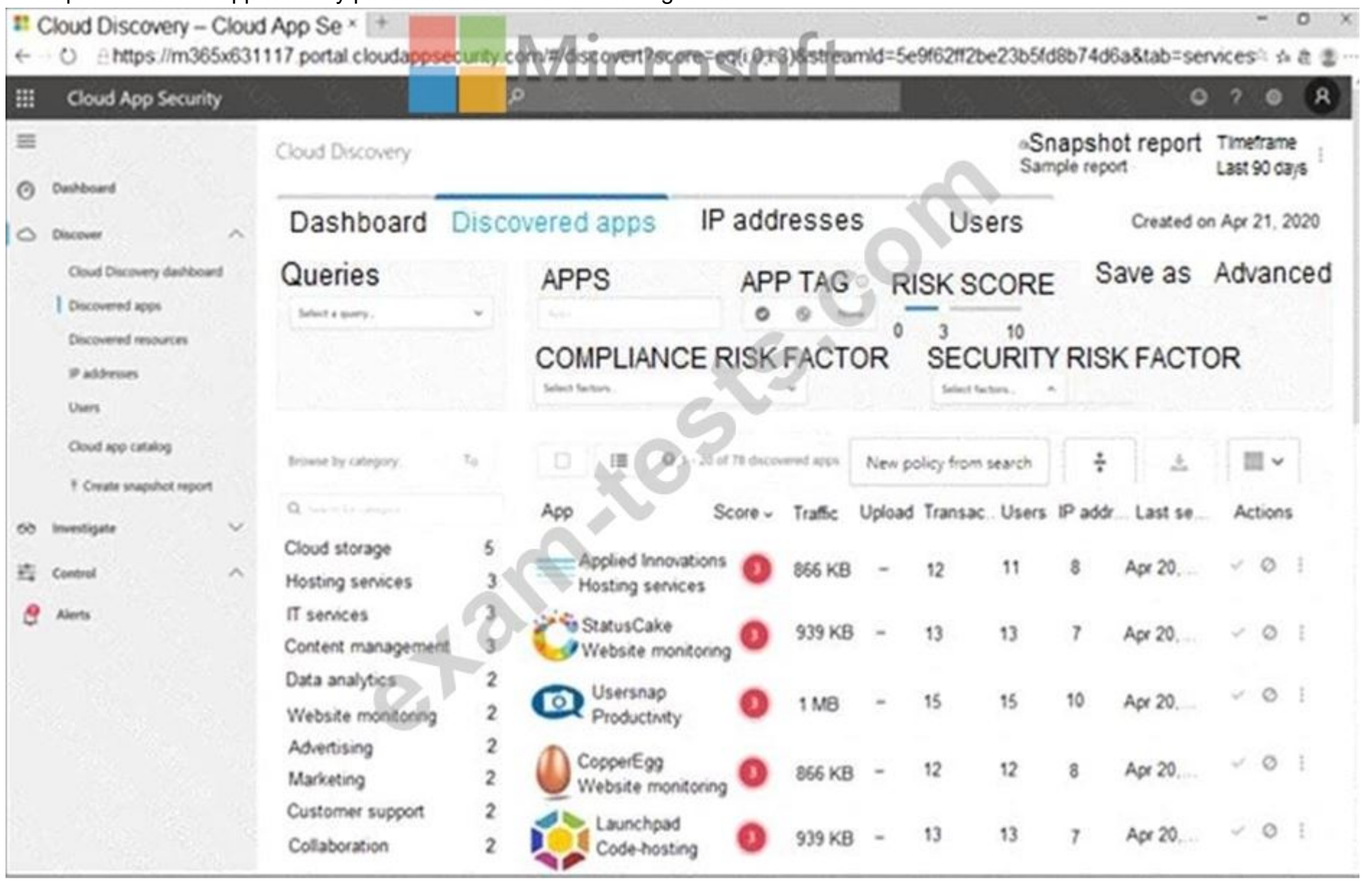


Answer:



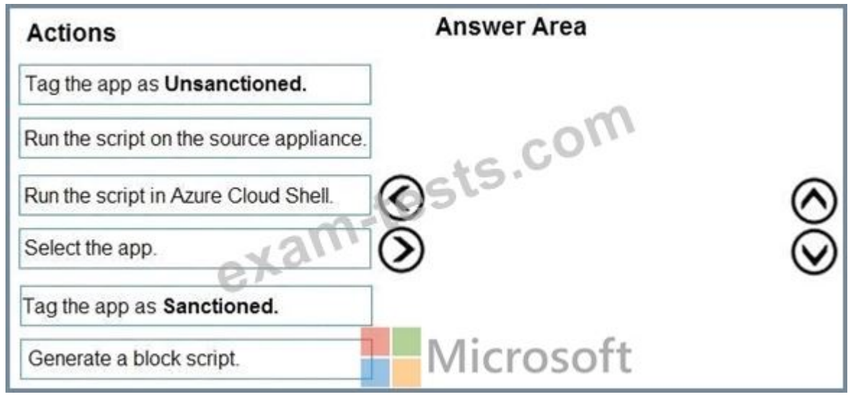
NEW QUESTION: 39

You open the Cloud App Security portal as shown in the following exhibit.

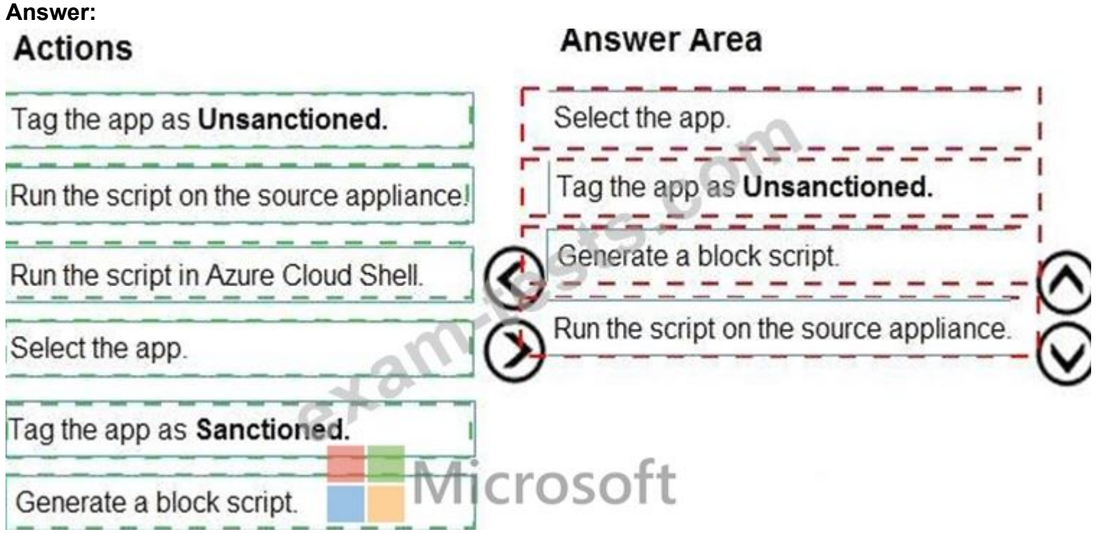


You need to remediate the risk for the Launchpad app.

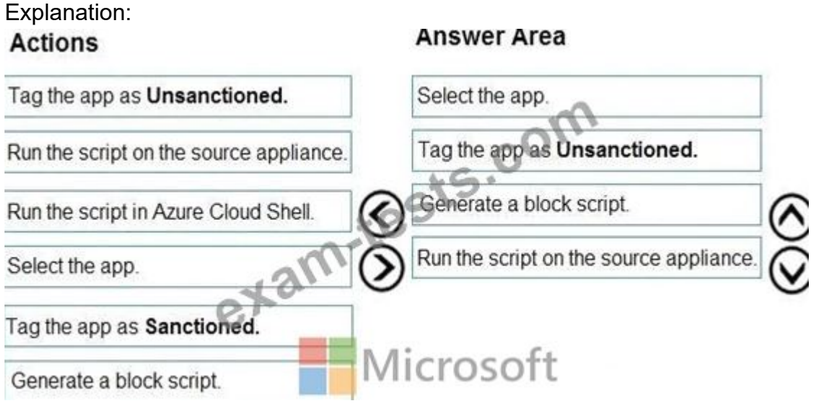
Which four actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.



Answer:



Explanation:



Reference:

https://docs.microsoft.com/en-us/cloud-app-security/governance-discovery

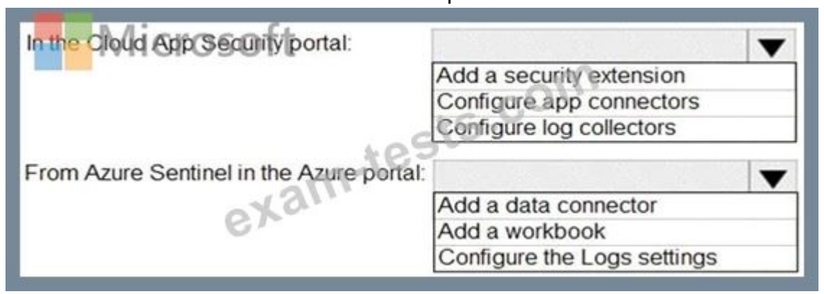
NEW QUESTION: 40
You have a Microsoft 365 subscription.
You have 1,000 Windows devices that have a third-party antivirus product installed and Microsoft Defender Antivirus in passive mode. You need to ensure that the devices are protected from malicious artifacts that were undetected by the third-party antivirus product Solution: You enable automated investigation and response (AIR).
Does this meet the goal?
A. No
B. Yes
Answer: A (LEAVE A REPLY)

NEW QUESTION: 41
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.

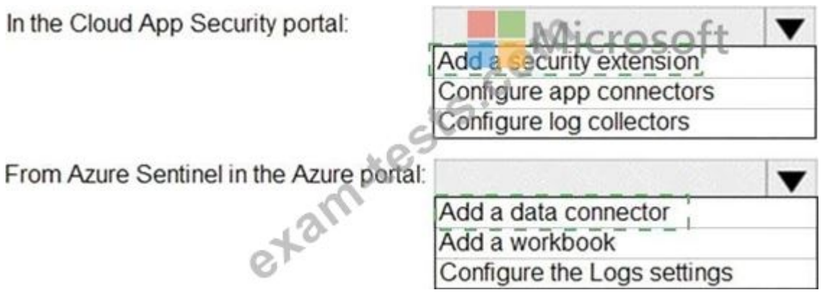
Answer:

NEW QUESTION: 42
You need to configure the Azure Sentinel integration to meet the Azure Sentinel requirements.

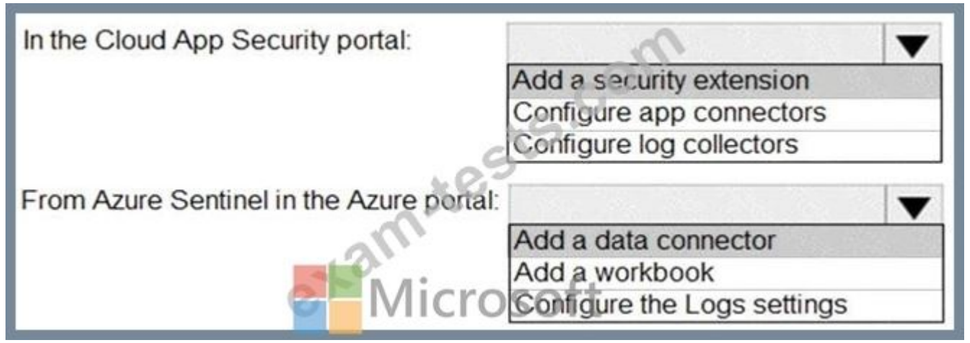
What should you do? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



Answer:



Explanation:

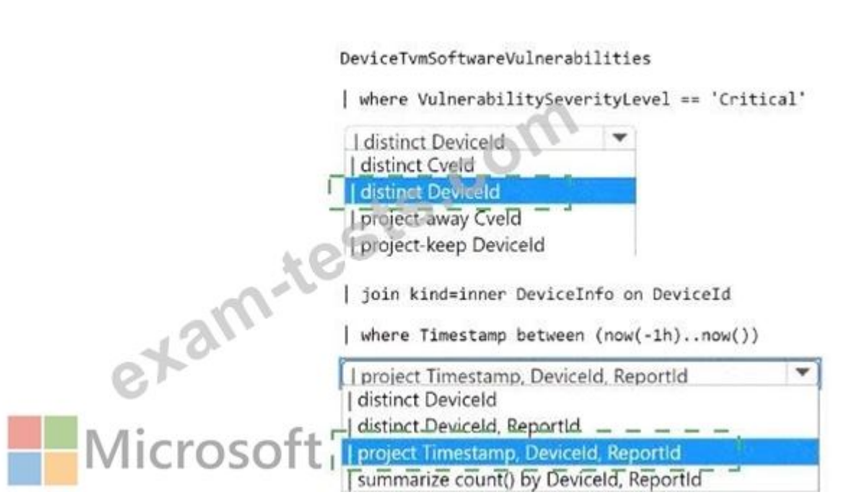


Reference:
https://docs.microsoft.com/en-us/cloud-app-security/siem-sentinel

NEW QUESTION: 43
You have a Microsoft 365 E5 subscription that uses Microsoft Defender for Endpoint. You need to create a detection rule that meets the following requirements:
* Is triggered when a device that has critical software vulnerabilities was active during the last hour
* Limits the number of duplicate results
NOTE: Each correct selection is worth one point.
How should you complete the KQL query? To answer, select the appropriate options in the answer area.

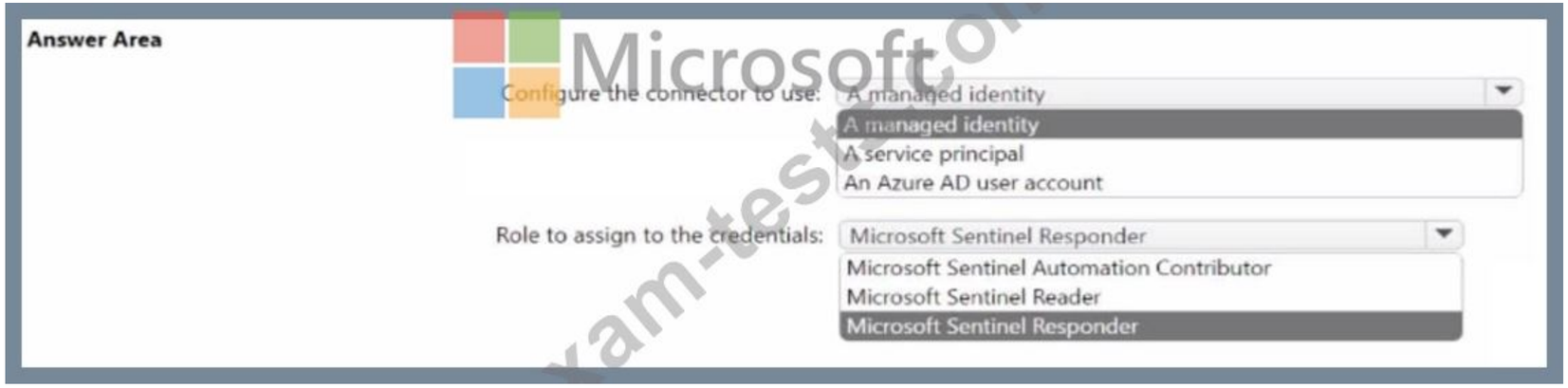
Answer Area

Answer:

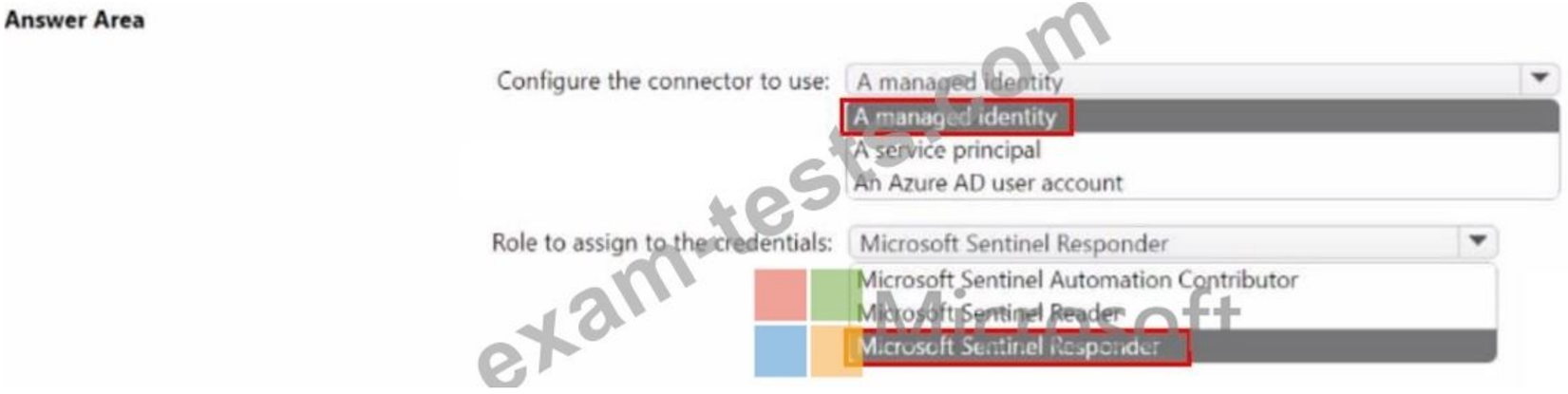


Explanation:

NEW QUESTION: 44
You have a Microsoft Sentinel workspace named sws1.
You plan to create an Azure logic app that will raise an incident in an on-premises IT service management system when an incident is generated in sws1.
You need to configure the Microsoft Sentinel connector credentials for the logic app. The solution must meet the following requirements:
* Minimize administrative effort.
* Use the principle of least privilege.
How should you configure the credentials? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



Answer:



NEW QUESTION: 45
You have an Azure subscription that uses Azure Defender.
You plan to use Azure Security Center workflow automation to respond to Azure Defender threat alerts.
You need to create an Azure policy that will perform threat remediation automatically.
What should you include in the solution? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

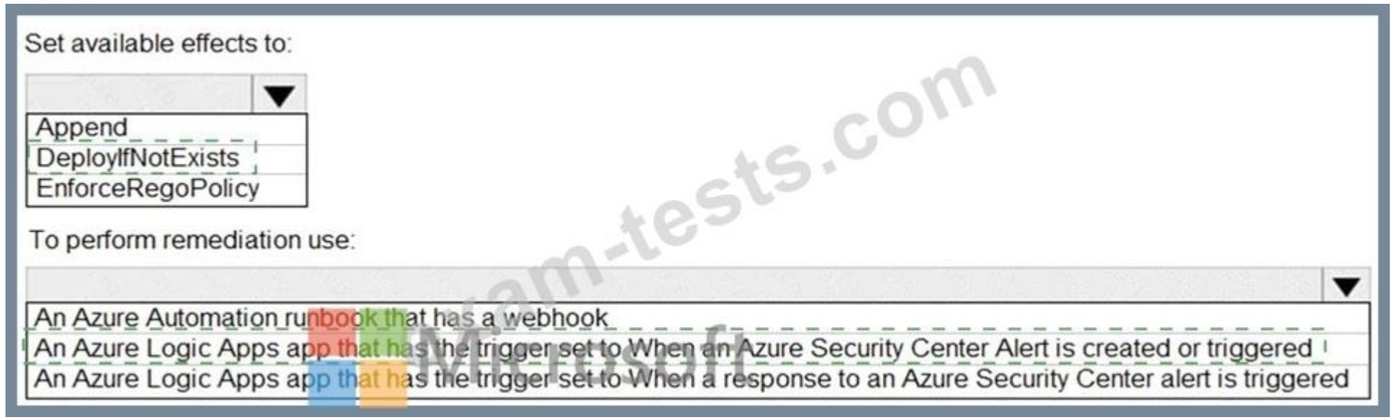
Set available effects to:

Append
DeployIfNotExists
EnforceRegoPolicy

To perform remediation use:

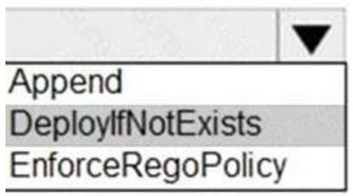
An Azure Automation runbook that has a webhook
An Azure Logic Apps app that has the trigger set to When an Azure Security Center Alert is created or triggered
An Azure Logic Apps app that has the trigger set to When a response to an Azure Security Center alert is triggered

Answer:

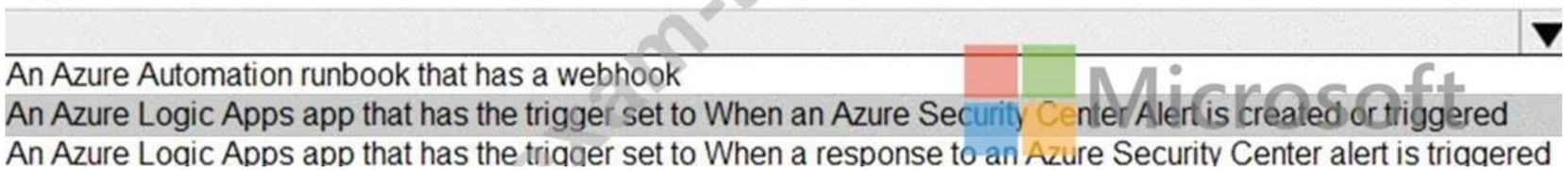


Explanation:

Set available effects to:



To perform remediation use:



Reference:
https://docs.microsoft.com/en-us/azure/governance/policy/concepts/effects
https://docs.microsoft.com/en-us/azure/security-center/workflow-automation

NEW QUESTION: 46
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 Functions
Answer: B (LEAVE A REPLY)
D Azure Sentinel livestreams
Reference:
https://docs.microsoft.com/en-us/azure/sentinel/automate-responses-with-playbooks
Topic 1, Contoso Ltd
Existing Environment
End-User Environment
All users at Contoso use Windows 10 devices. Each user is licensed for Microsoft 365. In addition, iOS devices are distributed to the members of the sales team at Contoso.
Cloud and Hybrid Infrastructure
All Contoso applications are deployed to Azure.
You enable Microsoft Cloud App Security.
Contoso and Fabrikam have different Azure Active Directory (Azure AD) tenants. Fabrikam recently purchased an Azure subscription and enabled Azure Defender for all supported resource types.
Current Problems
The security team at Contoso receives a large number of cybersecurity alerts. The security team spends too much time identifying which cybersecurity alerts are legitimate threats, and which are not.
The Contoso sales team uses only iOS devices. The sales team members exchange files with customers by using a variety of third-party tools. In the past, the sales team experienced various attacks on their devices.
The marketing team at Contoso has several Microsoft SharePoint Online sites for collaborating with external vendors. The marketing team has had several incidents in which vendors uploaded files that contain malware.
The executive team at Contoso suspects a security breach. The executive team requests that you identify which files had more than five activities during the past 48 hours, including data access, download, or deletion for Microsoft

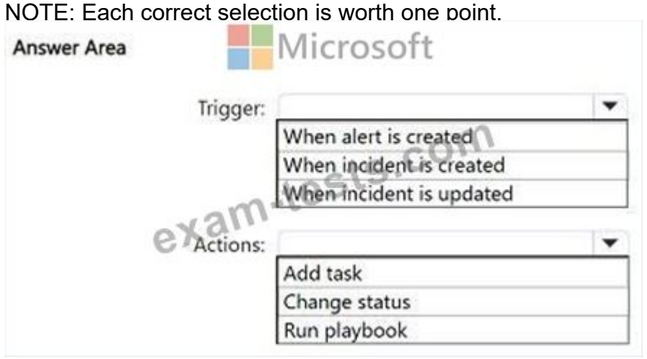
Cloud App Security-protected applications.
Requirements
Planned Changes
Contoso plans to integrate the security operations of both companies and manage all security operations centrally.
Technical Requirements
Contoso identifies the following technical requirements:
Receive alerts if an Azure virtual machine is under brute force attack.
Use Azure Sentinel to reduce organizational risk by rapidly remediating active attacks on the environment.
Implement Azure Sentinel queries that correlate data across the Azure AD tenants of Contoso and Fabrikam.
Develop a procedure to remediate Azure Defender for Key Vault alerts for Fabrikam in case of external attackers and a potential compromise of its own Azure AD applications.
Identify all cases of users who failed to sign in to an Azure resource for the first time from a given country. A junior security administrator provides you with the following incomplete query.
BehaviorAnalytics
| where ActivityType == "FailedLogOn"
| where _____ == True

NEW QUESTION: 47
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 (LEAVE A REPLY)
In Microsoft Defender for Cloud (previously Azure Security Center and Azure Defender), email notifications for security alerts are configured under the "Pricing & settings" section of the workspace or subscription settings. According to Microsoft documentation, each subscription connected to Defender for Cloud has a "Pricing & settings" page that allows administrators to manage configurations such as Defender plan activation, data collection settings, and email notifications for security alerts .
To enable the SOC team to receive alert notifications, you navigate to Microsoft Defender for Cloud # Environment settings # [Select Subscription] # Pricing & settings # Email notifications . There, you can specify:
* The email addresses (up to 200) that will receive alerts.
* Whether to send notifications for high-severity alerts only or for all alerts.
* Whether to send to subscription owners, contributors, or specific emails .
This configuration ensures that alert emails are automatically sent whenever Defender for Cloud generates new security alerts, allowing the Security Operations team to stay informed without manual monitoring.
The other options are incorrect because:
* Security solutions is for integrating third-party or partner security products.

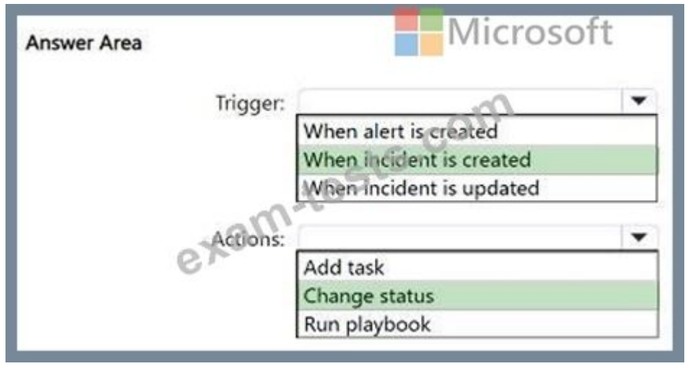
* Security policy defines compliance and assessment standards.
* Security alerts shows existing alerts but does not control notification settings.
* Azure Defender is the protection plan; it doesn't control notification preferences.
Therefore, the correct answer is C. Pricing & settings .

NEW QUESTION: 48
You need to visualize Microsoft Sentinel data and enrich the data by using third-party data sources to identify indicators of compromise (IoC).
What should you use?
A. notebooks in Microsoft Sentinel
B. Microsoft Defender for Cloud Apps
C. Azure Monitor
Answer: A (LEAVE A REPLY)
Notebooks are interactive tools that allow you to run Python code, query data, perform machine learning, and create visualizations. Notebooks can help you hunt for threats, investigate incidents, and perform data analysis using Microsoft Sentinel data and external data sources.

NEW QUESTION: 49
Hotspot Question
You have a Microsoft Sentinel workspace.
You need to configure the Fusion analytics rule to temporarily suppress incidents generated by a Microsoft Defender connector. The solution must meet the following requirements:
- Minimize impact on the ability to detect multistage attacks.
- Minimize administrative effort.
How should you configure the rule? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



Answer:



NEW QUESTION: 50
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. Configure auto-provisioning by setting the security event storage 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. Configure auto-provisioning by setting the security event storage to All Events.
E. From Defender for Cloud in the Azure portal, enable Microsoft Defender for Servers.
Answer: A,E (LEAVE A REPLY)
Enable Auto-Provisioning from Defender for Cloud. And there you will be ask which Secrity Events should be stored. It is Nonne - Common - All. And without enabling Defender for servers in the Defender for Cloud Portal this won't work.

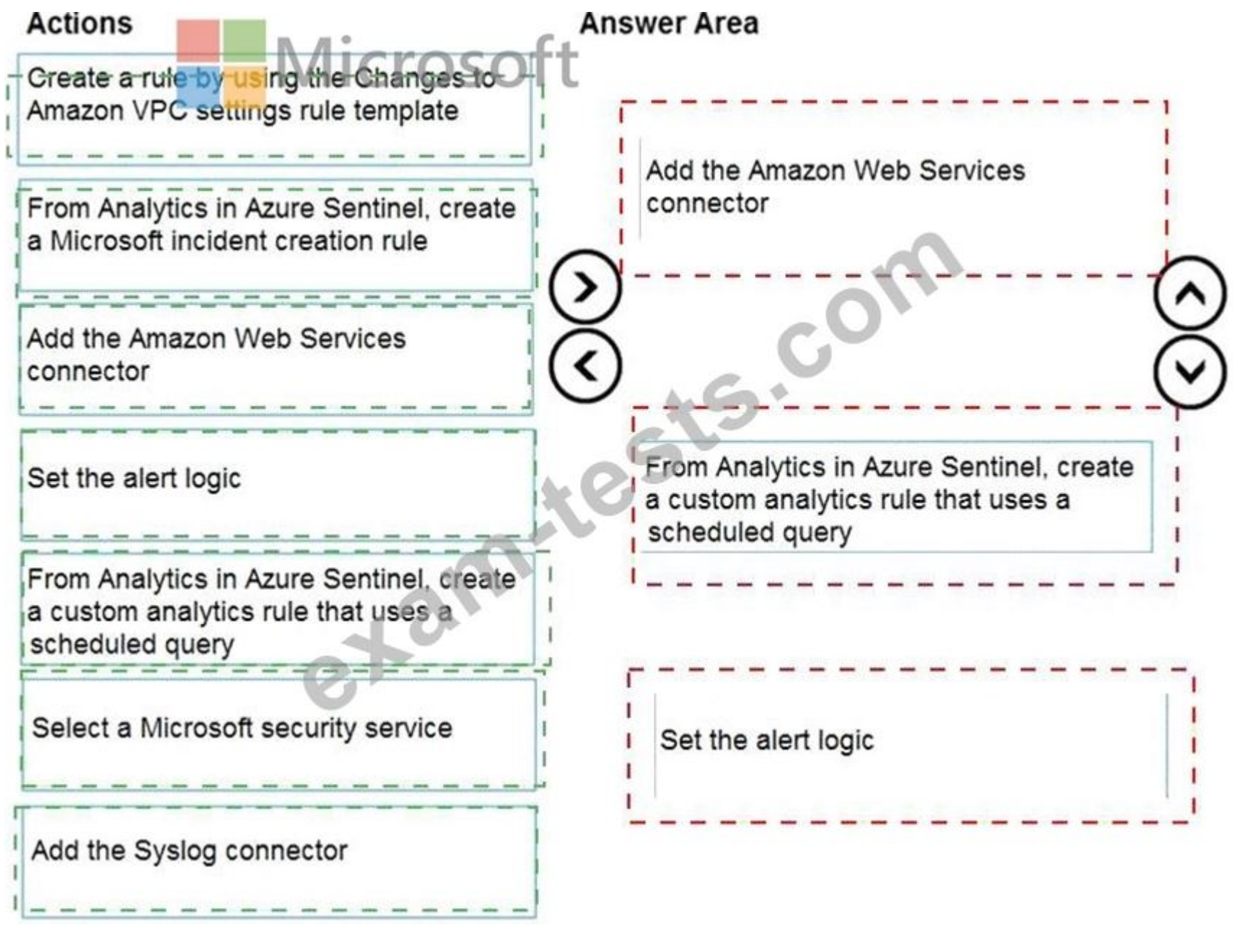
NEW QUESTION: 51
You need to use an Azure Sentinel analytics rule to search for specific criteria in Amazon Web Services (AWS) logs and to generate incidents.
Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.
a Microsoft 365 E5

Actions

- 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

Answer Area

Answer:



Explanation:

Reference:
https://docs.microsoft.com/en-us/azure/sentinel/detect-threats-custom

NEW QUESTION: 52
You have an Azure subscription that contains a user named User1 and a Microsoft Sentinel workspace named WS1. WS1 uses Microsoft Defender for Cloud.
You have the Microsoft security analytics rules shown in the following table.

Name	Service	Severity	Action
Rule1	Defender for Cloud	High	Create incident
Rule2	Defender for Cloud	High	Create incident
Rule3	Defender for Cloud	High	Create incident
Rule4	Defender for Cloud	High	Create incident

User1 performs an action that matches Rule1, Rule2, Rule3, and Rule4. How many incidents will be created in WS1?
A. 2
B. 4
C. 1
D. 3
Answer: C (LEAVE A REPLY)

NEW QUESTION: 53
You need to use an Azure Resource Manager template to create a workflow automation that will trigger an automatic remediation when specific security alerts are received by Azure Security Center.
How should you complete the portion of the template that will provision the required Azure resources? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

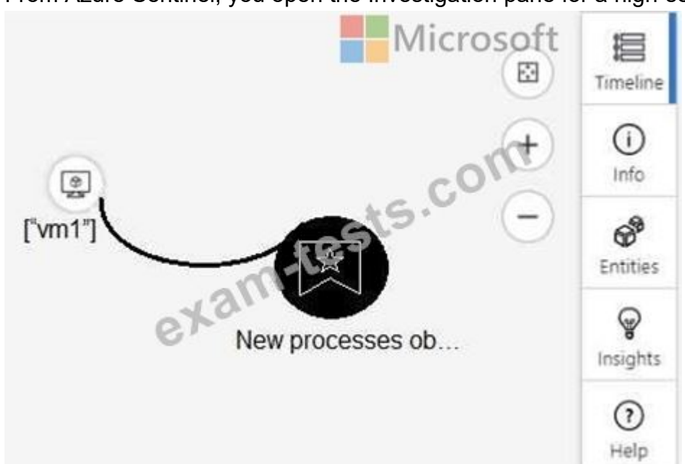
```
"resources": [
  {
    "type": "[ Microsoft.Automation | Microsoft.Logic | Microsoft.Security ]/automations",
    "apiVersion": "2019-01-01-preview",
    "name": "[parameters('name')]",
    "location": "[parameters('location')]",
    "properties": {
      "description": "[format(variables('description'), '{0}', parameters
('subscriptionId'))]",
      "isEnabled": true,
      "actions": [
        {
          "actionType": "LogicApp",
          "logicAppResourceId": "[resourceId('ITEM2/workflows', parameters
('appName'))]",
          "uri": "[listCallbackURL(resourceId(parameters('subscriptionId')
parameters('resourceGroupName'), '[ Microsoft.Automation | Microsoft.Logic | Microsoft.Security ]/workflows/triggers',
parameters('appName'), 'manual'), '2019-05-01').value]"
        }
```

Answer:

```
"resources": [
   {
     "type": "                                  /automations",
                Microsoft.Automation
                Microsoft.Logic
                Microsoft.Security
     "apiVersion": "2019-01-01-preview",
     "name": "[parameters('name')]",
     "location": "[parameters('location')]",
     "properties": {
        "description": "[format(variables('description'), '{0}', parameters
('subscriptionId'))]",
        "isEnabled": true,
        "actions": [
           {
              "actionType": "LogicApp",
              "logicAppResourceId": "[resourceId('ITEM2/workflows', parameters
('appName'))]",
              "uri": "[listCallbackURL(resourceId(parameters('subscriptionId'),
parameters('resourceGroupName'), '                                  /workflows/triggers',
                                   Microsoft.Automation
                                   Microsoft.Logic
                                   Microsoft.Security
parameters('appName'), 'manual'), '2019-05-01').value]"
           }
     ],
```


Reference:
https://docs.microsoft.com/en-us/azure/security-center/quickstart-automation-alert

NEW QUESTION: 54
HOTSPOT
From Azure Sentinel, you open the Investigation pane for a high-severity incident as shown in the following exhibit.

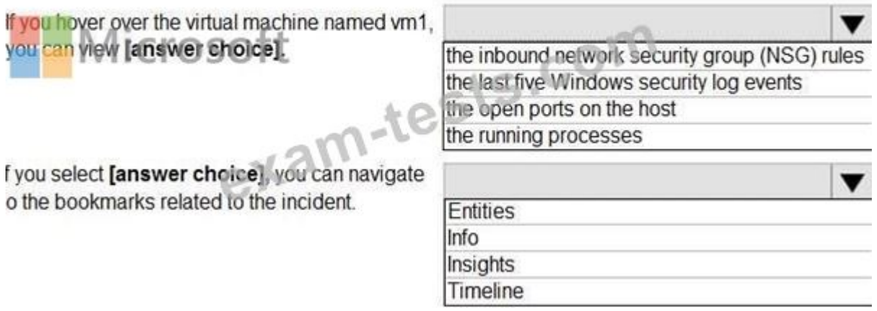


Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.

NOTE: Each correct selection is worth one point.

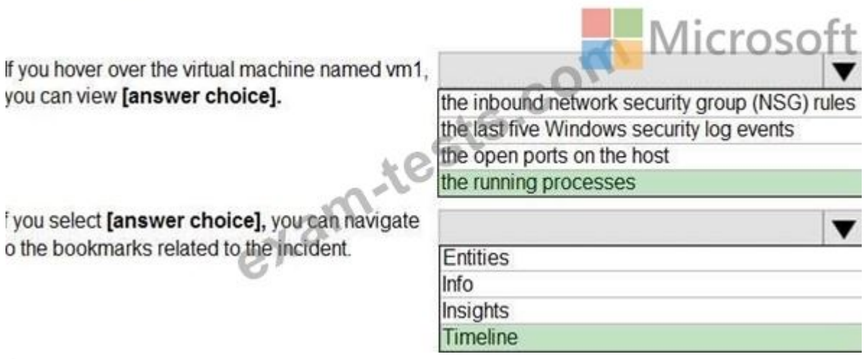
Hot Area:

Answer Area



Answer:

Answer Area



Section: [none]

Explanation/Reference:

https://docs.microsoft.com/en-us/azure/sentinel/tutorial-investigate-cases#use-the-investigation-graph-to-deep- dive

NEW QUESTION: 55

You have an Azure subscription.

You need to delegate permissions to meet the following requirements:

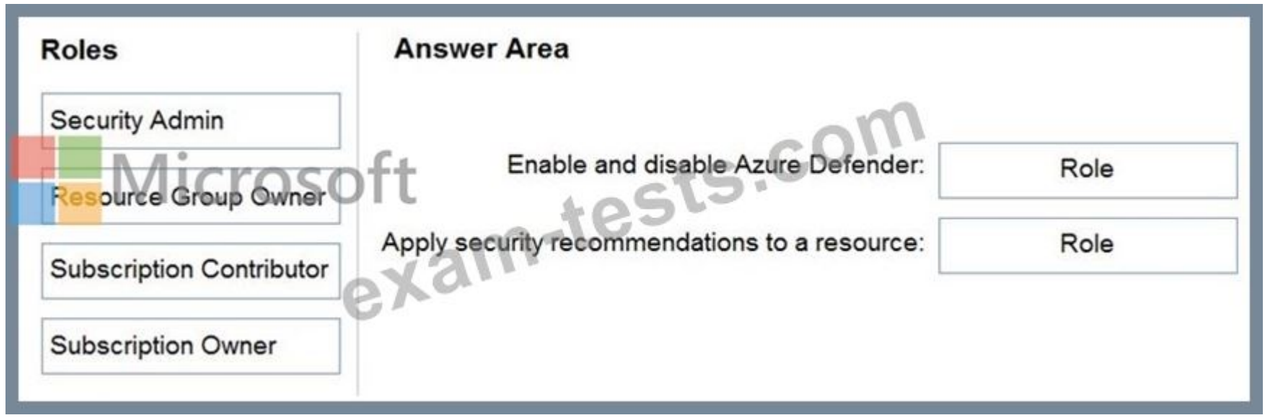
Enable and disable Azure Defender.

Apply security recommendations to resource.

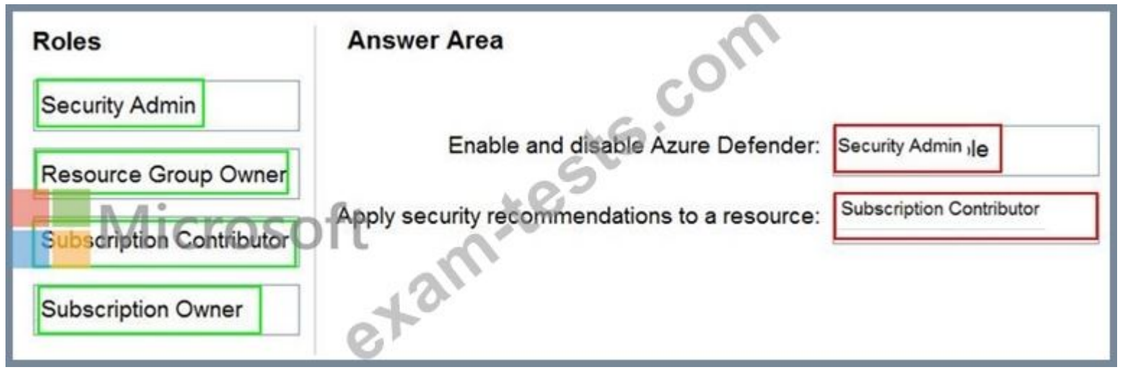
The solution must use the principle of least privilege.

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.



Answer:



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

NEW QUESTION: 56
You use Azure Sentinel to monitor irregular Azure activity.
You create custom analytics rules to detect threats as shown in the following exhibit.

Home > Azure Sentinel workspaces > Azure Sentinel

Analytics rule wizard – Edit existing rule

DeployVM

General | Set rule logic | Incident settings | Automated response | Review and create

Define the logic for your new analytics rule.

Rule query

Any time details set here will be within the scope defined below in the Query scheduling fields.

```
AzureActivity
| where OperationName == "Create or Update Virtual Machine"
or OperationName == "Create Deployment"
| where ActivityStatus == "Succeeded"
| make-series dcount(ResourceId) default=0
on EventSubmissionTimestamp in range(ago(7d), now(), 1d) by Caller
```

View query results >

Map entities

Map the entities recognized by Azure Sentinel to the appropriate columns available in your query results. This enables Azure Sentinel to recognize the entities that are part of the alerts for further analysis. Entity type must be a string.

Entity Type	Column	
Account	Choose column	Add
Host	Choose column	Add
IP	Choose column	Add
URL	Choose column	Add
FileHash	Choose column	Add

Query scheduling

Run query every *

5 | Minutes

Lookup data from the last *

5 | Hours

Alert threshold

Generate alert when number of query results *

Is greater than | 2

Event grouping

Configure how rule query results are grouped into alerts

- (•) Group all events into a single alert
- ( ) Trigger an alert for each event

Suppression

Stop running query after alert is generated

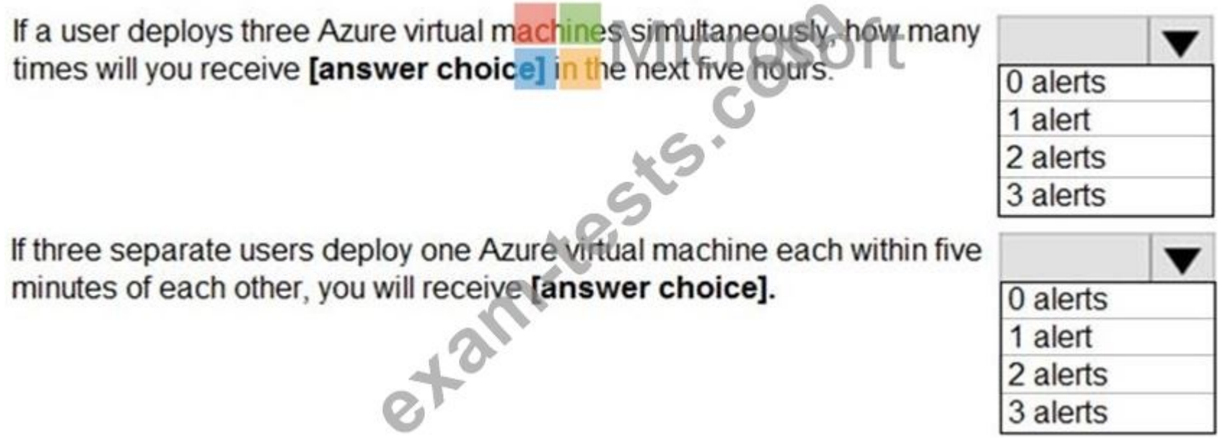
On | Off

Stop running query for *

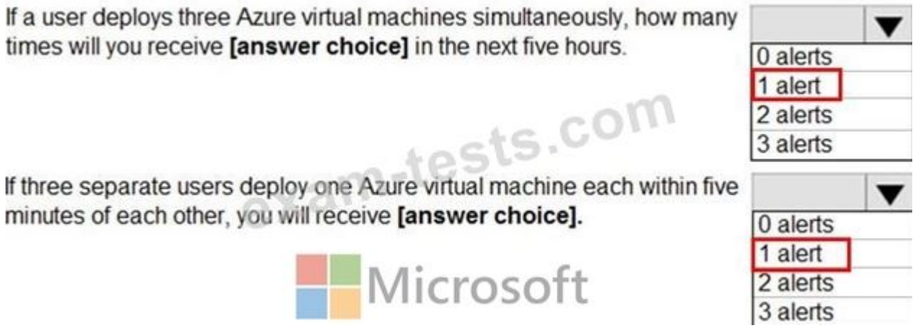
5 | Hours

Previous | Next : Incident settings >

You do NOT define any incident settings as part of the rule definition.
Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.
NOTE: Each correct selection is worth one point.

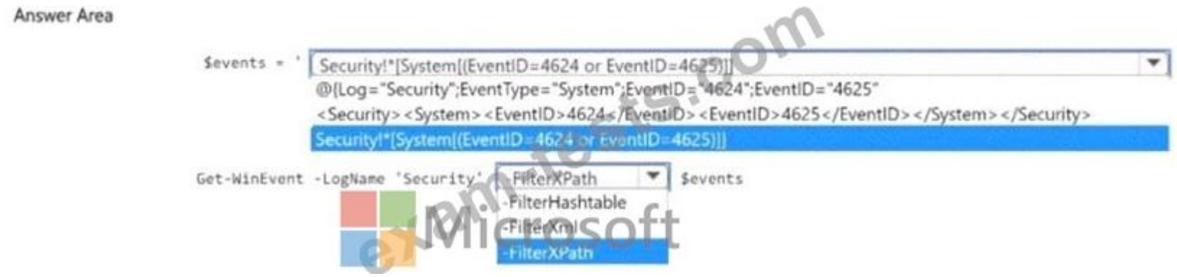


Answer:



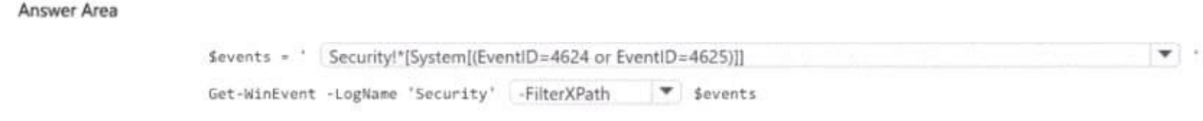
Reference:
https://docs.microsoft.com/en-us/azure/sentinel/tutorial-detect-threats-custom

NEW QUESTION: 57
You have on-premises servers that run Windows Server.
You have a Microsoft Sentinel workspace named SW1. SW1 is configured to collect Windows Security log entries from the servers by using the Azure Monitor Agent data connector.
You plan to limit the scope of collected events to events 4624 and 462S only.
You need to use a PowerShell script to validate the syntax of the filter applied to the connector.
How should you complete the script? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



Answer:

Explanation:



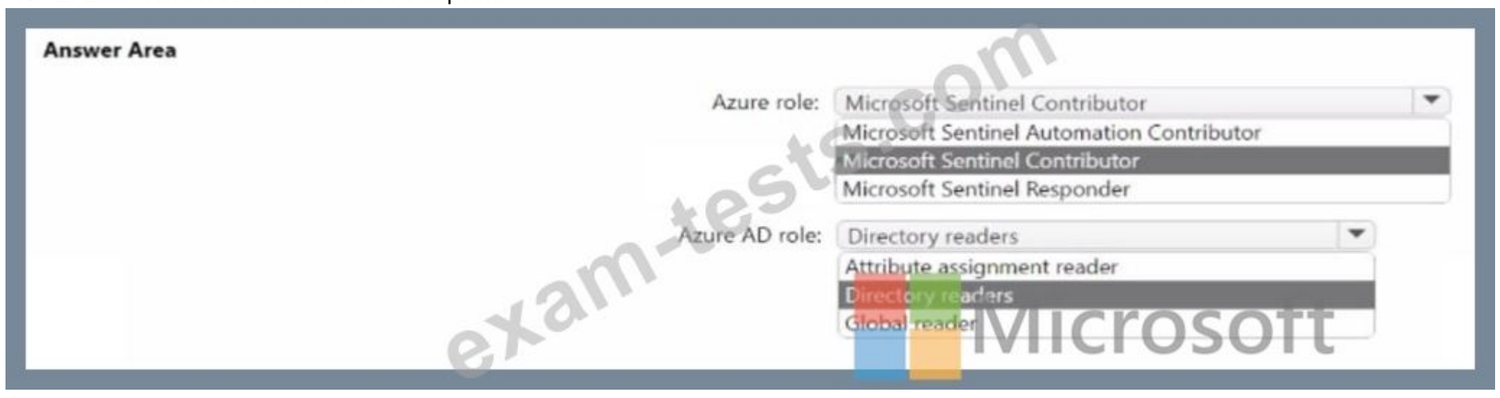
NEW QUESTION: 58

You have an Azure subscription that contains a quest user named Userl and a Microsoft Sentinel workspace named workspacel.

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.

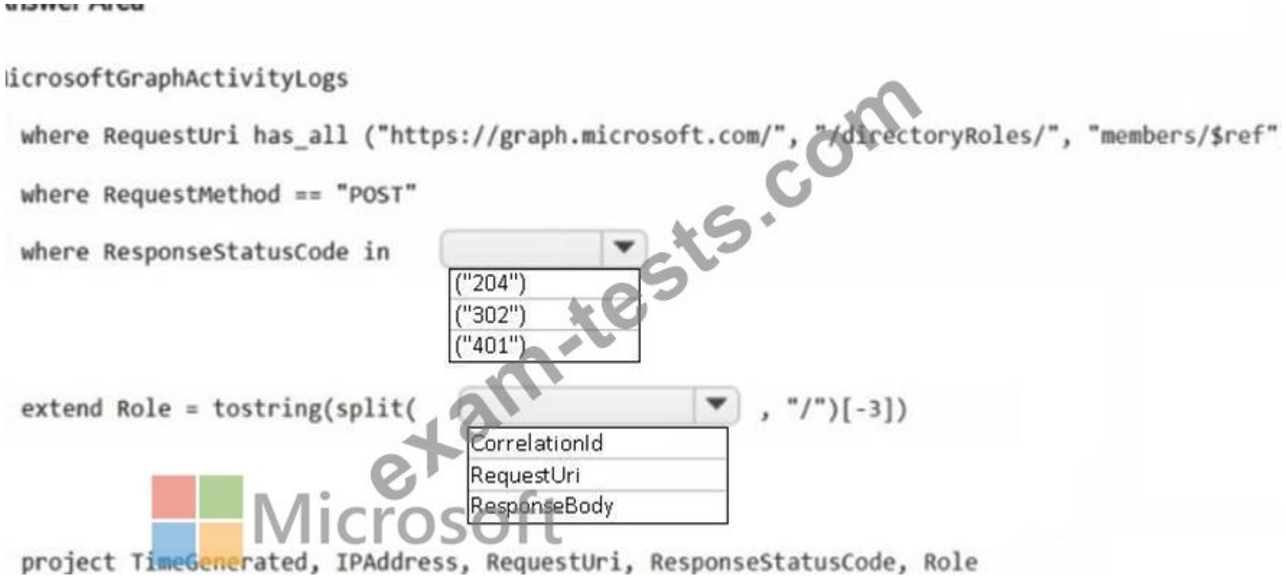
NOTE: Each correct selection is worth one point.



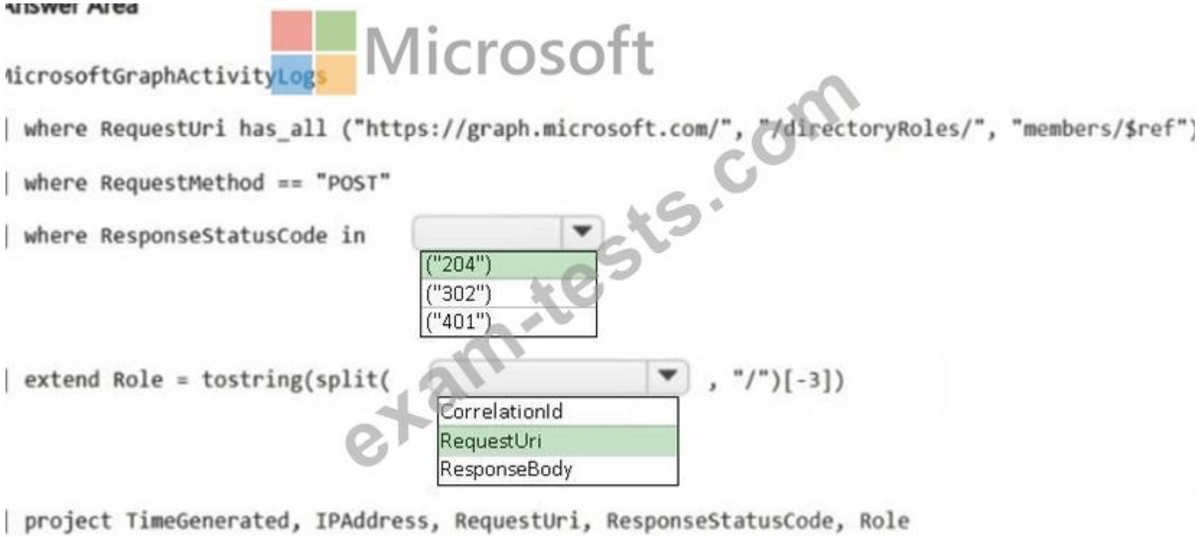
Answer:

NEW QUESTION: 59
You have two Microsoft Entra tenants named Tenantl and Tenant2. Each tenant is linked to an Azure subscription. Tenant! contains a group named Group1. Tenant2 contains a group named Group2.
You need to implement Microsoft Sentinel for each tenant. The solution must meet the following requirements:
* Ensure that Group1 can manage security incidents for Tenantl and Tenant2 in a single workspace.
* Ensure that Group2 can manage security incidents only for Tenant2.
* Minimize the use of guest accounts.
* Minimize administrative effort.
* Minimize costs.
What should you include in the solution?
A. two workspaces and Azure Lighthouse
B. two workspaces and granular delegated admin privileges (GDAP)
C. one workspace and Privileged Identity Management (PIM)
D. one workspace and multiple role-based access control (RBAC) role assignments
Answer: A (LEAVE A REPLY)

NEW QUESTION: 60
Hotspot Question
You have a Microsoft 365 E5 subscription that is linked to a Microsoft Entra tenant named contoso.com.
You need to query Microsoft Graph activity logs to identify changes to the roles in contoso.com.
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:



NEW QUESTION: 61

You have a Microsoft 365 E5 subscription that uses Microsoft SharePoint Online.

You delete users from the subscription.

You need to be notified if the deleted users downloaded numerous documents from SharePoint Online sites during the month before their accounts were deleted.

What should you use?

A. a file policy in Microsoft Defender for Cloud Apps

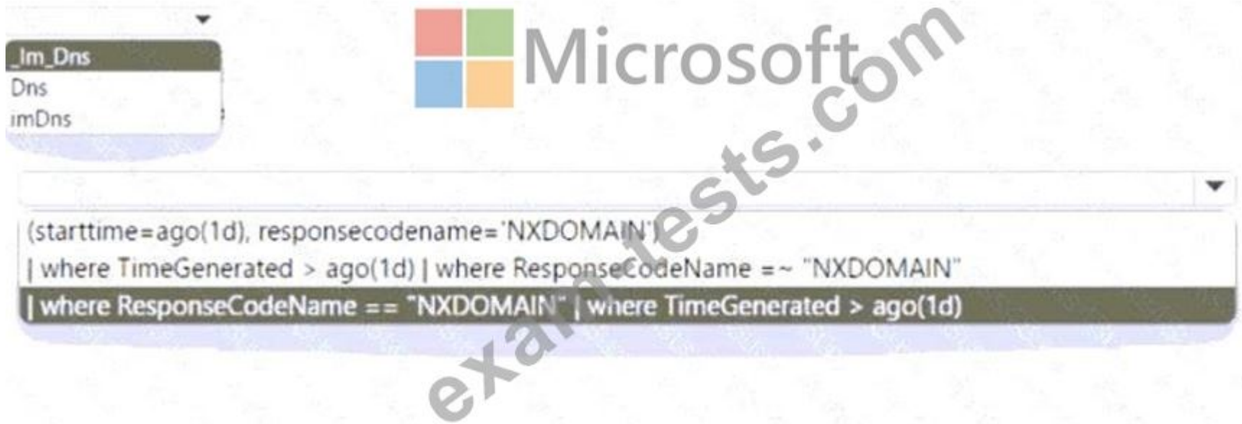
B. an alert policy in Microsoft Defender for Office 365

C. an access review in Microsoft Entra
D. an insider risk management policy in Microsoft Purview
Answer: D (LEAVE A REPLY)

NEW QUESTION: 62
You have an Azure subscription that uses Microsoft Defender for Cloud.
You need to configure Defender for Cloud to mitigate the following risks:
* Vulnerabilities within the application source code
* Exploitation toolkits in declarative templates
* Operations from malicious IP addresses
* Exposed secrets
Which two Defender for Cloud services should you use? Each correct answer presents part of the solution.
NOTE: Each correct answer is worth one point.
A. Microsoft Defender for APIs
B. Microsoft Defender for Resource Manager
C. Microsoft Defender for App Service
D. Microsoft Defender for DevOps
E. Microsoft Defender for Servers
Answer: (SHOW ANSWER)
Microsoft Defender for Cloud provides multiple specialized Defender plans to protect different layers of your environment.
* Microsoft Defender for DevOps helps identify vulnerabilities in source code, exposed secrets, and insecure dependencies by integrating with CI/CD systems like GitHub and Azure DevOps. It scans repositories for known vulnerabilities (CVEs), weak configurations, and exposed credentials before code is deployed. This directly addresses the risks:
* Vulnerabilities within application source code
* Exposed secrets
* Microsoft Defender for Resource Manager protects the Azure control plane and monitors management operations to detect threats such as deployment of malicious templates, exploitation toolkits in IaC (Infrastructure as Code), and operations from malicious IP addresses. It provides alerts when suspicious control-plane actions occur, for example, unexpected activity via ARM or Terraform. This covers:
* Exploitation toolkits in declarative templates
* Operations from malicious IP addresses
Together, these two Defender plans (Defender for DevOps + Defender for Resource Manager) mitigate all four risks listed in the question.
Correct answers: B. Microsoft Defender for Resource Manager and D. Microsoft Defender for DevOps

NEW QUESTION: 63
You have a Microsoft Sentinel workspace named Workspaces
You configure Workspace1 to c
ollect DNS events and deploy the Advanced Security information Model (ASIM) unifying parser for the DNS schema.

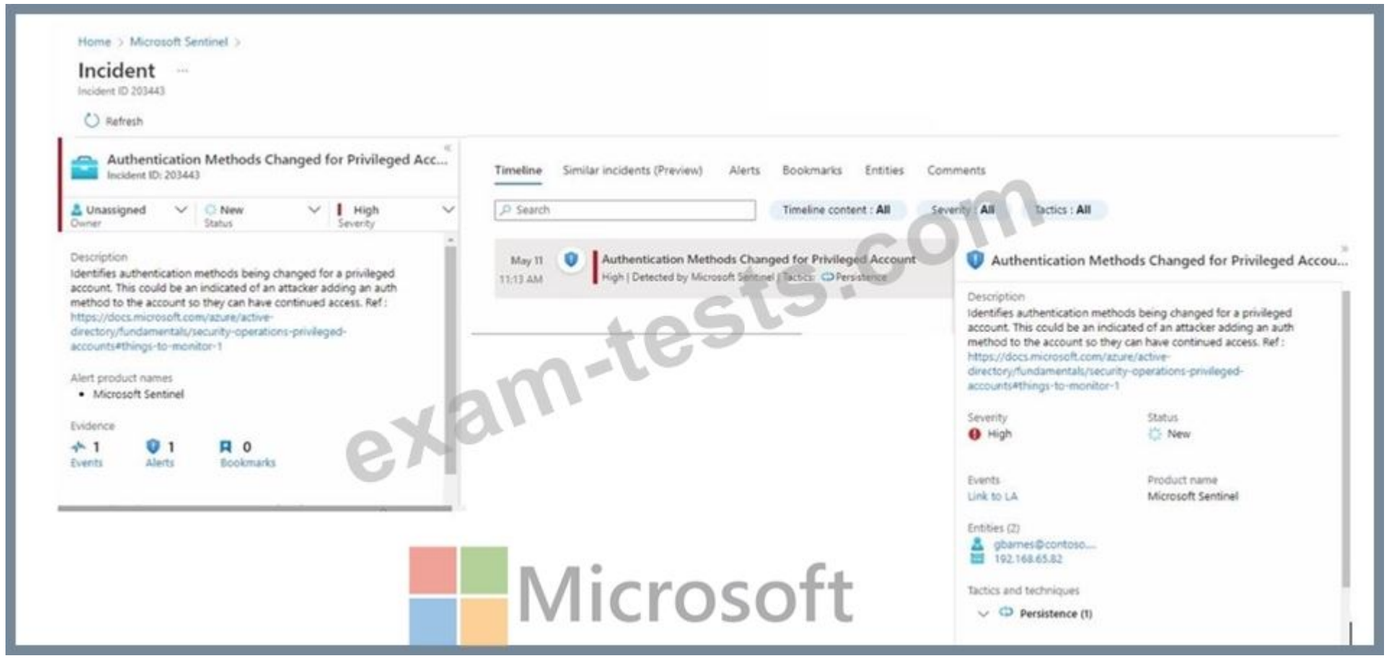
You need to query the ASIM DNS schema to list all the DNS events from the last 24 hours that have a response code of 'NXDOMAIN' and were aggregated by the source IP address in 15-minute intervals. The solution must maximize query performance.
How should you complete the query? To answer, select the appropriate options in the answer area NOTE: Each correct selection is worth one point.



Answer:

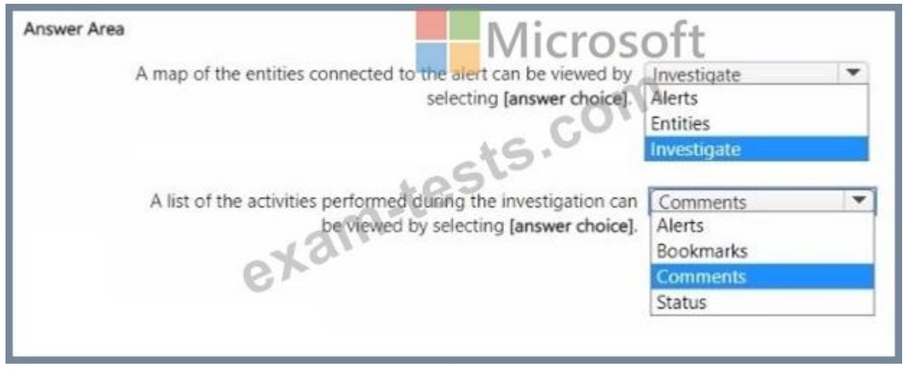
Explanation:

NEW QUESTION: 64
You have a Microsoft Sentinel workspace.
A Microsoft Sentinel incident is generated as shown in the following exhibit.



Use the drop-down menus to select the answer choice that completes each statement based on the information presented in [the graphic.

NOTE: Each correct selection is worth one point.



Answer:

NEW QUESTION: 65
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 (LEAVE A REPLY)
Reference:
https://docs.microsoft.com/en-us/azure/security-center/azure-defender
Topic 2, Litware inc.
Overview
This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.
To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.
At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.
To start the case study
To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.
Overview
Litware Inc. is a renewable company.
Litware has offices in Boston and Seattle. Litware also has remote users located across the United States. To access Litware resources, including cloud resources, the remote users establish a VPN connection to either office.
Existing Environment
Identity Environment
The network contains an Active Directory forest named litware.com that syncs to an Azure Active Directory (Azure AD) tenant named litware.com.
Microsoft 365 Environment
Litware has a Microsoft 365 E5 subscription linked to the litware.com Azure AD tenant. Microsoft Defender for Endpoint is deployed to all computers that run Windows 10. All Microsoft Cloud App Security built-in anomaly detection policies are enabled.
Azure Environment
Litware has an Azure subscription linked to the litware.com Azure AD tenant. The subscription contains resources in the East US Azure region as shown in the following table.

Name	Type	Description
LA1	Log Analytics workspace	Contains logs and metrics collected from all Azure resources and on-premises servers
VM1	Virtual machine	Server that runs Windows Server 2019
VM2	Virtual machine	Server that runs Ubuntu 18.04 LTS

Network Environment
Each Litware office connects directly to the internet and has a site-to-site VPN connection to the virtual networks in the Azure subscription.
On-premises Environment

Name	Operating system	Office	Description
DC1	Windows Server 2019	Boston	Domain controller in litware.com that connects directly to the internet
CLIENT1	Windows 10	Boston	Domain-joined client computer

Current problems

Cloud App Security frequently generates false positive alerts when users connect to both offices simultaneously.

Planned Changes

Litware plans to implement the following changes:

Create and configure Azure Sentinel in the Azure subscription.

Validate Azure Sentinel functionality by using Azure AD test user accounts.

Business Requirements

Litware identifies the following business requirements:

Azure Information Protection Requirements

All files that have security labels and are stored on the Windows 10 computers must be available from the Azure Information Protection - Data discovery dashboard.

Microsoft Defender for Endpoint Requirements

All Cloud App Security unsanctioned apps must be blocked on the Windows 10 computers by using Microsoft Defender for Endpoint.

Microsoft Cloud App Security Requirements

Cloud App Security must identify whether a user connection is anomalous based on tenant-level data.

Azure Defender Requirements

All servers must send logs to the same Log Analytics workspace.

Azure Sentinel Requirements

Litware must meet the following Azure Sentinel requirements:

Integrate Azure Sentinel and Cloud App Security.

Ensure that a user named admin1 can configure Azure Sentinel playbooks.

Create an Azure Sentinel analytics rule based on a custom query. The rule must automatically initiate the execution of a playbook.

Add notes to events that represent data access from a specific IP address to provide the ability to reference the IP address when navigating through an investigation graph while hunting.

Create a test rule that generates alerts when inbound access to Microsoft Office 365 by the Azure AD test user accounts is detected. Alerts generated by the rule must be grouped into individual incidents, with one incident per test user account.

NEW QUESTION: 66

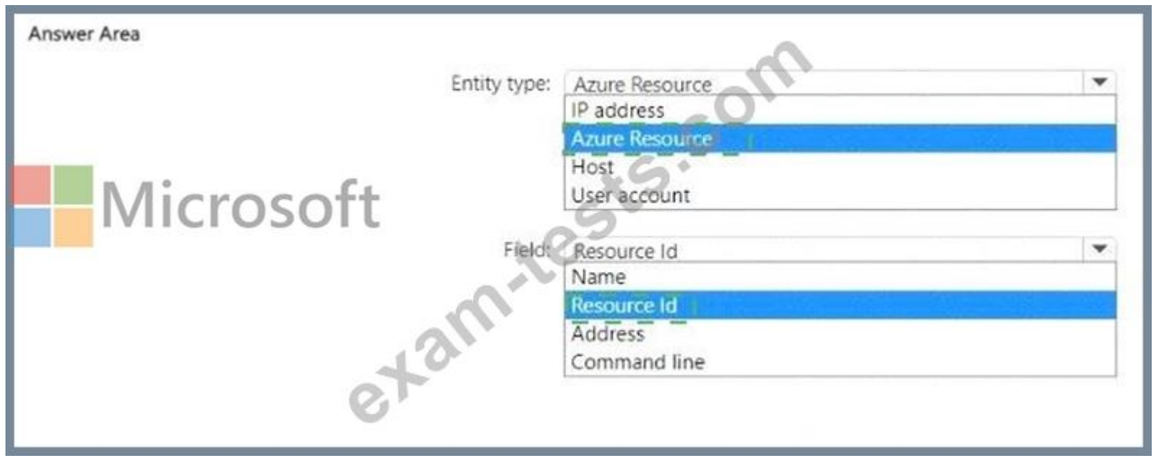
You have an Azure Storage account that will be accessed by multiple Azure Functions apps during the development of an application.

You need to hide Microsoft Defender for Cloud 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.

Answer:



Explanation:

NEW QUESTION: 67

You have a Microsoft 365 E5 subscription that contains a device named Device 1. Device 1 is enrolled in Microsoft Defender for End point.

Device1 reports an incident that includes a file named File1 exe as evidence.

You initiate the Collect Investigation Package action and download the ZIP file.

You need to identify the first and last time File1.exe was executed.

What should you review in the investigation package?

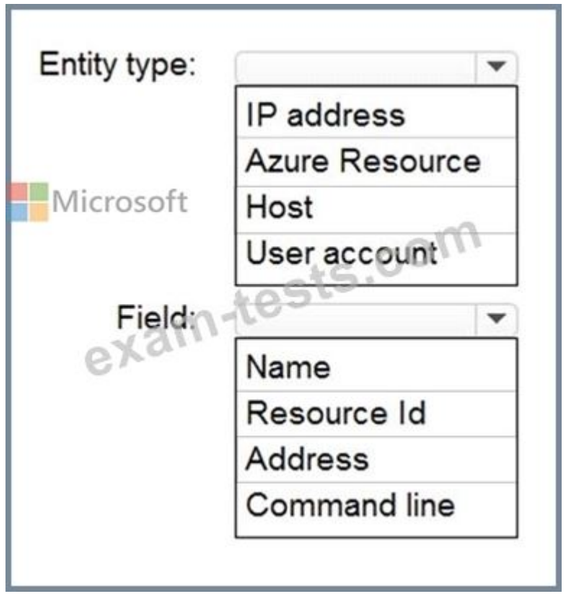
A. Processes

B. Scheduled tasks
C. Autoruns
D. Security event log
E. Prefetch files
Answer: E (LEAVE A REPLY)
When you initiate the Collect Investigation Package action on a device in Microsoft Defender for Endpoint, the package includes many forensic artifacts that help you trace file usage, process execution, and system behavior. Among those artifacts are prefetch files. Prefetch files record metadata about which executables were run and when, and can provide first/last execution timestamps. Whizlabs+2InfoSec Write-ups+2 Specifically, Microsoft documents (e.g. Respond-machine alerts) describe that the investigation package contains folders such as Autoruns, Processes, Scheduled tasks, Security event log, Users and Groups, Prefetch files, among others. InfoSec Write-ups+2Whizlabs+2 Among those, the Prefetch files are the best source to determine the first and last run time of a given executable (like File1.exe). Other artifacts (process history, event logs) might also show execution events, but prefetch is the artifact designed for showing executable run metadata and is most commonly used for that purpose in forensic investigations. InfoSec Write-ups+2ExamTopics+2 Because the question specifically asks "first and last time File1.exe was executed," reviewing Prefetch files in the investigation package is the correct approach.

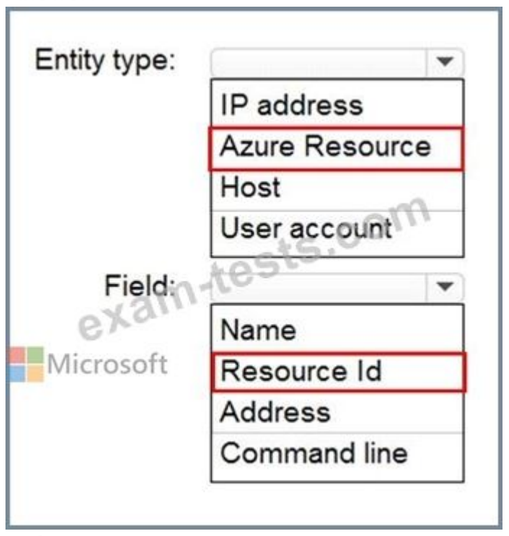
NEW QUESTION: 68
You need to modify the anomaly detection policy settings to meet the Cloud App Security requirements.
Which policy should you modify?
A. Activity from suspicious IP addresses
B. Activity from anonymous IP addresses
C. Impossible travel
D. Risky sign-in
Answer: C (LEAVE A REPLY)
Section: [none]
Explanation/Reference:
https://docs.microsoft.com/en-us/cloud-app-security/anomaly-detection-policy

NEW QUESTION: 69
You have an Azure subscription named Sub1 that uses Microsoft Defender for Cloud.
You need to assign the PCI DSS 4.0 initiative to Sub1 and have the initiative displayed in the Defender for Cloud Regulatory compliance dashboard.
From Security policies in the Environment settings, you discover that the option to add more industry and regulatory standards is unavailable.
What should you do first?
A. Configure the Continuous export settings for Azure Event Hubs.
B. Configure the Continuous export settings for Log Analytics.
C. Disable the Microsoft Cloud Security Benchmark (MCSB) assignment.
D. Enable the Cloud Security Posture Management (CSPM) plan for the subscription.
Answer: (SHOW ANSWER)

NEW QUESTION: 70
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.



Answer:



Reference:
https://techcommunity.microsoft.com/t5/azure-security-center/suppression-rules-for-azure-security-center-alerts-are-now/ba-p/1404920

NEW QUESTION: 71
You have an Azure subscription.
You need to delegate permissions to meet the following requirements:
* Enable and disable advanced features of Microsoft Defender for Cloud.
* Apply security recommendations to a resource.

The solution must use the principle of least privilege.
Which Microsoft Defender for Cloud role should you use for each requirement? To answer, drag the appropriate roles to the correct requirements. Each role may be used once, mote 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.

Answer:

NEW QUESTION: 72
Drag and Drop Question
You have 50 on-premises servers.
You have an Azure subscription that uses Microsoft Defender for Cloud. The Defender for Cloud deployment has Microsoft Defender for Servers and automatic provisioning enabled.
You need to configure Defender for Cloud to support the on-premises servers. The solution must meet the following requirements:
- Provide threat and vulnerability management.
- Support data collection rules.
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 the Add servers with Azure Arc settings in the Azure portal, generate an installation script.
- From the Data controller settings in the Azure portal, create an Azure Arc data controller.
- On the on-premises servers, install the Log Analytics agent.
- On the on-premises servers, install the Azure Connected Machine agent.
- On the on-premises servers, install the Azure Monitor agent.

Answer Area

Answer:

Actions

- From the Data controller settings in the Azure portal, create an Azure Arc data controller.
- On the on-premises servers, install the Log Analytics agent.

Answer Area

- From the Add servers with Azure Arc settings in the Azure portal, generate an installation script.
- On the on-premises servers, install the Azure Connected Machine agent.
- On the on-premises servers, install the Azure Monitor agent.

Explanation:
https://learn.microsoft.com/en-us/azure/azure-monitor/essentials/data-collection
https://learn.microsoft.com/en-us/azure/azure-arc/servers/learn/quick-enable-hybrid-vm

NEW QUESTION: 73
Hotspot Question
Your on-premises network contains a Hyper-V cluster. The cluster contains the virtual machines shown in the following table.

Name	Operating system	Azure Connected Machine agent	Azure Monitoring Agent
Server1	Windows Server 2019	Not installed	Installed
Server2	Windows Server 2016	Installed	Not installed
Server3	Linux Ubuntu 20.04	Not installed	Installed

You have a Microsoft Sentinel workspace named SW1.

You have a data collection rule (DCR) that has the following configurations:

- Name: DCR1
- Destination: SW1
- Platform type: All
- Data collection endpoint: None
- Data source: Windows event logs, Linux syslog

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
Server1 can be added to DCR1 as a resource and all the Windows event logs can be gathered.	○	○
Server2 can be added to DCR1 as a resource and specific Windows event log events can be gathered.	○	○
Server3 can be added to DCR1 as a resource and all the Linux syslog data can be gathered.	○	○

Answer:

Answer Area

Statements	Yes	No
Server1 can be added to DCR1 as a resource and all the Windows event logs can be gathered.	○	○
Server2 can be added to DCR1 as a resource and specific Windows event log events can be gathered.	○	○
Server3 can be added to DCR1 as a resource and all the Linux syslog data can be gathered.	○	○

NEW QUESTION: 74
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: A,C,D (LEAVE A REPLY)
https://docs.microsoft.com/en-us/learn/modules/deploy-microsoft-defender-for-endpoints-environment/4-manage-access

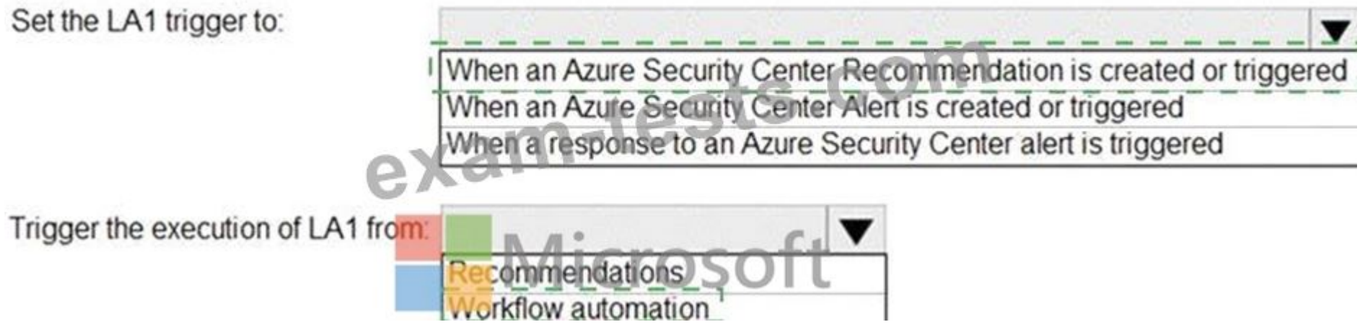
NEW QUESTION: 75
You have an Azure subscription that has Azure Defender enabled for all supported resource types.
You create an Azure logic app named LA1.
You plan to use LA1 to automatically remediate security risks detected in Azure Security Center.
View the window
You need to test LA1 in Security 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

Answer Area



Explanation:

Reference:
https://docs.microsoft.com/en-us/azure/security-center/workflow-automation#create-a-logic-app-and-define-whe

NEW QUESTION: 76
You need to use an Azure Resource Manager template to create a workflow automation that will trigger an automatic remediation when specific security alerts are received by Azure Security Center.
How should you complete the portion of the template that will provision the required Azure resources? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

```
resources": [
  {
    "type": "                                  /automations",
                Microsoft.Automation
                Microsoft.Logic
                Microsoft.Security
    "apiVersion": "2019-01-01-preview",
    "name": "[parameters('name')]",
    "location": "[parameters('location')]",
    "properties": {
       "description": "[format(variables('description'), '{0}', parameters
['subscriptionId'))]",
       "isEnabled": true,
       "actions": [
          {
             "actionType": "LogicApp",
             "logicAppResourceId": "[resourceId('ITEM2/workflows', parameters
['appName'))]",
             "uri": "[listCallbackURL(resourceId(parameters('subscriptionId')
parameters('resourceGroupName'), '                    /workflows/triggers',
                Microsoft.Automation
                Microsoft.Logic
                Microsoft.Security
parameters('appName'), 'manual'), '2019-05-01').value]"
          }
```

Answer:

```
"resources": [
  {
    "type": "                                  /automations",
                Microsoft.Automation
                Microsoft.Logic
                Microsoft.Security
    "apiVersion": "2019-01-01-preview",
    "name": "[parameters('name')]",
    "location": "[parameters('location')]",
    "properties": {
       "description": "[format(variables('description'), '{0}', parameters
('subscriptionId'))]",
       "isEnabled": true,
       "actions": [
          {
             "actionType": "LogicApp",
             "logicAppResourceId": "[resourceId('ITEM2/workflows', parameters
('appName'))]",
             "uri": "[listCallbackURL(resourceId(parameters('subscriptionId'),
parameters('resourceGroupName'), '                    /workflows/triggers',
                Microsoft.Automation
                Microsoft.Logic
                Microsoft.Security
parameters('appName'), 'manual'), '2019-05-01').value]"
          }
       ],
```

Reference:
https://docs.microsoft.com/en-us/azure/security-center/quickstart-automation-alert

NEW QUESTION: 77
You have the following SQL 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 = Computer, '
```

Answer Area

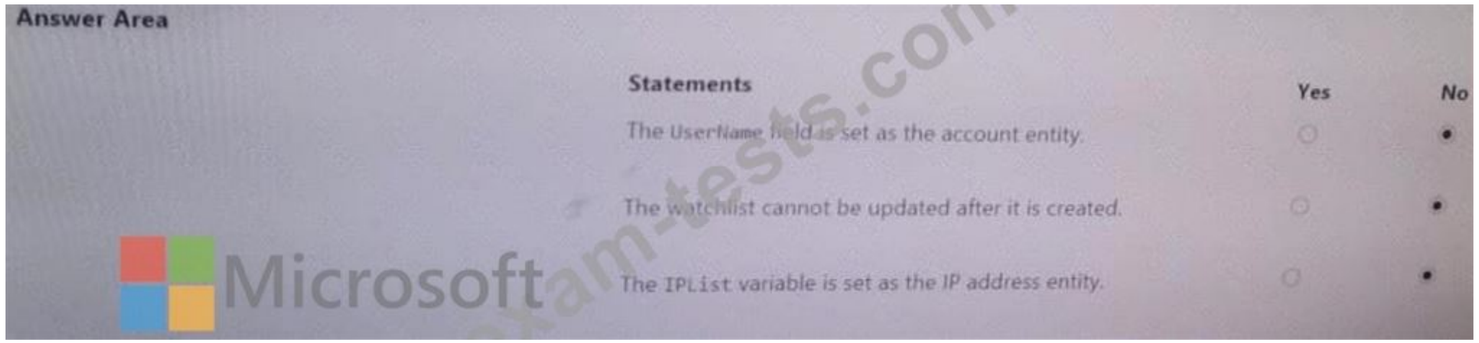
Statements	Yes	No
The UserName field is set as the account entity.		
The watchlist cannot be updated after it is created.		
The IPList variable is set as the IP address entity.		

Answer:

Answer Area

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.		

Explanation



NEW QUESTION: 78

You have an Azure subscription that contains a Microsoft Sentinel workspace named WS1. WS1 has the Azure Activity connector and the Microsoft Entra ID connector configured.

You need to investigate which accounts have the most alerts and any corresponding incident information for each alert. The solution must minimize administrative effort.

What should you do first in WS1?

A. Enable User and Entity Behavior Analytics (UEBA).

B. From Content hub, install Cloud Identity Threat Protection Essentials.

C. From Content hub, install the Microsoft Purview insider risk management solution.

D. Use User and Entity Behavior Analytics (UEBA) to detect anomalies.

Answer: (SHOW ANSWER)

NEW QUESTION: 79

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, '
```

Answer:

Explanation:

* UserName field set as the account entity: Yes
* Watchlist cannot be updated after created: No
* IPList variable set as the IP address entity: Yes

This Kusto Query Language (KQL) snippet is used in Microsoft Sentinel to correlate event data (Sysmon logs) with a watchlist containing known malicious IP addresses. The watchlist is retrieved using the _GetWatchlist() function, and entity mappings are explicitly set for account, host, and IP entities.

Step-by-step analysis:

1. UserName field as the Account entity # YES

At the end of the query, the entity mappings are defined as:

extend timestamp = TimeGenerated, AccountCustomEntity = UserName, HostCustomEntity = Computer In Microsoft Sentinel, when an analytics rule uses this query, the AccountCustomEntity mapping links the UserName field to the account entity .

This enables account-level correlation in incidents and investigation graphs.

Therefore, Ye s , the UserName field is set as the account entity.

2. The watchlist cannot be updated after it is created # NO

This statement is incorrect.

In Sentinel, watchlists are designed to be dynamic and can be updated, edited, or replaced at any time.

Official Microsoft documentation confirms:

"You can edit, update, or replace a watchlist at any time to ensure your detection logic uses current data." Hence, watchlists can be updated , either manually via the portal or programmatically via API/PowerShell.

Therefore, No , the watchlist can be updated after it is created.

3. The IPList variable is set as the IP address entity # YES

The first line of the query defines:

let IPList = _GetWatchlist(' Bad_IPs ');

This loads a list of known malicious IPs from the Bad_IPs watchlist.

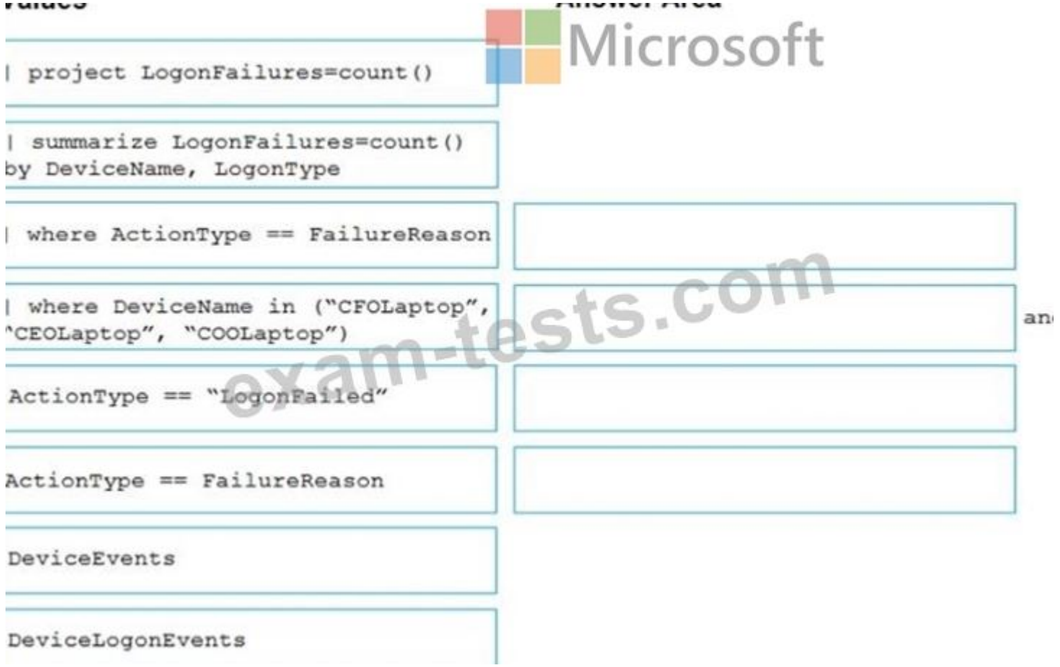
Later in the query:

where SourceIP in (IPList) or DestinationIP in (IPList)

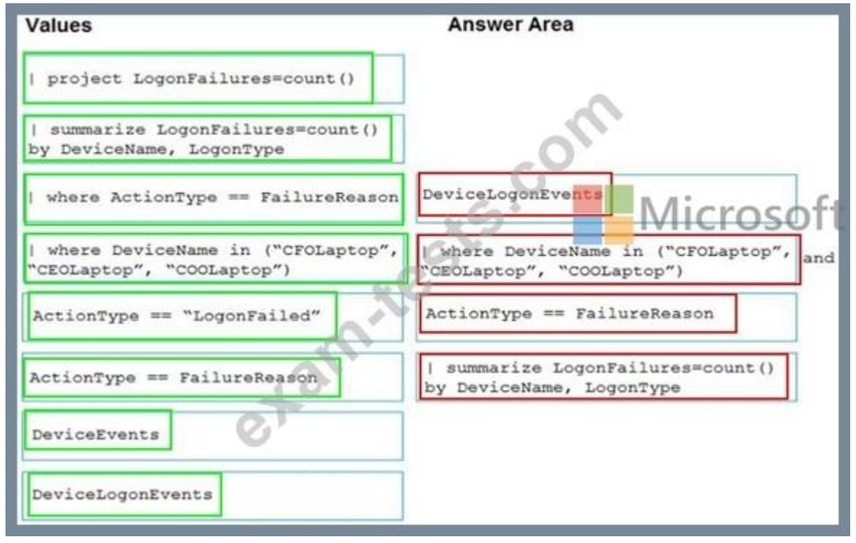
This confirms IPList contains IP address values used for matching with the event's SourceIP or DestinationIP.
In Sentinel analytics rules, this variable represents IP address entities for correlation and visualization.
Therefore, Yes , the IPList variable is set as the IP address entity.

NEW QUESTION: 80
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: B (LEAVE A REPLY)
Microsoft Sentinel provides built-in workbooks for operational insights. To analyze mean time metrics (Mean Time to Acknowledge, Mean Time to Resolve, Mean Time to Mitigate), the correct workbook is Security Operations Efficiency.
According to Microsoft's Sentinel documentation:
"The Security Operations Efficiency workbook helps SOC teams monitor and improve operational performance by showing incident trends and key performance indicators such as mean time to acknowledge (MTTA), mean time to resolve (MTTR), and incident closure rates." Other options:
* Analytics Efficiency - tracks analytic rule performance.
* Event Analyzer - provides event data analysis, not MTTA/MTTR.
* Investigation Insights - focuses on incident investigation details, not SOC metrics.
# Correct workbook: Security Operations Efficiency

NEW QUESTION: 81
You are investigating an incident by using Microsoft 365 Defender.
You need to create an advanced hunting query to count failed sign-in authentications on three devices named CFOLaptop. CEOLaptop, and COOLaptop.
How should you complete the query? To answer, select the appropriate options in the answer area.
NOTE Each correct selection is worth one point



Answer:



NEW QUESTION: 82

Drag and Drop Question

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.

Actions

- Install the Log Analytics agent for Linux on the virtual machines.
- Add Microsoft Sentinel to a workspace.
- Add a Security Events connector to the workspace.
- Add an Microsoft Sentinel workbook.
- Add a Syslog connector to the workspace.

Answer area

Answer:

Actions

- Add a Security Events connector to the workspace.
- Add an Microsoft Sentinel workbook.

Answer area

- Add Microsoft Sentinel to a workspace.
- Add a Syslog connector to the workspace.
- Install the Log Analytics agent for Linux on the virtual machines.

Explanation:

https://docs.microsoft.com/en-us/azure/sentinel/connect-syslog

NEW QUESTION: 83

You have the resources shown in the following table.

Name	Type	Description	Location
Server1	Server	File server that runs Windows Server	On-premises
Server2	Virtual machine	Application server that runs Linux	Amazon Web Services (AWS)
Server3	Virtual machine	Domain controller that runs Windows Server	Azure
Server4	Server	Domain controller that runs Windows Server	On-premises

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

You need to enable Microsoft Defender for Servers on each resource.

Which resources will require the installation of the Azure Arc agent?

A. Server3 only

B. Server1 and Server4 only

C. Server1, Server2, and Server4 only

D. Server1, Server2, Server3, and Server4

Answer: C (LEAVE A REPLY)

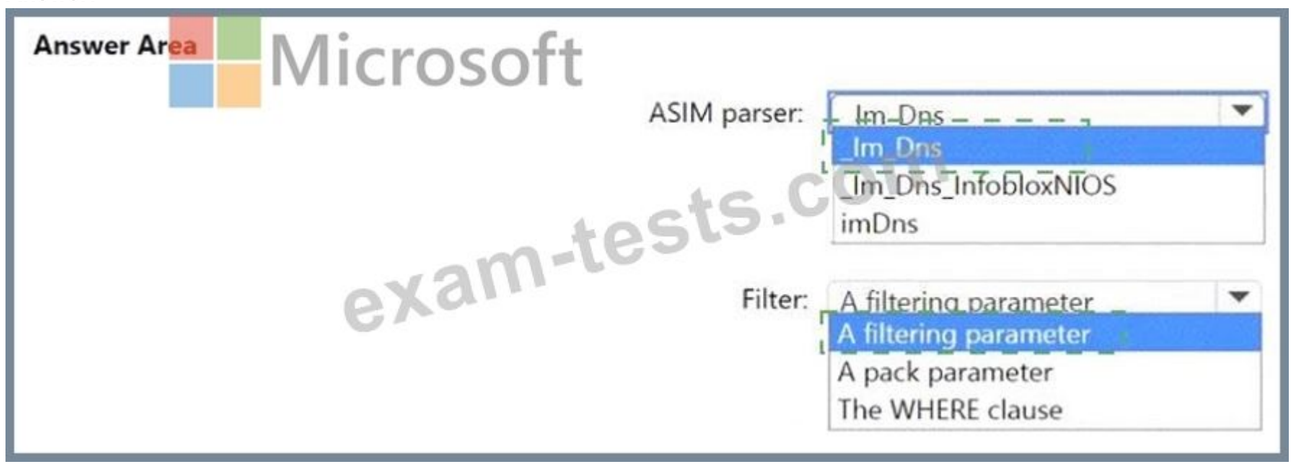
Azure Arc agent is a software that enables you to manage your Windows and Linux machines hosted outside of Azure on your corporate network or other cloud providers. It allows you to project your existing non-Azure and/or on-premises resources into Azure Resource Manager

NEW QUESTION: 84

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

Answer:



Explanation:

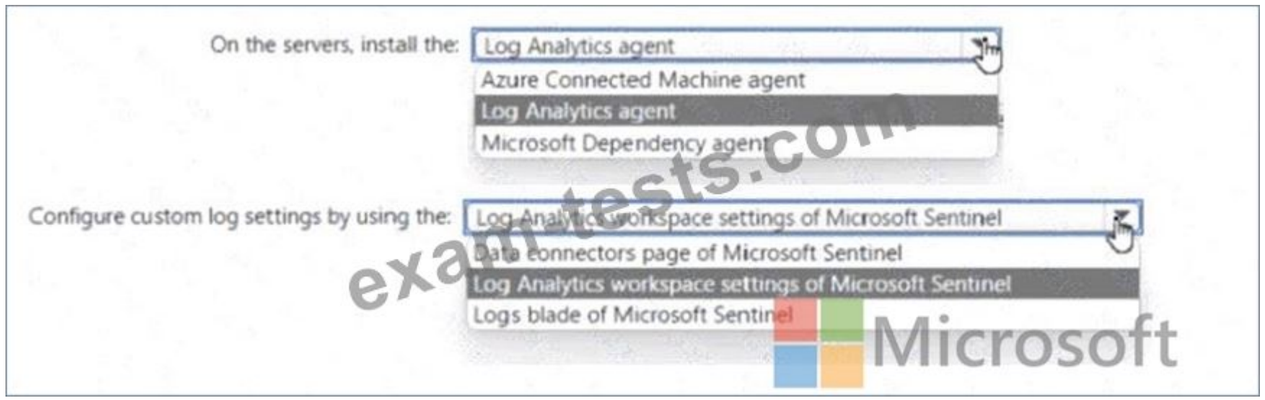
NEW QUESTION: 85

Your on-premises network contains 100 servers that run Windows Server.

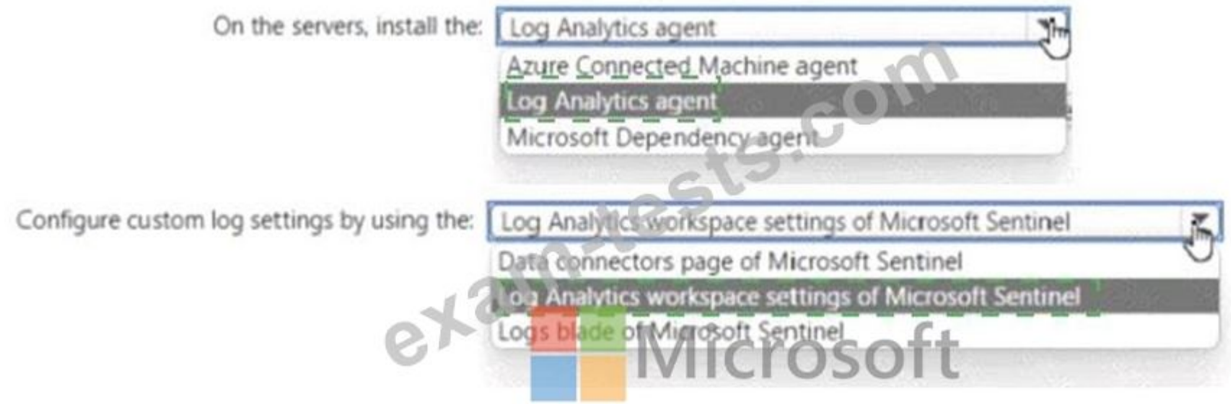
You have an Azure subscription that uses Microsoft Sentinel.

You need to upload custom logs from the on-premises servers to Microsoft Sentinel.

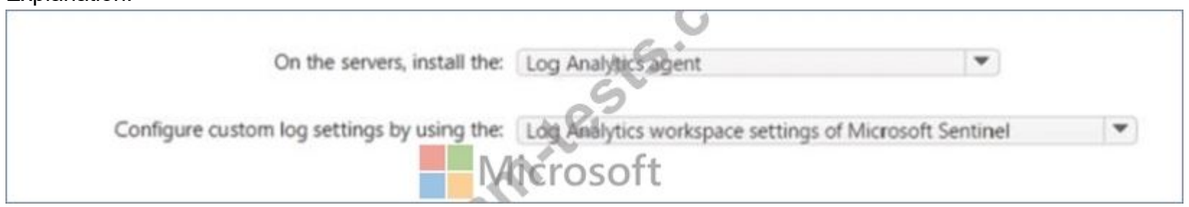
What should you do? To answer, select the appropriate options m the answer area.



Answer:



Explanation:



To ingest custom logs from on-premises servers into Microsoft Sentinel , the logs must first be collected through the L og Analytics workspace that Sentinel is built on. According to Microsoft Sentinel and Azure Monitor documentation, the required steps are:

* Install the Log Analytics agent (MMA/OMS agent) on each on-premises Windows Server that will send logs.
* This agent securely forwards Windows event logs, performance data, and custom log files to the Log Analytics workspace in Azure Monitor.
* Although Azure Monitor Agent (AMA) is the newer option, custom log collection is still supported primarily via the Log Analytics a gent until full parity is achieved.
* The Microsoft Dependency agent is used only for service map and dependency data, not for log ingestion.
* The Azure Connected Machine agent (for Azure Arc) can onboard machines for management but does not directly handle c ustom log configuration for Sentinel.
* Configure custom log ingestion by defining custom log collection rules in the Log Analytics workspace settings .
* In Sentinel, navigate to the underlying workspace # Advanced settings # Data # Custom Logs to define the log format, file path, and collection parameters.
* The custom log configuration is always managed at the workspace level , since Sentinel queries data from the connected workspace's tables.

Other options, like the Data connectors page or Logs blade of Sentin el, are used for connecting integrated services or for querying data, not for defining custom ingestion sources.
Therefore, based on official Microsoft Defender XDR and Sentinel integration guidance, the correct configuration steps are:
On the servers, i nstall the: Log Analytics agent
Configure custom log settings by using the: Log Analytics workspace settings of Microsoft Sentinel

NEW QUESTION: 86
You use Microsoft Sentinel.
You need to receive an alert in near real-time 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: (SHOW ANSWER)

NEW QUESTION: 87
Hotspot Question
You have an Azure subscription that uses Microsoft Defender for Cloud.
You need to use an Azure Resource Manager (ARM) template to create a workflow automation that will trigger a logic app when specific alerts are received by Microsoft Defender for Cloud.
How should you complete the template? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Answer Area

```
"actions": [
  {
    "actionType": "LogicApp",
    "logicAppResourceId": "[resourceId('                    /workflows', parameters('logicAppName'))]",
    "uri": "[listCallbackURL(resourceId(parameters('subscriptionId'), parameters('logicAppResourceGroupName'),
  ...
}
```

- Microsoft.AlertsManagement
- Microsoft.Automation
- Microsoft.Logic
- Microsoft.Security

Answer:

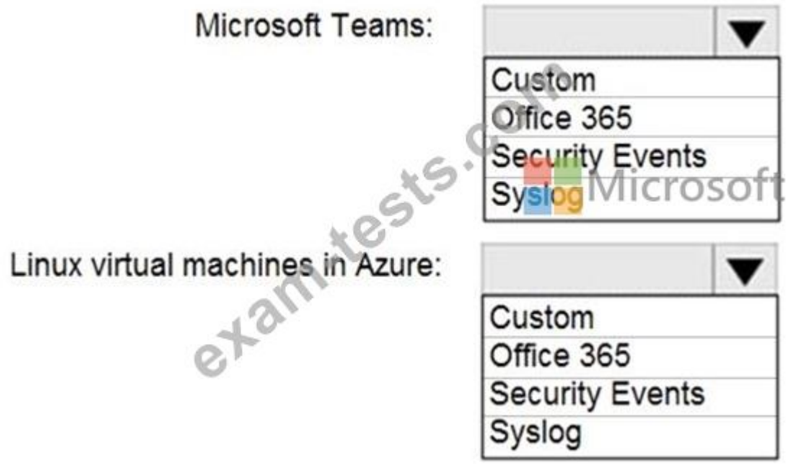
Answer Area

```
"actions": [
  {
    "actionType": "LogicApp",
    "logicAppResourceId": "[resourceId('                    /workflows', parameters('logicAppName'))]",
    "uri": "[listCallbackURL(resourceId(parameters('subscriptionId'), parameters('logicAppResourceGroupName'),
  ...
}
```

- Microsoft.AlertsManagement
- Microsoft.Automation
- Microsoft.Logic
- Microsoft.Security

NEW QUESTION: 88

You deploy Azure Sentinel.
You need to implement connectors in Azure Sentinel to monitor Microsoft Teams and Linux virtual machines in Azure. The solution must minimize administrative effort.
Which data connector type should you use for each workload? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



Answer:

Reference:
https://docs.microsoft.com/en-us/azure/sentinel/connect-office-365
https://docs.microsoft.com/en-us/azure/sentinel/connect-syslog

NEW QUESTION: 89
You have a Microsoft Sentinel workspace.
You enable User and Entity Behavior Analytics (UFBA) by using Audit logs and Signin logs. The following entities are detected in the Azure AD tenant:
* App name: App1

* IP address: 192.168.1.2
* Computer name: Device1
* Used client app: Microsoft Edge
* Email address: user1@company.com
* Sign-in URL: https://www.company.com

Which entities can be investigated by using UEBA?

A. app name, computer name, IP address, email address, and used client app only
B. IP address and email address only
C. used client app and app name only
D. IP address only

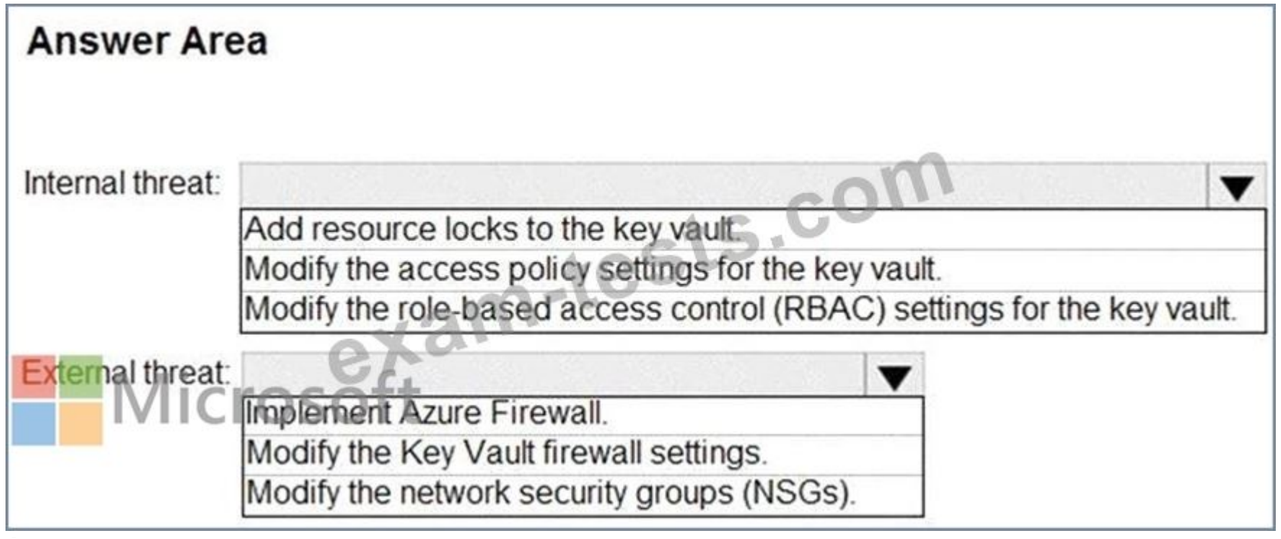
Answer: (SHOW ANSWER)

Microsoft Sentinel UEBA (User and Entity Behavior Analytics) focuses on users and hosts (devices) and enriches data with contextual information.
When enabling UEBA with Audit logs and Signin logs, the only entities supported for investigation are:
* User accounts (email addresses)
* Hosts or devices (including IP addresses)

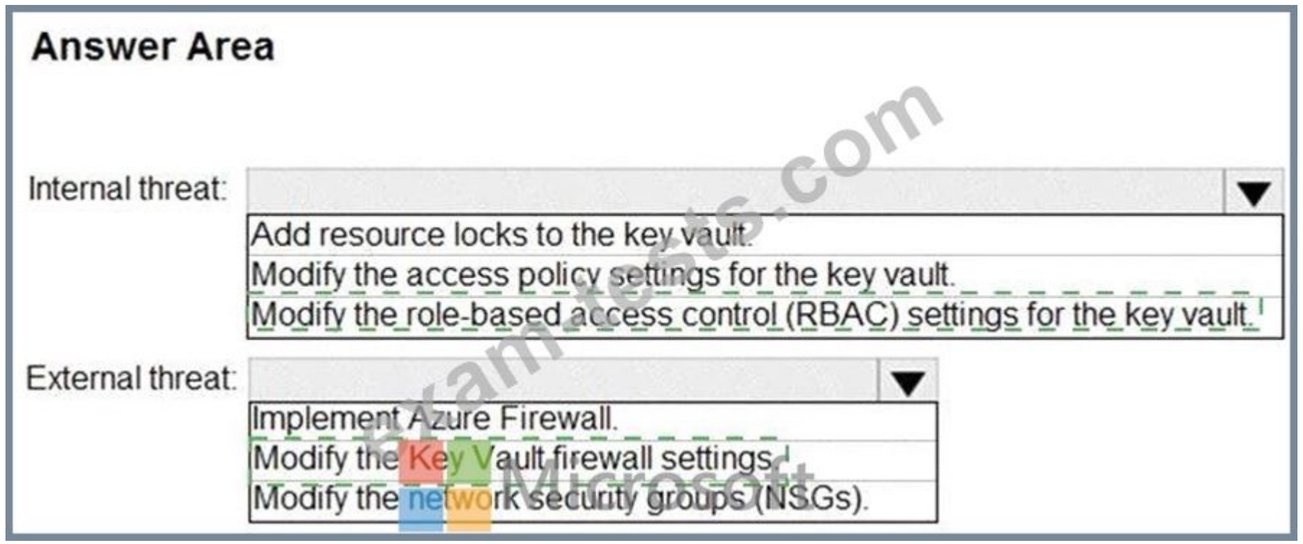
Other values like App name, Used client app, and Sign-in URL are attributes in log data but not tracked entities in UEBA investigations.

NEW QUESTION: 90

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.



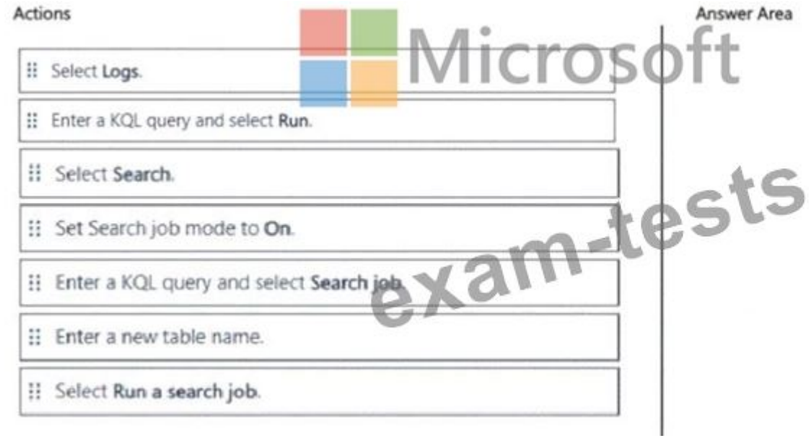
Answer:



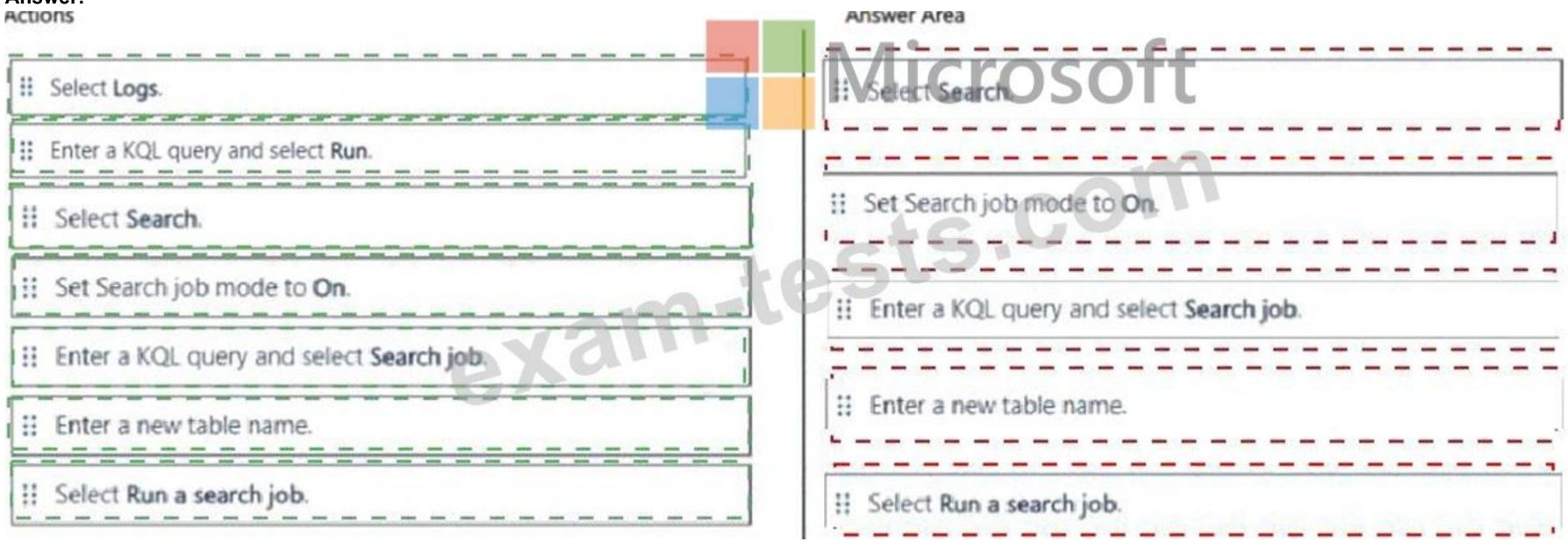
Explanation:

Reference:
https://docs.microsoft.com/en-us/azure/key-vault/general/secure-your-key-vault

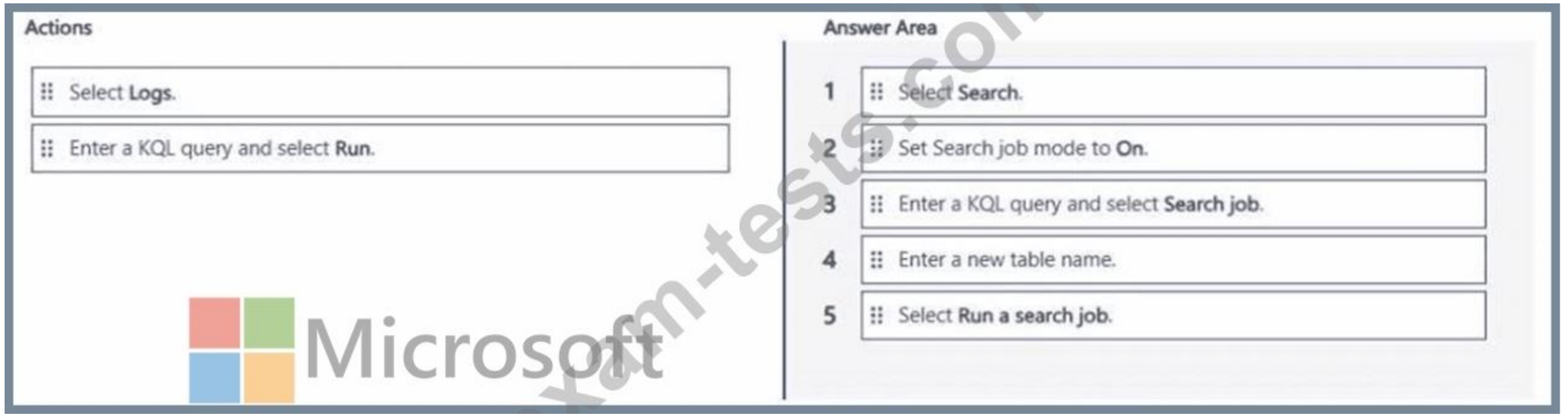
NEW QUESTION: 91
You have a Microsoft Sentinel workspace named Workspace1.
You need to run a KQL query as a search job.
Which five actions should you perform in Workspace 1 in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.



Answer:



Explanation:



NEW QUESTION: 92

You have a Microsoft Sentinel workspace that contains a custom workbook.

You need to query for a summary of security events. The solution must meet the following requirements:

* Identify the number of security events ingested during the past week.
* Display the count of events by day in a chart.

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:

Explanation:

To summarize security events over the last week and chart them by day , use KQL time binning on the event timestamp. In Sentinel/Log Analytics, bin() groups records into fixed time buckets on a datetime column- here, TimeGenerated . Pair that with a time filter for the past 7 days and render as a timechart. The key pattern is:

SecurityEvent

| where TimeGenerated > = ago(7d)

| summarize Count = count() by bin(TimeGenerated, 1d)

| render timechart

* bin is the correct aggregator for time-based bucketing.

* TimeGenerated is the standard timestamp column used across Sentinel tables for ingestion time.

* Using a 1-day bin shows the daily counts; the where TimeGenerated > = ago(7d) limits results to the past week .

* render timechart visualizes the grouped counts over time.

In the answer area shown, you select bin and TimeGenerated ; (the full query would also include the where line and a 1d bin size to meet the "by day" requirement).

NEW QUESTION: 93

Hotspot Question

You need to use an Azure Resource Manager template to create a workflow automation that will trigger an automatic remediation when specific security alerts are received by Azure Security Center.

How should you complete the portion of the template that will provision the required Azure resources? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

```
"resources": [
   {
     "type": "                                  /automations",
     "apiVersion": "2019-01-01-preview",
     "name": "[parameters('name')]",
     "location": "[parameters('location')]",
     "properties": {
        "description": "[format(variables('description'), '{0}', parameters
('subscriptionId'))]",
        "isEnabled": true,
        "actions": [
           {
              "actionType": "LogicApp",
              "logicAppResourceId": "[resourceId('ITEM2/workflows', parameters
('appName'))]",
              "uri": "[listCallbackURL(resourceId(parameters('subscriptionId'),
parameters('resourceGroupName'), '                                  /workflows/triggers',
parameters('appName'), 'manual'), '2019-05-01').value]"
           }
     ],
```

- Microsoft.Automation
- Microsoft.Logic
- Microsoft.Security

- Microsoft.Automation
- Microsoft.Logic
- Microsoft.Security

Answer:

Answer Area

```
"resources": [
  {
    "type": "[ Microsoft.Automation | Microsoft.Logic | Microsoft.Security ]/automations",
    "apiVersion": "2019-01-01-preview",
    "name": "[parameters('name')]",
    "location": "[parameters('location')]",
    "properties": {
      "description": "[format(variables('description'), '{0}', parameters
('subscriptionId'))]",
      "isEnabled": true,
      "actions": [
        {
          "actionType": "LogicApp",
          "logicAppResourceId": "[resourceId('ITEM2/workflows', parameters
('appName'))]",
          "uri": "[listCallbackURL(resourceId(parameters('subscriptionId'),
parameters('resourceGroupName'), '[ Microsoft.Automation | Microsoft.Logic | Microsoft.Security ]/workflows/triggers',
parameters('appName'), 'manual'), '2019-05-01').value]"
        }
      ],
```


Explanation:
https://docs.microsoft.com/en-us/azure/security-center/quickstart-automation-alert
https://raw.githubusercontent.com/Azure/azure-quickstart-templates/master/quickstarts/microsoft.security/securitycenter-create-automation-for- alertnamecontains/azuredeploy.json

NEW QUESTION: 94
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You are configuring Microsoft Defender for Identity integration with Active Directory.
From the Microsoft Defender for identity portal, you need to configure several accounts for attackers to exploit.
Solution: From Entity tags, you add the accounts as Honeytoken accounts.
Does this meet the goal?
A. Yes
B. No
Answer: A (LEAVE A REPLY)
Reference:
https://docs.microsoft.com/en-us/defender-for-identity/manage-sensitive-honeytoken-accounts

NEW QUESTION: 95
You have a Microsoft 365 E5 subscription that uses Microsoft Defender and an Azure subscription that uses Azure Sentinel.
You need to identify all the devices that contain files in emails sent by a known malicious email sender. The query will be based on the match of the SHA256 hash.

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

NOTE: Each correct selection is worth one point.

```
EmailAttachmentInfo
| where SenderFromAddress =~ "MaliciousSender@example.com"
where isnotempty [ ▼ ]
```

- (DeviceId)
- (RecipientEmailAddress)
- (SenderFromAddress)
- (SHA256)

```
| join (
DeviceFileEvents
| project FileName, SHA256
) on [ ▼ ]
```

- (DeviceId)
- (RecipientEmailAddress)
- (SenderFromAddress)
- (SHA256)

```
| project Timestamp, FileName, SHA256, DeviceName, DeviceId
NetworkMessageId, SenderFromAddress, RecipientEmailAddress
```

Answer:

```
EmailAttachmentInfo
| where SenderFromAddress =~ "MaliciousSender@example.com"
where isnotempty [ ▼ ]
```

- (DeviceId)
- (RecipientEmailAddress)
- (SenderFromAddress)
- (SHA256)

```
| join (
DeviceFileEvents
| project FileName, SHA256
) on [ ▼ ]
```

- (DeviceId)
- (RecipientEmailAddress)
- (SenderFromAddress)
- (SHA256)

```
| project Timestamp, FileName, SHA256, DeviceName, DeviceId,
NetworkMessageId, SenderFromAddress, RecipientEmailAddress
```

Explanation:

```
EmailAttachmentInfo
| where SenderFromAddress =~ "MaliciousSender@example.com"
where isnotempty [(DeviceId) / (RecipientEmailAddress) / (SenderFromAddress) / (SHA256)]
| join (
DeviceFileEvents
| project FileName, SHA256
) on [(DeviceId) / (RecipientEmailAddress) / (SenderFromAddress) / (SHA256)]
| project Timestamp, FileName, SHA256, DeviceName, DeviceId
NetworkMessageId, SenderFromAddress, RecipientEmailAddress
```

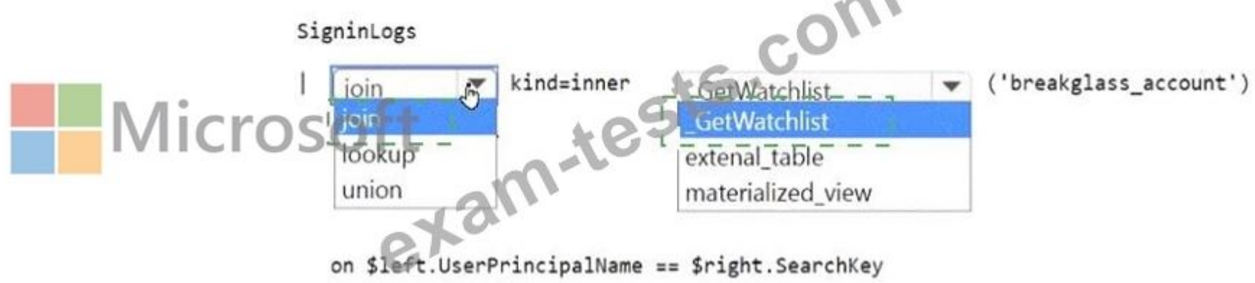
Reference:
https://docs.microsoft.com/en-us/microsoft-365/security/defender/advanced-hunting-query-emails-devices?view=o365-worldwide

NEW QUESTION: 96

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:

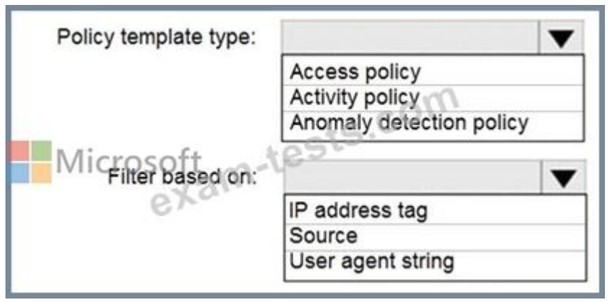
Answer Area



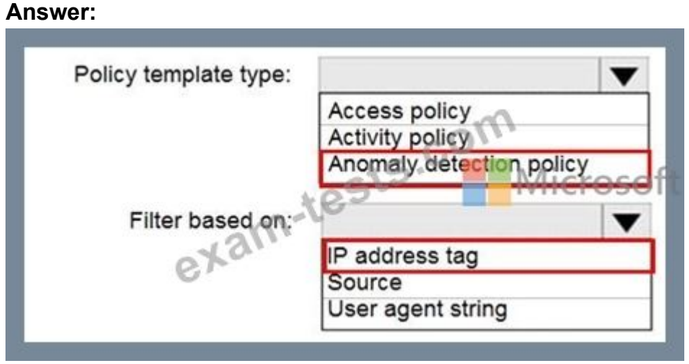
Explanation:

For a near-real-time (NRT) analytics rule that detects sign-ins by a designated break-glass account, the most direct and performant pattern is to filter SigninLogs by joining to a Microsoft Sentinel watchlist that contains the protected account(s). Sentinel exposes watchlists to KQL through the helper function
_GetWatchlist(' < watchlist-name > ') , which returns a table with standard columns (including SearchKey) plus any custom columns you imported. Using join kind=inner ensures the result set includes only those SigninLogs rows whose UserPrincipalName matches an entry in the watchlist-ideal for alerting on a high- value account without post-filtering.
The completed query is:
SigninLogs | join kind=inner (_GetWatchlist(' breakglass_account ')) on $left.UserPrincipalName == $right.
SearchKey
This approach satisfies the requirement to implement an NRT rule for the break-glass account because:
* NRT rules support KQL with joins and watchlists and are optimized for rapid evaluation over fresh data.
* Using a watchlist lets SecOps adjust monitored accounts without editing the rule-minimizing administrative effort and aligning with least-privilege operations (no extra permissions beyond watchlist management).
* The inner join pattern reduces noise by returning only matched events, which are then turned into alerts
/incidents by the NRT rule.
Thus, select join and GetWatchlist , and join UserPrincipalName to the watchlist's SearchKey .

NEW QUESTION: 97
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.



Answer:



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

NEW QUESTION: 98
You have a Microsoft 365 E5 subscription that uses Microsoft Defender 365.
You need to ensure that you can investigate threats by using data in the unified audit log of Microsoft Defender for Cloud Apps.
What should you configure first?
A. the User enrichment settings
B. the Azure connector
C. the Office 365 connector
D. the Automatic log upload settings
Answer: (SHOW ANSWER)
https://learn.microsoft.com/en-us/defender-cloud-apps/connect-office-365

NEW QUESTION: 99
Hotspot Question
You have an Azure subscription that has Microsoft Defender for Cloud 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 Defender for Cloud.
You need to test LA1 in Defender for Cloud.
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 a Defender for Cloud Recommendation is created or triggered
- When a Defender for Cloud Alert is created or triggered
- When a response to a Defender for Cloud alert is triggered

Trigger the execution of LA1 from:

- Recommendations
- Security alerts
- Regulatory compliance standards

Answer:

Answer Area

Set the LA1 trigger to:

- When a Defender for Cloud Recommendation is created or triggered
- When a Defender for Cloud Alert is created or triggered
- When a response to a Defender for Cloud alert is triggered

Trigger the execution of LA1 from:

- Recommendations
- Security alerts
- Regulatory compliance standards

NEW QUESTION: 100

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 Common Event Format (CEF) connector

C. a Log Analytics Data Collector API

D. a SysJog connector

Answer: (SHOW ANSWER)

NEW QUESTION: 101

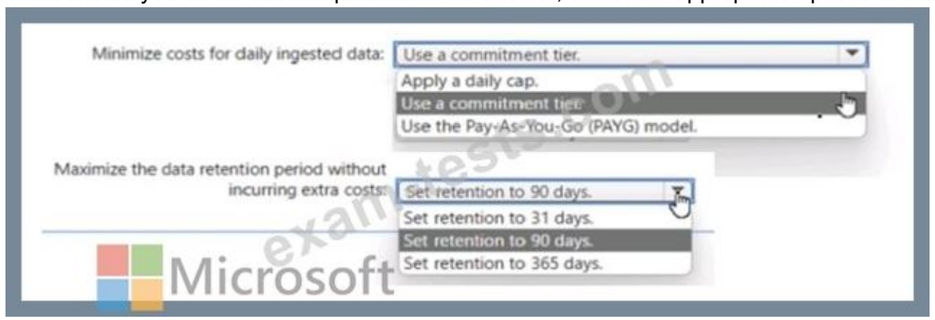
You have an Azure subscription.

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 are a. NOTE Each correct selection is worth one point.



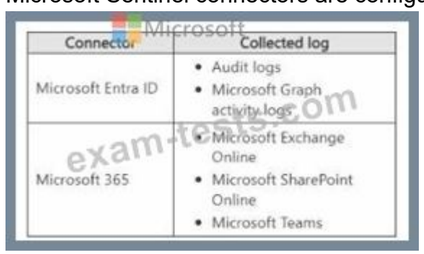
Answer:

NEW QUESTION: 102

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

You have a Microsoft Sentinel workspace.

Microsoft Sentinel connectors are configured as shown in the following table.



Connector	Collected log
Microsoft Entra ID	• Audit logs • Microsoft Graph activity logs
Microsoft 365	• Microsoft Exchange Online • Microsoft SharePoint Online • Microsoft Teams

You use Microsoft Sentinel to investigate suspicious Microsoft Graph API activity related to Conditional Access policies. You need to search for the following activities:

* Downloads of the Conditional Access policies by using PowerShell

* Updates to the Conditional Access policies by using the Microsoft Entra admin center Which tables should you query for each activity? lo answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

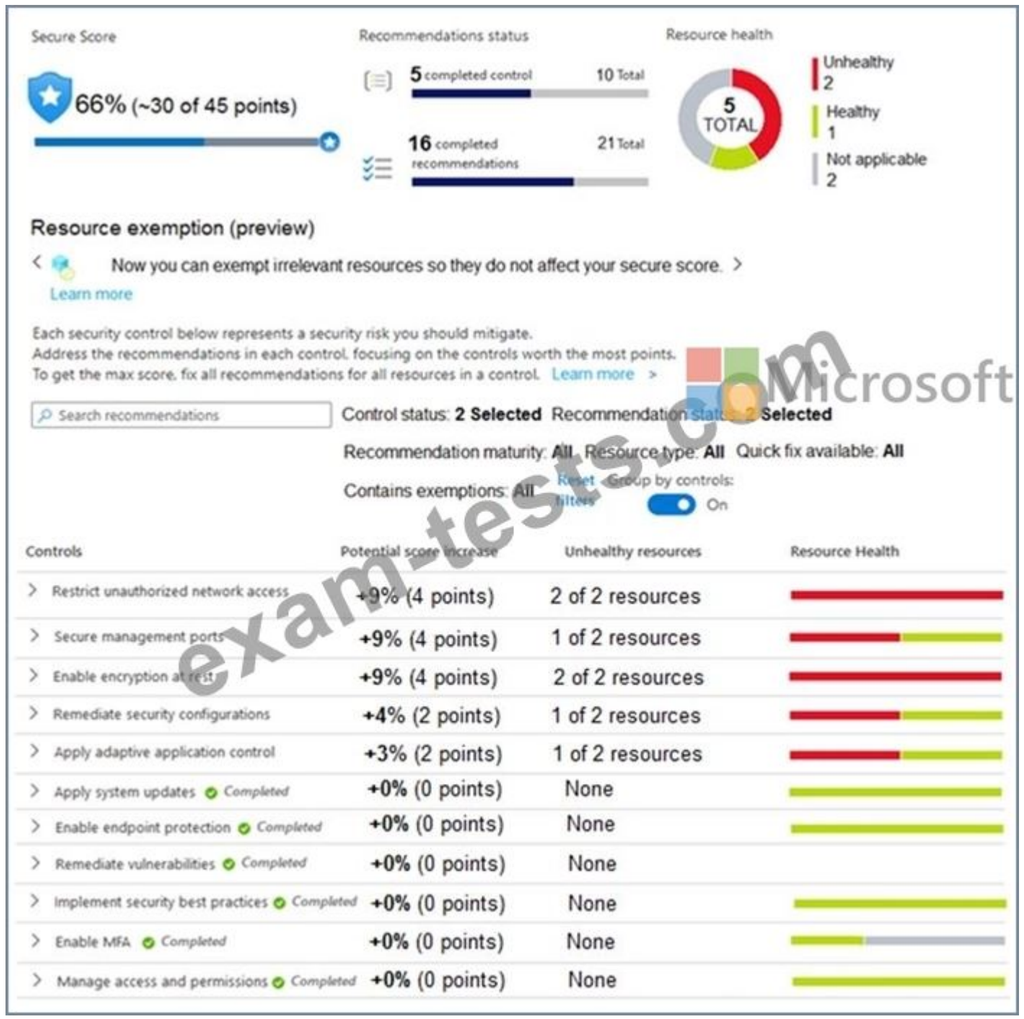
Answer:

Explanation:

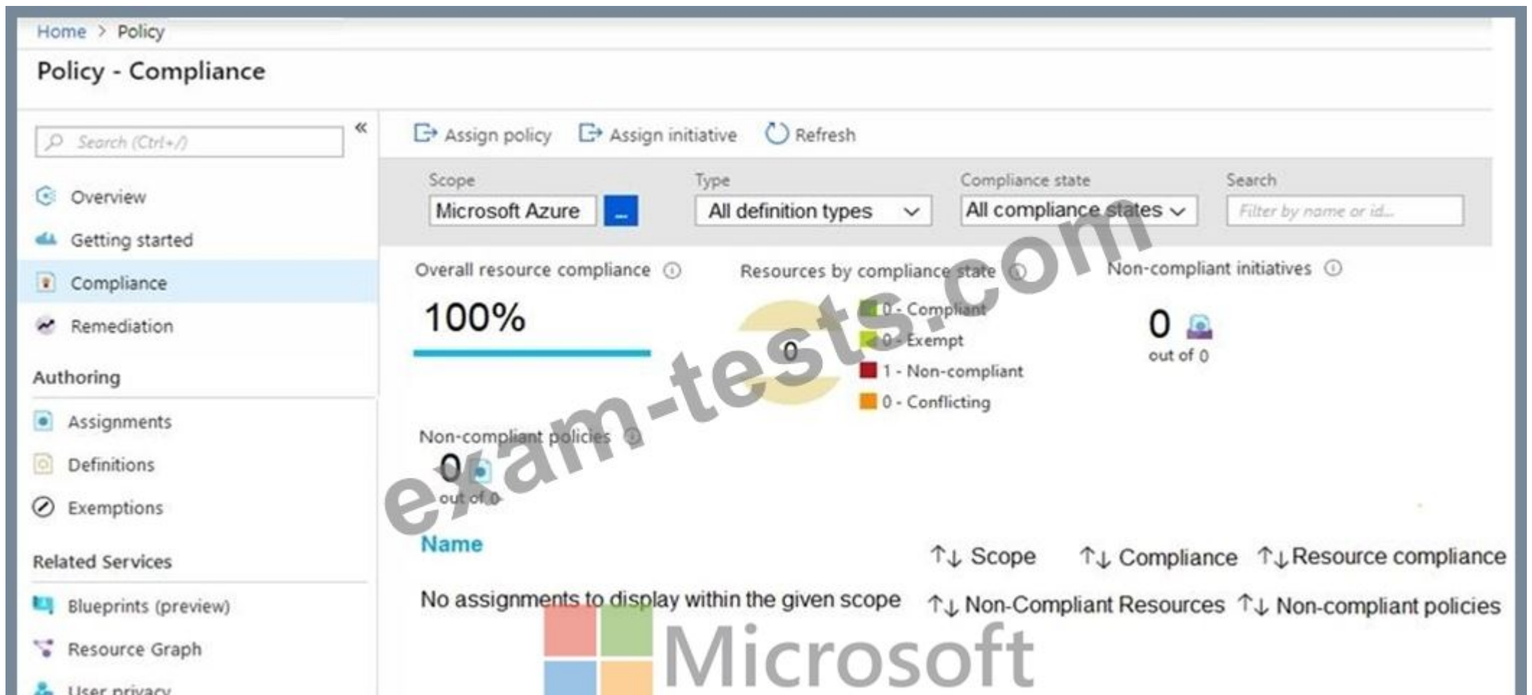
NEW QUESTION: 103

You manage the security posture of an Azure subscription that contains two virtual machines name vm1 and vm2.

The secure score in Azure Security Center is shown in the Security Center exhibit. (Click the Security Center tab.)



Azure Policy assignments are configured as shown in the Policies exhibit. (Click the Policies tab.)



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
Both virtual machines have inbound rules that allow access from either Any or Internet ranges.	○	○
Both virtual machines have management ports exposed directly to the internet.	○	○
If you enable just-in-time network access controls on all virtual machines, you will increase the secure score by four point.	○	○

Answer:

Answer Area

Statements	Yes	No
Both virtual machines have inbound rules that allow access from either Any or Internet ranges.	○	○
Both virtual machines have management ports exposed directly to the internet.	○	○
If you enable just-in-time network access controls on all virtual machines, you will increase the secure score by four point.	○	○

Explanation:

Answer Area

Statements	Yes	No
Both virtual machines have inbound rules that allow access from either Any or Internet ranges.	○	○
Both virtual machines have management ports exposed directly to the internet.	○	○
If you enable just-in-time network access controls on all virtual machines, you will increase the secure score by four point.	○	○

Reference:

https://techcommunity.microsoft.com/t5/azure-security-center/security-control-restrict-unauthorized-network-acc

https://techcommunity.microsoft.com/t5/azure-security-center/security-control-secure-management-ports/ba-p/15

NEW QUESTION: 104

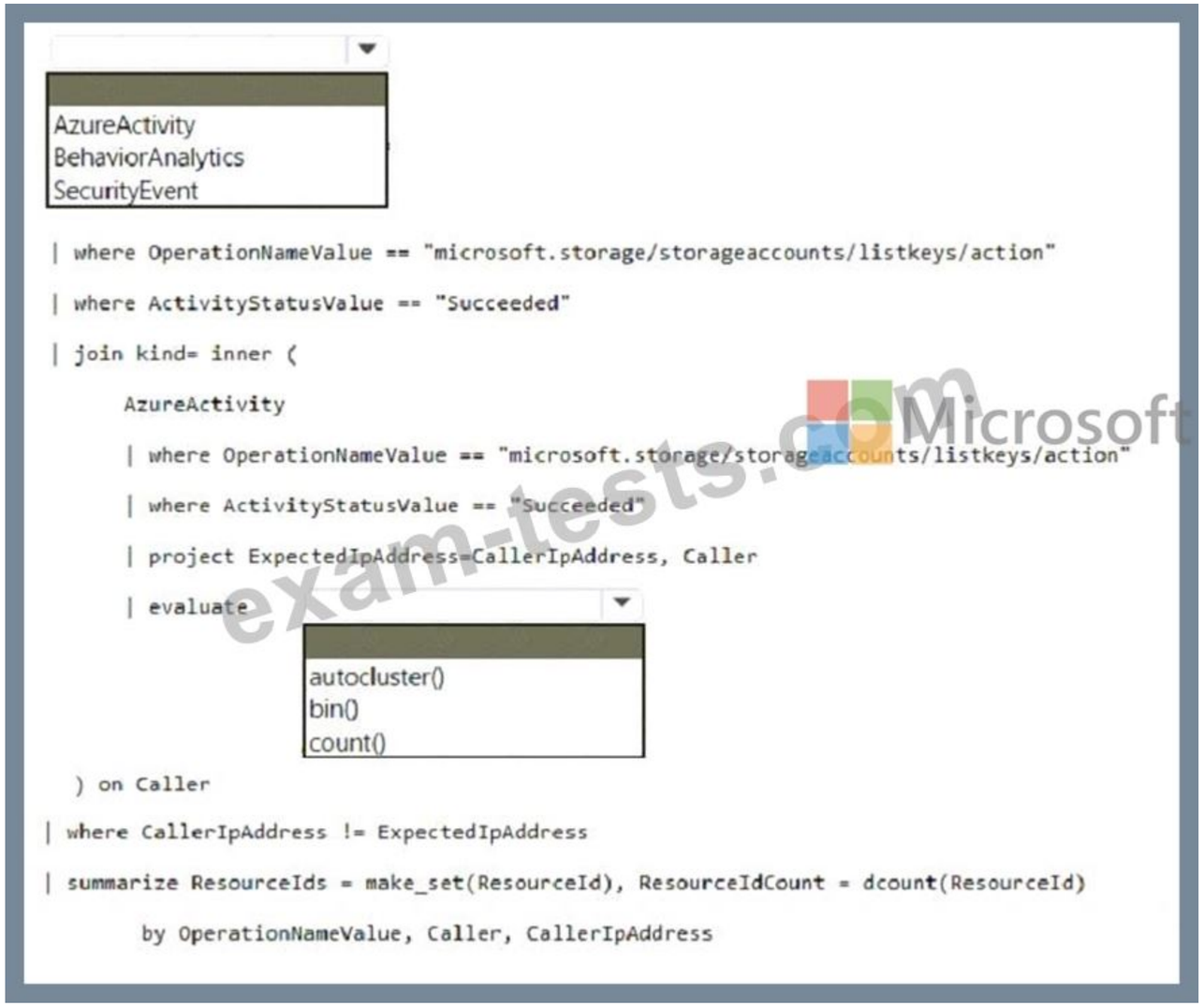
You have a Microsoft Sentinel workspace named sws1.

You need to create a hunting query to identify users that list storage keys of multiple Azure Storage accounts.

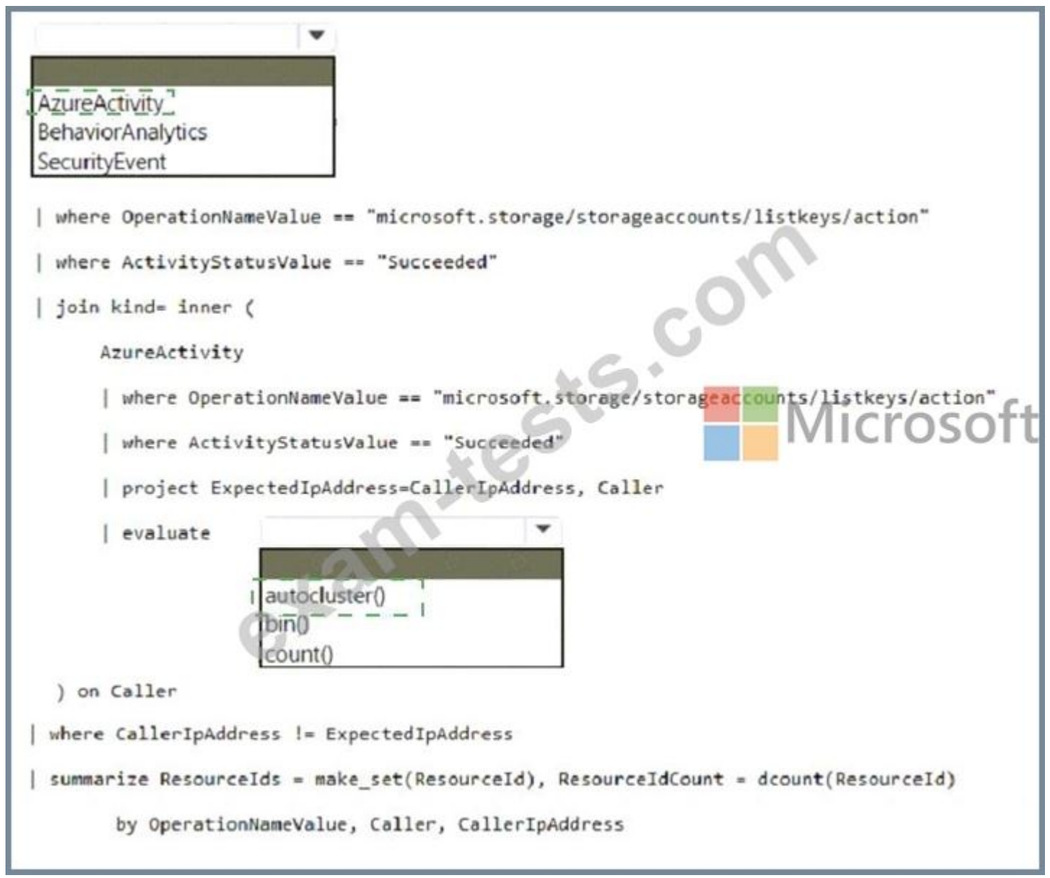
The solution must exclude users that list storage keys for a single storage account.

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

NOTE: Each correct selection is worth one point.


AzureActivity
BehaviorAnalytics
SecurityEvent
| where OperationNameValue == "microsoft.storage/storageaccounts/listkeys/action"
| where ActivityStatusValue == "Succeeded"
| join kind= inner (
AzureActivity
| where OperationNameValue == "microsoft.storage/storageaccounts/listkeys/action"
| where ActivityStatusValue == "Succeeded"
| project ExpectedIpAddress=CallerIpAddress, Caller
| evaluate
autocluster()
bin()
count()
) on Caller
| where CallerIpAddress != ExpectedIpAddress
| summarize ResourceIds = make_set(ResourceId), ResourceIdCount = dcount(ResourceId)
by OperationNameValue, Caller, CallerIpAddress

Answer:



Explanation

Box 1: AzureActivity

The AzureActivity table includes data from many services, including Microsoft Sentinel. To filter in only data from Microsoft Sentinel, start your query with the following code:

Box 2: autocluster()

Example: description: |

'Listing of storage keys is an interesting operation in Azure which might expose additional secrets and PII to callers as well as granting access to VMs. While there are many benign operations of this type, it would be interesting to see if the account performing this activity or the source IP address from which it is being done is anomalous.

The query below generates known clusters of ip address per caller, notice that users which only had single operations do not appear in this list as we cannot learn from it their normal activity (only based on a single event). The activities for listing storage account keys is correlated with this learned clusters of expected activities and activity which is not expected is returned.' AzureActivity

| where OperationNameValue =~ "microsoft.storage/storageaccounts/listkeys/action"

| where ActivityStatusValue == "Succeeded"

| join kind= inner (

AzureActivity

| where OperationNameValue =~ "microsoft.storage/storageaccounts/listkeys/action"

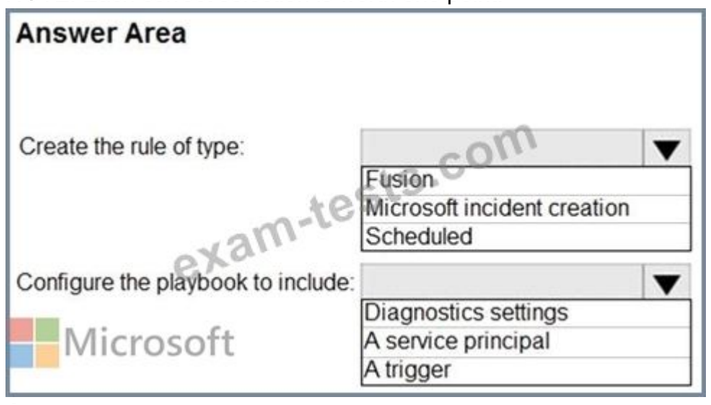
| where ActivityStatusValue == "Succeeded"

| project ExpectedIpAddress=CallerIpAddress, Caller

| evaluate autocluster()
) on Caller
| where CallerIpAddress != ExpectedIpAddress
| summarize StartTime = min(TimeGenerated), EndTime = max(TimeGenerated), ResourceIds = make_set(ResourceId), ResourceIdCount = dcount(ResourceId) by OperationNameValue, Caller, CallerIpAddress
| extend timestamp = StartTime, AccountCustomEntity = Caller, IPCustomEntity = CallerIpAddress Reference:
https://github.com/Azure/Azure-Sentinel/blob/master/Hunting%20Queries/AzureActivity/Anomalous_Listing_O

NEW QUESTION: 105
You need to receive a security alert when a user attempts to sign in from a location that was never used by the other users in your organization to sign in.
Which anomaly detection policy should you use?
A. Impossible travel
B. Activity from anonymous IP addresses
C. Activity from infrequent country
D. Malware detection
Answer: C (LEAVE A REPLY)
Reference:
https://docs.microsoft.com/en-us/cloud-app-security/anomaly-detection-policy

NEW QUESTION: 106
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:

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: 107

You have a Microsoft Sentinel workspace named sws1.

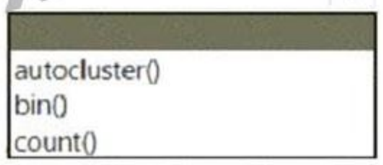
You need to create a hunting query to identify users that list storage keys of multiple Azure Storage accounts.

The solution must exclude users that list storage keys for a single storage account.

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

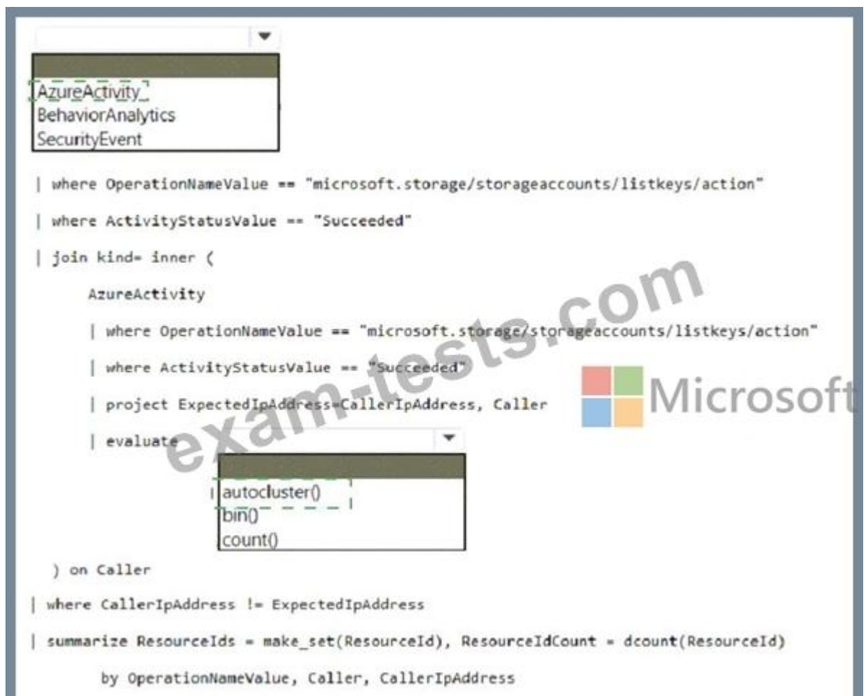
NOTE: Each correct selection is worth one point.


```
| where OperationNameValue == "microsoft.storage/storageaccounts/listkeys/action"
| where ActivityStatusValue == "Succeeded"
| join kind= inner (
      AzureActivity
      | where OperationNameValue == "microsoft.storage/storageaccounts/listkeys/action"
      | where ActivityStatusValue == "Succeeded"
      | project ExpectedIpAddress=CallerIpAddress, Caller
      | evaluate
```




```
  ) on Caller
| where CallerIpAddress != ExpectedIpAddress
| summarize ResourceIds = make_set(ResourceId), ResourceIdCount = dcount(ResourceId)
        by OperationNameValue, Caller, CallerIpAddress
```


Answer:



Explanation:

Box 1: AzureActivity

The AzureActivity table includes data from many services, including Microsoft Sentinel. To filter in only data from Microsoft Sentinel, start your query with the following code:

Box 2: autocluster()

Example: description: |

'Listing of storage keys is an interesting operation in Azure which might expose additional secrets and PII to callers as well as granting access to VMs. While there are many benign operations of this type, it would be interesting to see if the account performing this activity or the source IP address from which it is being done is anomalous.

The query below generates known clusters of ip address per caller, notice that users which only had single operations do not appear in this list as we cannot learn from it their normal activity (only based on a single event). The activities for listing storage account keys is correlated with this learned clusters of expected activities and activity which is not expected is returned.' AzureActivity

```
| where OperationNameValue =~ "microsoft.storage/storageaccounts/listkeys/action"
| where ActivityStatusValue == "Succeeded"
| join kind= inner (
AzureActivity
| where OperationNameValue =~ "microsoft.storage/storageaccounts/listkeys/action"
| where ActivityStatusValue == "Succeeded"
| project ExpectedIpAddress=CallerIpAddress, Caller
| evaluate autocluster()
) on Caller
| where CallerIpAddress != ExpectedIpAddress
| summarize StartTime = min(TimeGenerated), EndTime = max(TimeGenerated), ResourceIds = make_set (ResourceId), ResourceIdCount = dcount(ResourceId) by OperationNameValue, Caller, CallerIpAddress
```

| extend timestamp = StartTime, AccountCustomEntity = Caller, IPCustomEntity = CallerIpAddress Reference: https://github.com/Azure/Azure-Sentinel/blob/master/Hunting%20Queries/AzureActivity/Anomalous_Listing_Of_Storage_Keys.yaml

NEW QUESTION: 108
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.	○	○

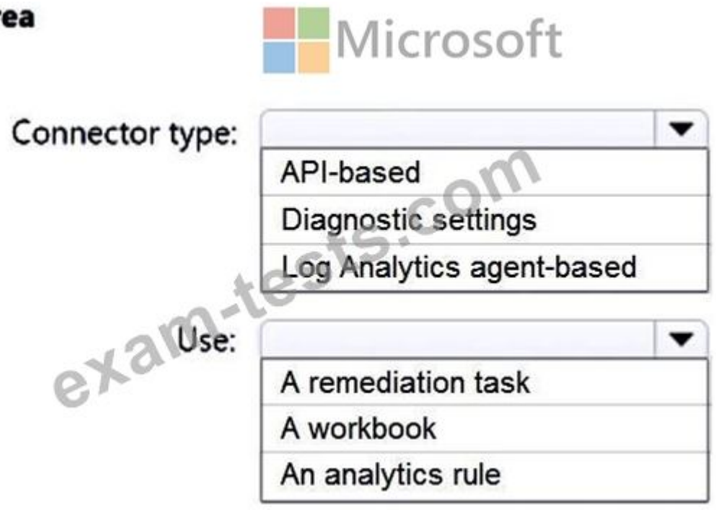
Answer:

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.	○	○

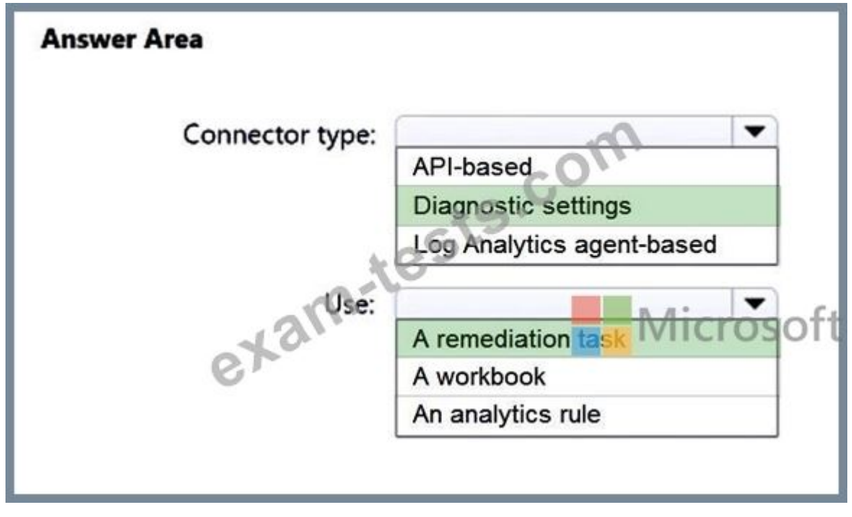
Explanation:

NEW QUESTION: 109
Hotspot Question
You have four Azure subscriptions. One of the subscriptions contains a Microsoft Sentinel workspace.
You need to deploy Microsoft Sentinel data connectors to collect data from the subscriptions by using Azure Policy. The solution must ensure that the policy will apply to new and existing resources in the subscriptions.
Which type of connectors should you provision, and what should you use to ensure that all the resources are monitored? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Answer Area



Answer:



NEW QUESTION: 110
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: (SHOW ANSWER)
Reference:
https://docs.microsoft.com/en-us/azure/azure-monitor/visualize/workbooks-chart-visualizations

NEW QUESTION: 111
You have a Microsoft 365 subscription.
You have 1,000 Windows devices that have a third-party antivirus product installed and Microsoft Defender Antivirus in passive mode. You need to ensure that the devices are protected from malicious artifacts that were undetected by the third-party antivirus product Solution: You enable automated investigation and response (AIR).
Does this meet the goal?
A. Yes
B. No
Answer: B (LEAVE A REPLY)
Automated Investigation and Response (AIR) automates investigation and remediation actions for alerts that Defender already detects: it triages alerts, runs investigation playbooks, and can execute remediation (quarantine files, terminate processes, remove persistence) based on the investigation outcome. AIR is powerful for reducing analyst load and quickly remediating detected threats. However, AIR only runs in response to detections/alerts it receives-if the third-party AV completely misses an artifact and no EDR
/behavioral detection generates an alert, AIR will not be triggered. In contrast, EDR in block mode is specifically built to catch post-breach detections that the primary AV missed and to remediate them.
Therefore, enabling AIR alone does not guarantee protection from artifacts missed by the third-party antivirus; AIR helps remediate once a detection exists but does not itself create the missed detection coverage that EDR in block mode provides.

NEW QUESTION: 112

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

SW1

CEF1

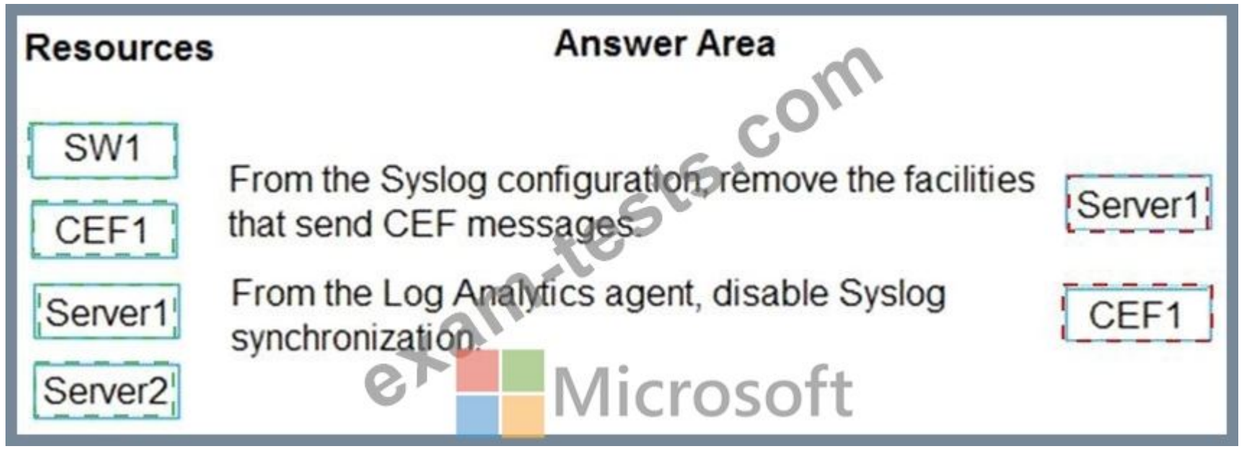
Server1

Server2

Answer Area

From the Syslog configuration, remove the facilities that send CEF messages. [ ]

From the Log Analytics agent, disable Syslog synchronization. [ ]

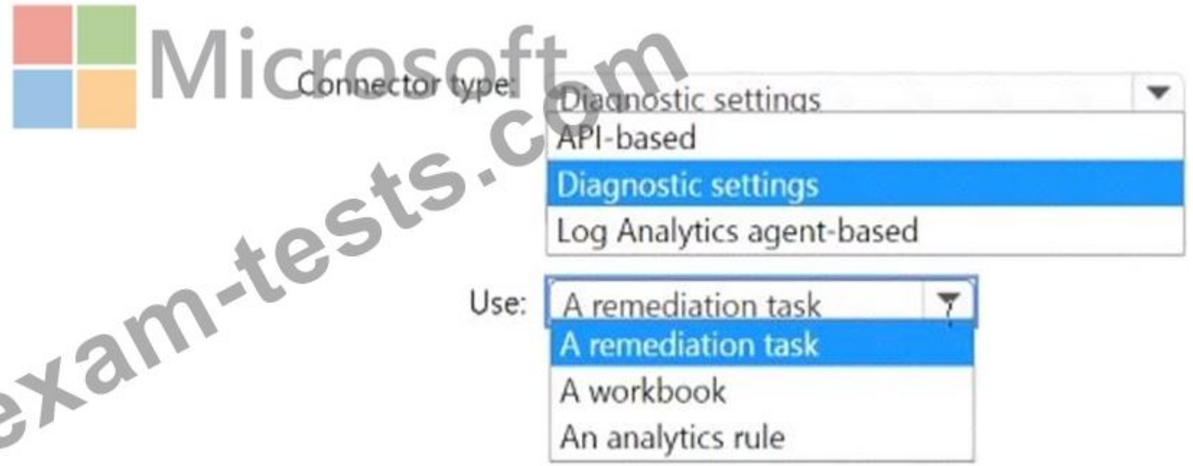


Explanation:

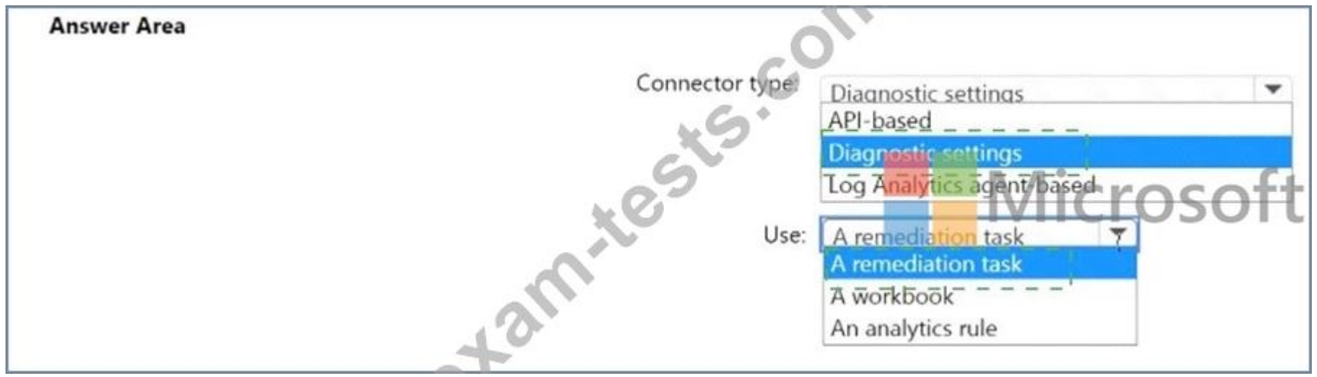
Reference:
https://docs.microsoft.com/en-us/azure/sentinel/connect-log-forwarder?tabs=rsyslog

NEW QUESTION: 113
You have four Azure subscriptions. One of the subscriptions contains a Microsoft Sentinel workspace.
You need to deploy Microsoft Sentinel data connectors to collect data from the subscriptions by using Azure Policy. The solution must ensure that the policy will apply to new and existing resources in the subscriptions.
Which type of connectors should you provision, and what should you use to ensure that all the resources are monitored? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Answer Area



Answer:

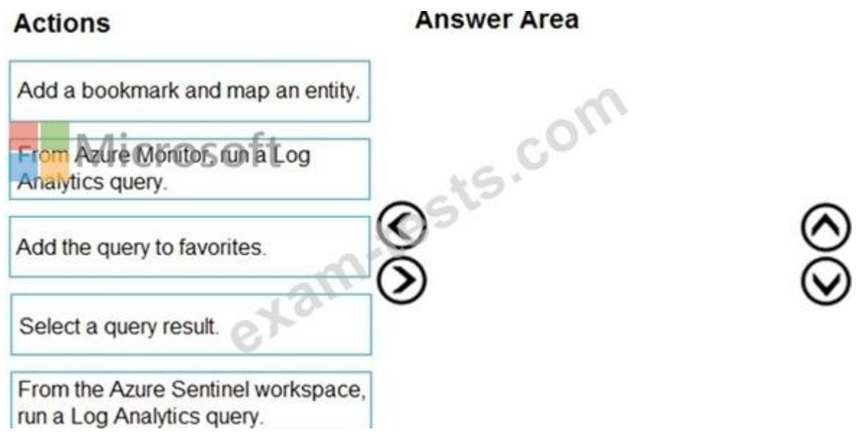


Explanation

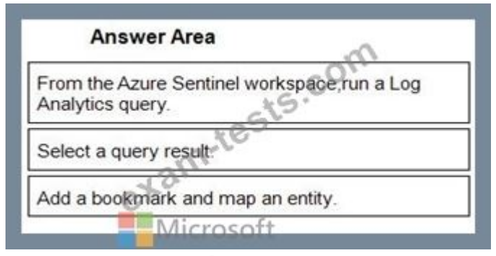
NEW QUESTION: 114

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.

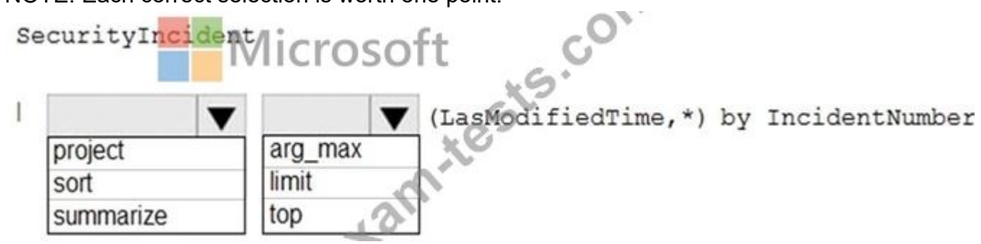


Answer:



1 - From the Azure Sentinel workspace,run a Log Analytics query.
2 - Select a query result.
3 - Add a bookmark and map an entity.
Reference:
https://docs.microsoft.com/en-us/azure/sentinel/bookmarks

NEW QUESTION: 115
You need to create a query for a workbook. The query must meet the following requirements:
List all incidents by incident number.
Only include the most recent log for each incident.
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:

Reference:
https://www.drware.com/whats-new-soc-operational-metrics-now-available-in-sentinel/

NEW QUESTION: 116
You have a Microsoft 365 E5 subscription that uses Microsoft Defender XDR.
You have a Microsoft Sentinel workspace.
Microsoft Sentinel connectors are configured as shown in the following table.

Connector	Collected log
Microsoft Entra ID	• Audit logs • Microsoft Graph activity logs
Microsoft 365	• Microsoft Exchange Online • Microsoft SharePoint Online • Microsoft Teams

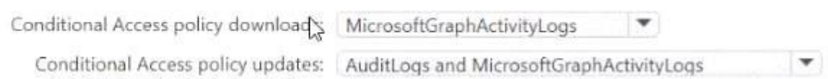
You use Microsoft Sentinel to investigate suspicious Microsoft Graph API activity related to Conditional Access policies. You need to search for the following activities:
* Downloads of the Conditional Access policies by using PowerShell
* Updates to the Conditional Access policies by using the Microsoft Entra admin center Which tables should you query for each activity? lo answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Answer:

Answer Area

Explanation:

Answer Area



NEW QUESTION: 117

You have a Microsoft 365 E5 subscription.

You plan to perform cross-domain investigations by using Microsoft 365 Defender.

You need to create an advanced hunting query to identify devices affected by a malicious email attachment.

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
| where SenderFromAddress =~ "MaliciousSender@example.com"
| where isnotempty (SHA256)
| [ extend / join / project / union ] (
DeviceFileEvents
| [ extend / join / project / union ] FileName, SHA256
) on SHA256
| [ extend / join / project / union ] Timestamp, FileName, SHA256, DeviceName, DeviceId,
NetworkMessageId, SenderFromAddress, RecipientEmailAddress
```

Answer:
Answer Area

```
EmailAttachmentInfo
| where SenderFromAddress =~ "MaliciousSender@example.com"
| where isnotempty (SHA256)
| [ join ] (
    DeviceFileEvents
    | [ project ] FileName, SHA256
) on SHA256
| [ project ] Timestamp, FileName, SHA256, DeviceName, DeviceId
```

(extend / join / project / union)

Reference:
https://docs.microsoft.com/en-us/microsoft-365/security/mtp/advanced-hunting-query-emails-devices?view=o365-worldwide

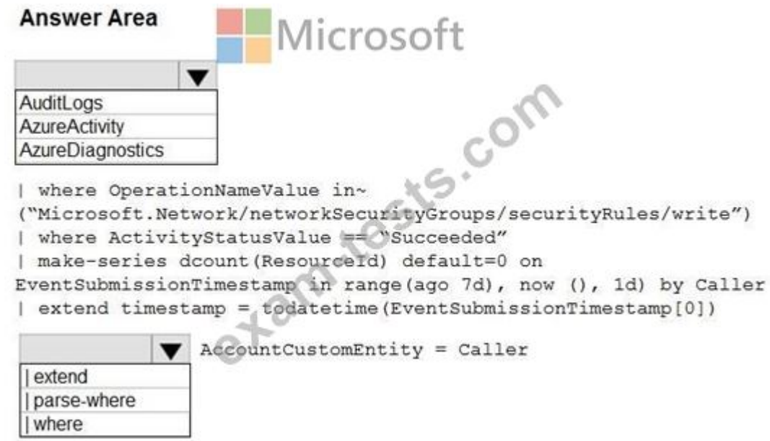
NEW QUESTION: 118
You have a Microsoft 365 B5 subscription that uses Microsoft Defender XDR. You are investigating an incident You need to review the incident tasks that were performed. What can you use on the Incident page?
A. Tasks and Alert timeline only
B. Tasks and Activity log only
C. Tasks only
D. Tasks, Activity log, and Alert timeline
Answer: (SHOW ANSWER)

NEW QUESTION: 119
Hotspot Question
You have an Azure subscription that contains a Microsoft Sentinel workspace.
You need to create a hunting query using Kusto Query Language (KQL) that meets the following requirements:
- Identifies an anomalous number of changes to the rules of a network
security group (NSG) made by the same security principal.
- Automatically associates the security principal with a Microsoft

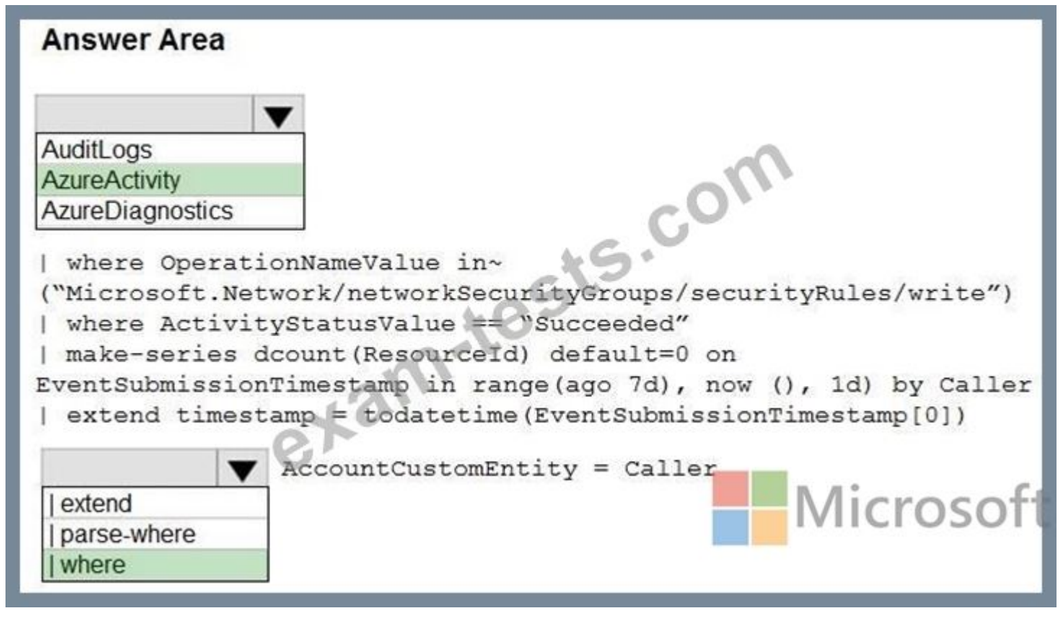
Sentinel entity.

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:



NEW QUESTION: 120

You have a Microsoft Sentinel workspace.

You need to configure the Fusion analytics rule to temporarily supress incidents generated by a Microsoft Defender connector. The solution must meet the following requirements:

* Minimize impact on the ability to detect multistage attacks.
* Minimize administrative effort.

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

NOTE: Each correct selection is worth one point.

Answer Area

Answer:

Explanation:

The Fusion analytics rule in Microsoft Sentinel automatically correlates alerts from multiple sources (including Microsoft Defender connectors) to detect multistage attacks . Because Fusion runs continuously and cannot be disabled without losing multi-stage detection, the best practice for temporarily suppressing incidents from a specific connector (like Microsoft Defender) is to use automation rul es , not by disabling the Fusion rule itself.

An automation rule can be configured to trigger on specific conditions (such as "When incident is updated" or "When incident is created") and then perform an action like running a playbook that applies suppressi on logic.

Here's the reasoning:

* Trigger:

* Setting the trigger to "When incident is updated" ensures that the rule evaluates changes to existing incidents-such as enrichment or tagging from Fusion-and provides finer control over suppression, minimizing impac t on the Fusion detection pipeline.

* Using "When incident is created" could interfere with Fusion's initial detection process.

* Action:

* The appropriate action is "Run playbook" , which allows automated handling (for example, tagging or closing certain inciden ts from a specific connector). This requires minimal administrative effort and avoids turning off the Fusion rule.

This configuration ensures that Fusion continues to detect multistage attacks (so detection isn't impacted) while automation handles temporar y suppression for specific connectors efficiently.

NEW QUESTION: 121
You have a Microsoft Sentinel workspace named SW1.
In SW1. you enable User and Entity Behavior Analytics (UEBA).
You need to use KQL to perform the following tasks:
* View the entity data that has fields for each type of entity.
* Assess the quality of rules by analyzing how well a rule performs.
Which table should you use in KQL for each task? To answer, drag the appropriate tables to the correct tasks.
Each table 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.

Answer:

Explanation:

NEW QUESTION: 122

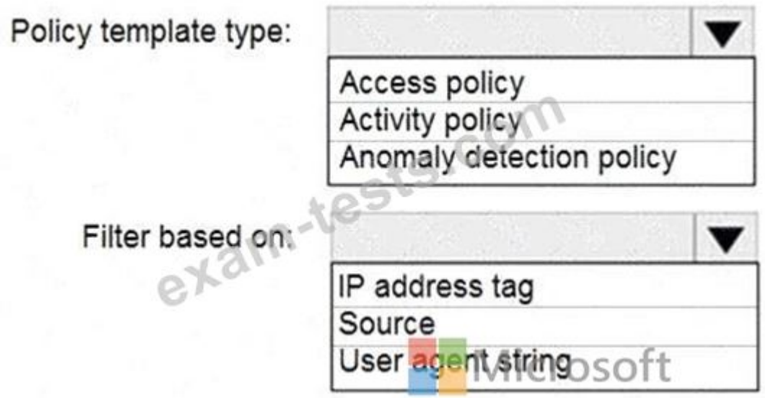
You purchase a Microsoft 365 subscription.

You plan to configure Microsoft Cloud App Security.

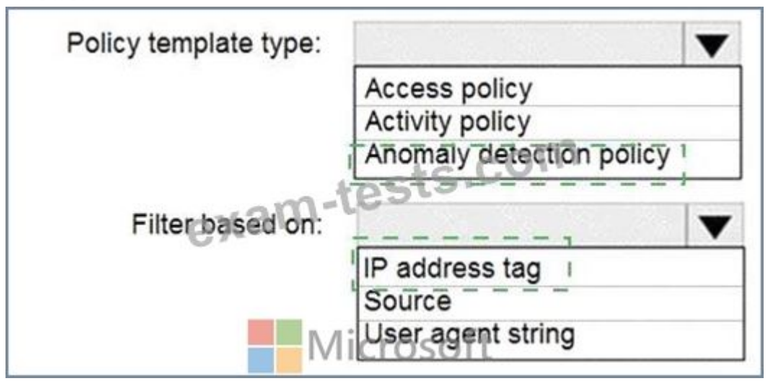
You need to create a custom template-based policy that detects connections to Microsoft 365 apps that originate from a botnet network.

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

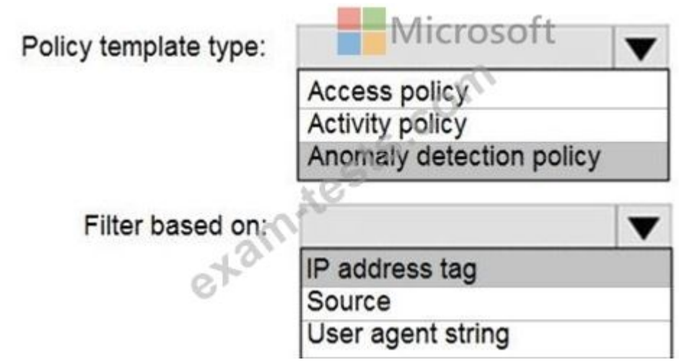
NOTE: Each correct selection is worth one point.



Answer:

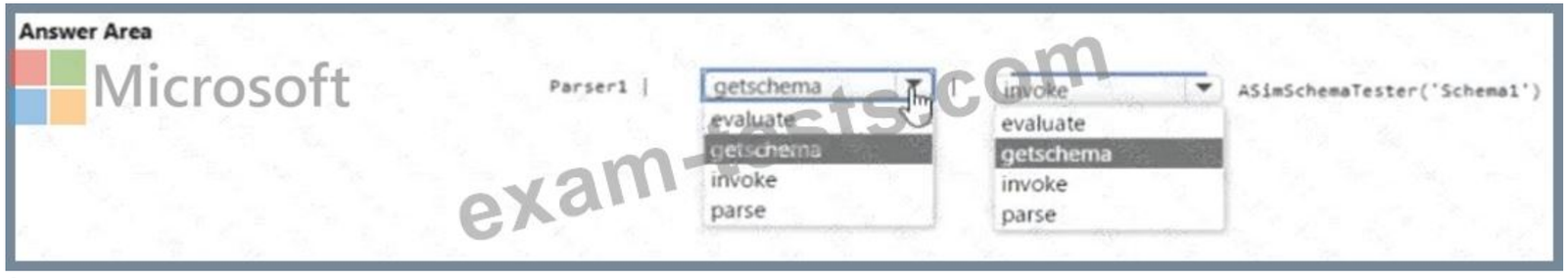


Explanation:

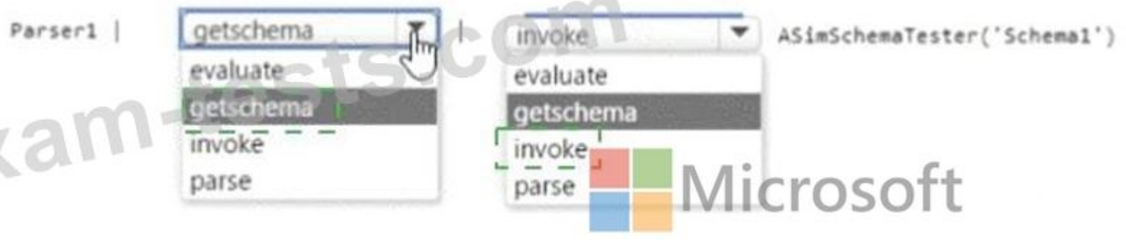


Reference:
https://docs.microsoft.com/en-us/cloud-app-security/anomaly-detection-policy

NEW QUESTION: 123
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.



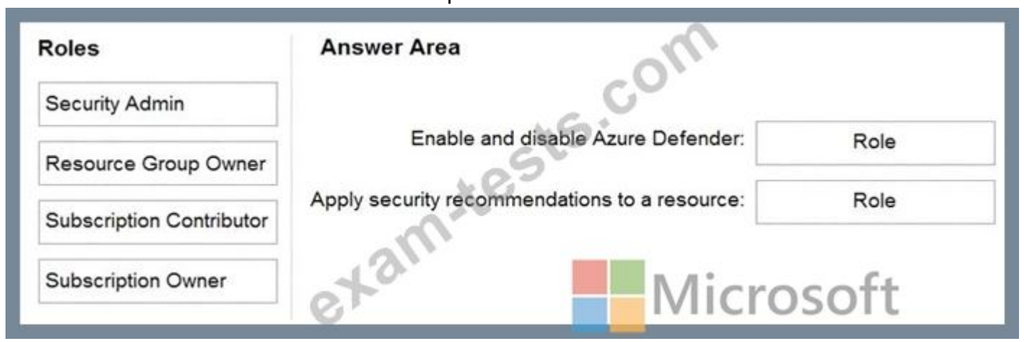
Answer:
Answer Area



Explanation:

To validate a custom ASIM parser output, you test that the parser's resulting table structure complies with the intended ASIM schema. In KQL, the getschema operator produces a tabular representation of the current pipeline's schema (column names, types, order). The invoke operator is then used to call a function on that tabular input. ASIM provides the helper function ASimSchemaTester(), which accepts the schema table and the target schema name and validates that the input conforms (columns exist, types match, required fields are present).
Therefore, the correct construction is to run the parser (here, Parser1), pipe its output to getschema to obtain the schema of the produced table, and then invoke ASimSchemaTester('Schema1') to perform the validation. Other options are not appropriate: evaluate is for plugins; parse extracts fields from strings rather than validate schema; and calling the tester without getschema would not pass the required schema table.
Hence, the correct command is:
Parser1 | getschema | invoke ASimSchemaTester('Schema1').

NEW QUESTION: 124
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.



Answer:

Explanation:

Reference:

https://docs.microsoft.com/en-us/azure/security-center/security-center-permissions

NEW QUESTION: 125

You have an on-premises datacenter that contains a custom web app named Appl. App1 uses Active Directory Domain Services (AD DS) authentication and is accessible by using Microsoft Entra application proxy.

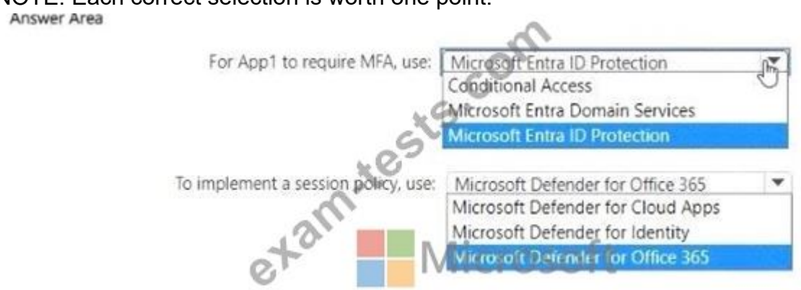
You have a Microsoft 365 E5 subscription that uses Microsoft Defender XDR.

You receive an alert that a user downloaded highly confidential documents.

You need to remediate the risk associated with the alert by requiring multi-factor authentication (MFA) when users use App1 to initiate the download of documents that have a Highly Confidential sensitivity label applied.

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

NOTE: Each correct selection is worth one point.



Answer:

Explanation:

NEW QUESTION: 126

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 (LEAVE A REPLY)

Reference:

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

NEW QUESTION: 127

You have a Microsoft Sentinel workspace that contains a custom workbook named Workbook1.

You need to create a visual based on the SecuntyEvent table. The solution must meet the following requirements:

* Identify the number of security events ingested during the past week.

* Display the count of events by day in a timechart

What should you add to Workbook1?

A. a query

B. a group

C. a metric

D. links or tabs

Answer: A (LEAVE A REPLY)

NEW QUESTION: 128

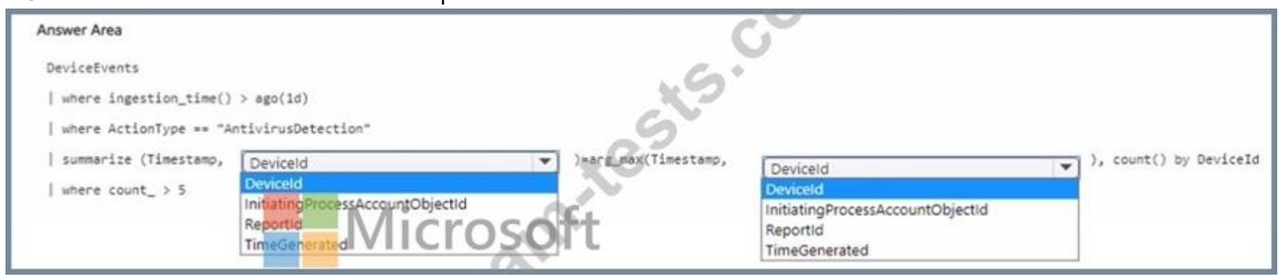
You have a Microsoft 365 E5 subscription that uses Microsoft Copilot for Security. You plan to run the following code to create a custom Copilot for Security plugin.

```
<code segment>
SkillGroups:
- Format: <target>
Skills:
```

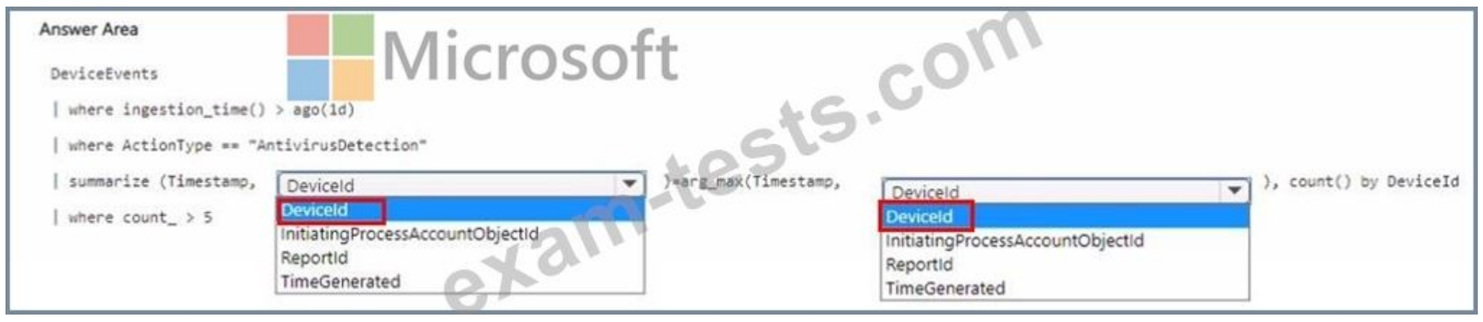
You need to specify a format and complete the code segment. Which format should you use for the <target> variable?

A. KQL
B. SQL
C. API
D. GPT
Answer: C (LEAVE A REPLY)

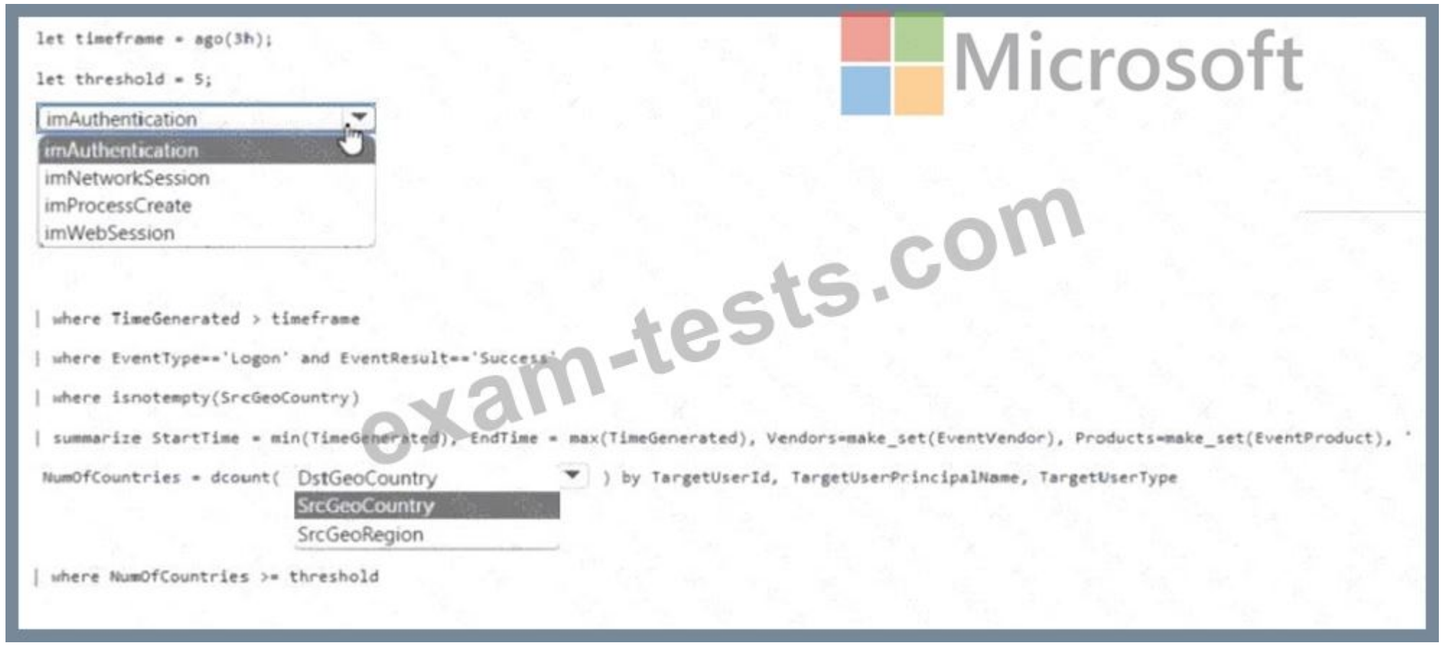
NEW QUESTION: 129
You have a Microsoft 365 subscription that uses Microsoft Defender XDR.
You need to create a custom detection rule that will identify devices that had more than five antivirus detections within the last 24 hours.
how should you complete the query? To answer, select the appropriate options in the answer area.
NOTE Each correct selection is worth one point.



Answer:



NEW QUESTION: 130
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



Answer:

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( SrcGeoCountry ) by TargetUserId, TargetUserPrincipalName, TargetUserType
```

NEW QUESTION: 131

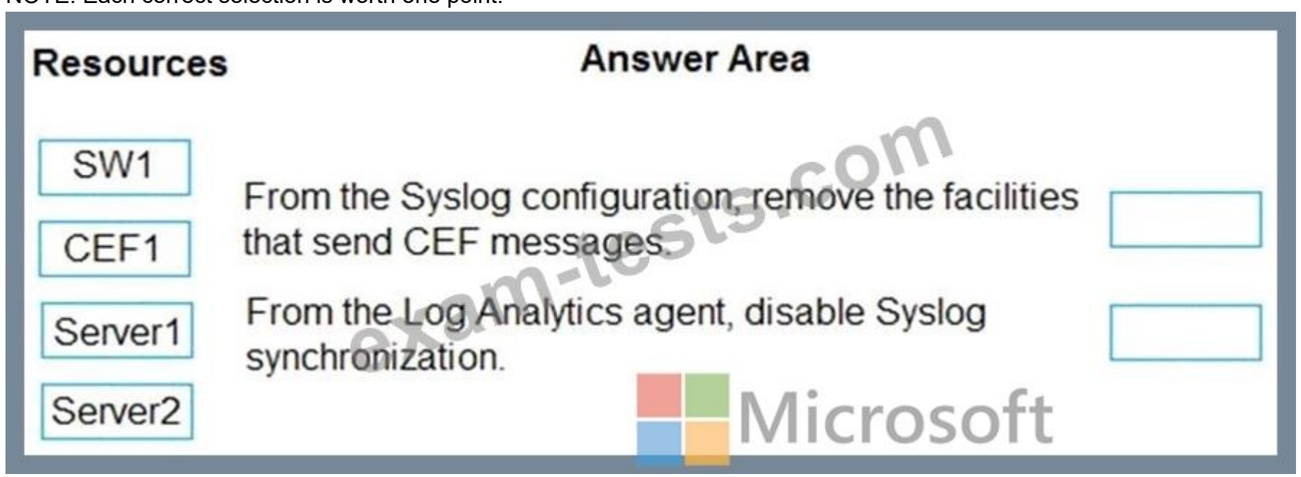
You have the resources shown in the following table.

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

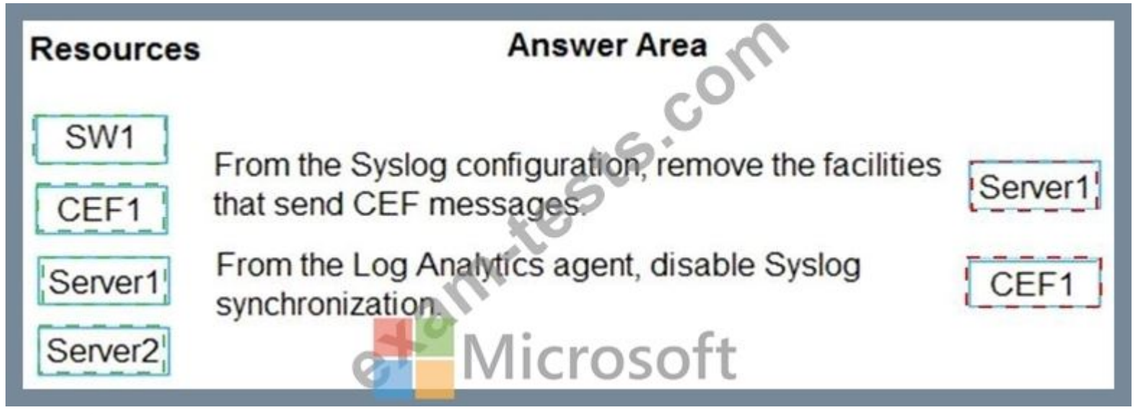
You need to prevent duplicate events from occurring in SW1.

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.

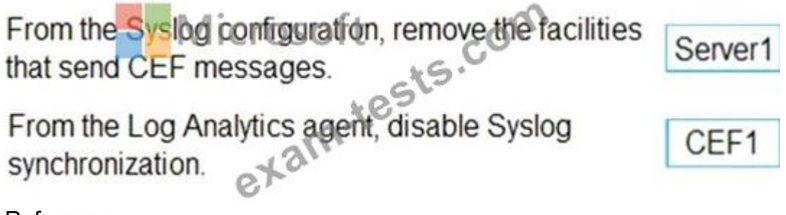
NOTE: Each correct selection is worth one point.



Answer:



Explanation:



Reference:
https://docs.microsoft.com/en-us/azure/sentinel/connect-log-forwarder?tabs=rsyslog

NEW QUESTION: 132
You have a Microsoft 365 E5 subscription that uses Microsoft Defender XDR.
You have a custom detection rule named Rule1 that generates an alert if more than five antivirus detections are identified on a device. Rule1 has a loopback period of 12 hours.
You need to change the loopback period to 48 hours.
What should you modify for Rule1?
A. the frequency
B. the summarize operator of the KQL query
C. the where operator of the KQL query
D. the scope
Answer: A (LEAVE A REPLY)
XDR Custom Detection Rules Documentation):
In Microsoft Defender XDR, custom detection rules are scheduled KQL queries that evaluate telemetry on a recurring schedule, using a lookback (loopback) period to determine how much historical data to analyze during each run.
The loopback period determines the time window over which data i s evaluated (e.g., 12 hours, 48 hours). To change this period, administrators modify the rule's schedule configuration - specifically the frequency or recurrence settings in the custom detection rule editor. The KQL query (including summarize or where oper ators) defines the logic but not the temporal scope of data evaluation.
Therefore, extending the loopback from 12 hours to 48 hours requires adjusting the frequency (schedule) configuration of the rule, not the query itself.
Correct Answer: A. the freque ncy

NEW QUESTION: 133
You have a Microsoft 365 E5 subscription that contains a device named Device1.

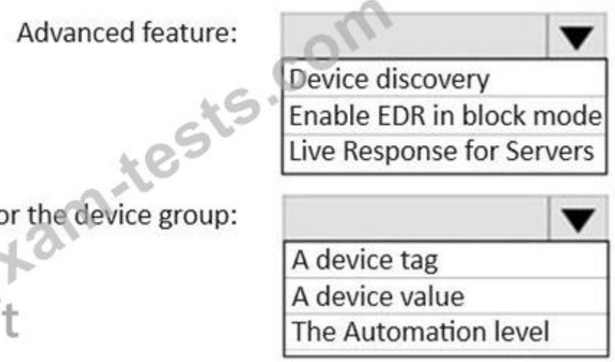
From the Microsoft Defender portal, you discover that an alert was triggered for Device1.
From the Device inventory page, you isolate Device1.
You need to collect a list of installed programs on Device1.
What should you do?
A. Initiate a live response session and run the library command.
B. Run an advanced hunting query against the DeviceTvmSoftwareInventory table.
C. Initiate a live response session and run the analyze command.
D. Initiate an automated investigation and view the results in the Action center.
Answer: B (LEAVE A REPLY)
Correct:
* Collect an investigation package and download the results from the Action center.
Collect investigation package from devices
As part of the investigation or response process, you can collect an investigation package from a device. By collecting the investigation package, you can identify the current state of the device and further understand the tools and techniques used by the attacker.
Investigation package contents for Windows devices
For Windows devices, the package contains the folders described in the following table:
-> Installed programs
This .CSV file contains the list of installed programs that can help identify what is currently installed on the device.
Etc.
* Run an advanced hunting query against the DeviceTvmSoftwareInventory table.
The DeviceTvmSoftwareInventory is a table in the Microsoft Defender XDR advanced hunting schema that contains the inventory of all software installed on devices within your organization, as identified by Microsoft Defender Vulnerability Management (MDVM). It provides details such as the software's vendor, name, version, and its end-of-support status, allowing organizations to hunt for specific software, track its lifecycle, and identify potential risks associated with end-of-life applications.
Incorrect:
* Initiate an automated investigation and view the results in the Action center.
* Initiate a live response session and run the library command.
* Initiate a live response session and run the analyze command.
Analyze - just analyses the entity with various incrimination engines to reach a verdict.
* Initiate a live response session and run the processes command.
Processes - just shows all processes running on the device, not all installed programs.
* Run an advanced hunting query against the DeviceProcessEvents table.
The DeviceProcessEvents table in the advanced hunting schema contains information about process creation and related events.
* Run an advanced hunting query against the DeviceTvmInfoGathering table.
The DeviceTvmInfoGathering table in the advanced hunting schema contains Microsoft Defender Vulnerability Management assessment events including the status of various configurations and attack surface area states of devices.
Reference:
https://learn.microsoft.com/en-us/defender-xdr/advanced-hunting-devicetvmsoftwareinventory- table
https://learn.microsoft.com/en-us/defender-endpoint/respond-machine-alerts

NEW QUESTION: 134
You have a Microsoft Sentinel workspace named SW1.

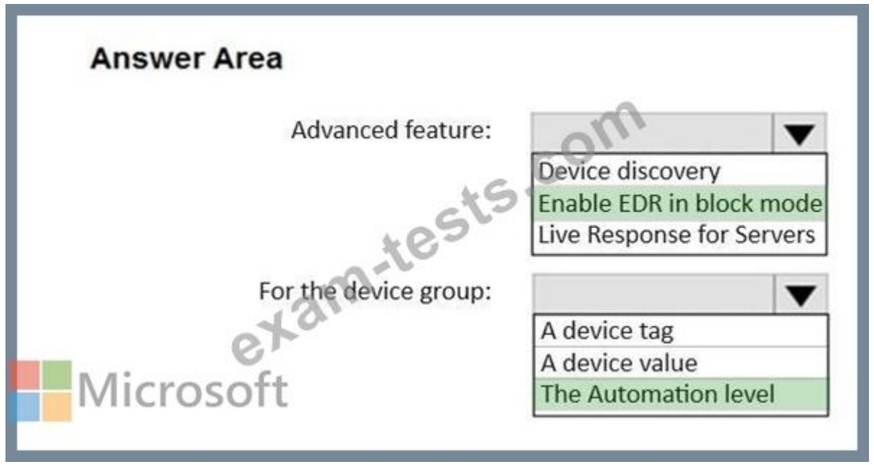
You need to identify which anomaly rules are enabled in SW1.
What should you review in Microsoft Sentine1?
A. Analytics
B. Content hub
C. Entity behavior
D. Settings
Answer: (SHOW ANSWER)

NEW QUESTION: 135
Hotspot Question
You have a Microsoft 365 E5 subscription that uses Microsoft 365 Defender for Endpoint.
You need to ensure that you can initiate remote shell connections to Windows servers by using the Microsoft 365 Defender portal.
What should you configure? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Answer Area



Answer:

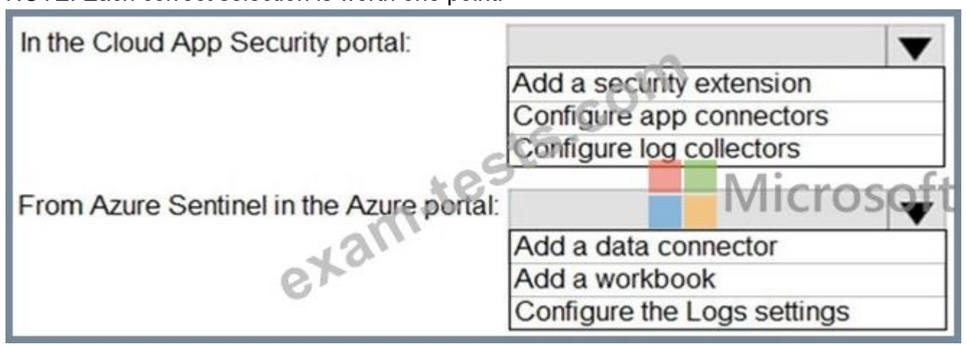


NEW QUESTION: 136

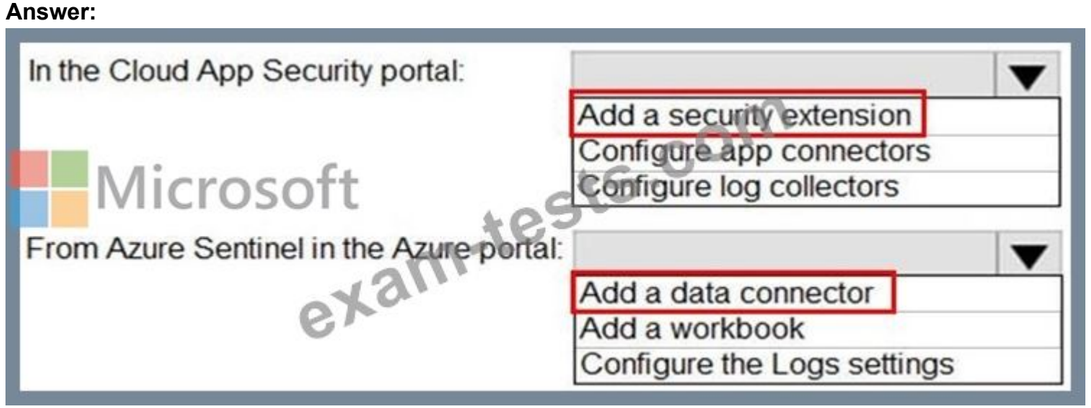
You need to configure the Azure Sentinel integration to meet the Azure Sentinel requirements.

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

NOTE: Each correct selection is worth one point.



Answer:

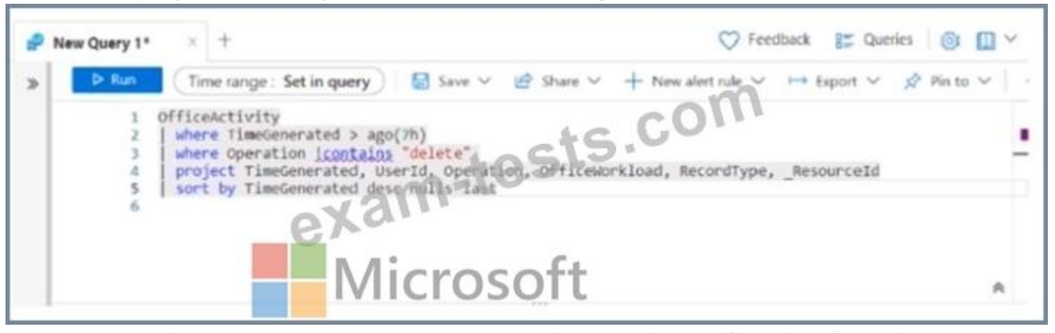


Reference:

https://docs.microsoft.com/en-us/cloud-app-security/siem-sentinel

NEW QUESTION: 137
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 Alert automation settings
B. entity mapping
C. the Incident automation settings
D. the query rule
Answer: B (LEAVE A REPLY)

NEW QUESTION: 138
You have a Microsoft Sentinel workspace.
You have a query named Query1 as shown in the following exhibit.

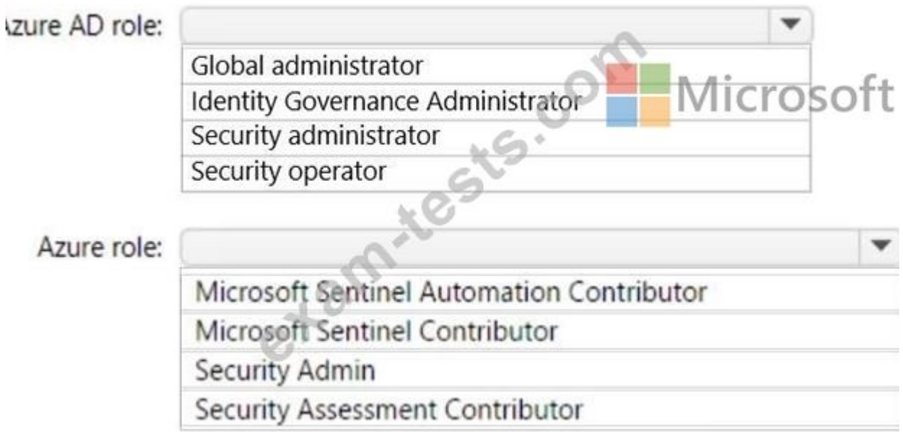


You plan to create a custom parser named Parser 1. You need to use Query1 in Parser1. What should you do first?
A. Remove line 2.
B. In line 4. remove the TimeGenerated predicate.
C. Remove line 5.
D. In line 3, replace the 'contains operator with the !has operator.
Answer: C (LEAVE A REPLY)
This can 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: 139
Hotspot Question

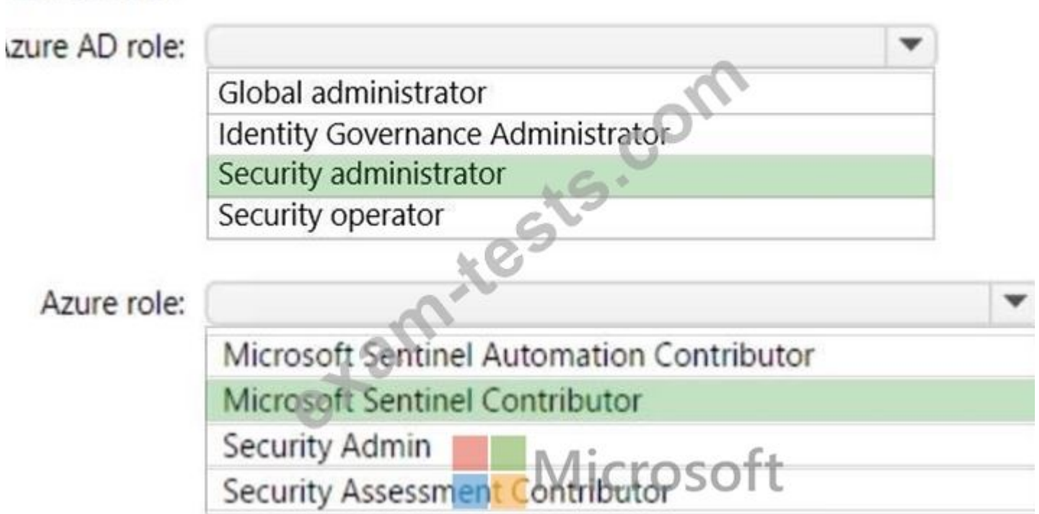
You have an Azure subscription that uses Microsoft Sentinel and contains a user named User1.
You need to ensure that User1 can enable User and Entity Behavior Analytics (UEBA) for entity behavior in Azure AD. The solution must use the principle of least privilege.
Which roles should you assign to User1? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Answer Area



Answer:

Answer Area



NEW QUESTION: 140
You have a Microsoft Sentinel workspace.
You need to configure the Fusion analytics rule to temporarily supress incidents generated by a Microsoft Defender connector. The solution must meet the following requirements:
* Minimize impact on the ability to detect multistage attacks.
* Minimize administrative effort.
How should you configure the rule? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Answer:

Explanation:

NEW QUESTION: 141

You have a Microsoft 365 subscription that uses Microsoft Copilot for Security.

You create a promptbook named Book1.

For Book1, you need to create a prompt that contains an input named IncidentID.

How should you format IncidentID?

A. < IncidentID >

B. SIncidentID$

C. ##IncidentID##

D. [IncidentID]

Answer: A (LEAVE A REPLY)

In Copilot for Security promptbooks, inputs are referenced as placeholders wrapped in angle brackets (for example, < SENTINEL_INCIDENT_ID >). To define an input named IncidentID in a prompt, format it as < IncidentID > .

NEW QUESTION: 142
Drag and Drop Question
You have an Azure subscription linked to an Azure Active Directory (Azure AD) tenant. The tenant contains two users named User1 and User2.
You plan to deploy Azure Defender.
You need to enable User1 and User2 to perform tasks at the subscription level as shown in the following table.

User	Task
User1	• Assign initiatives • Edit security policies • Enable automatic provisioning
User2	• View alerts and recommendations • Apply security recommendations • Dismiss alerts

The solution must use the principle of least privilege.
Which role should you assign to each user? To answer, drag the appropriate roles to the correct users. 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.

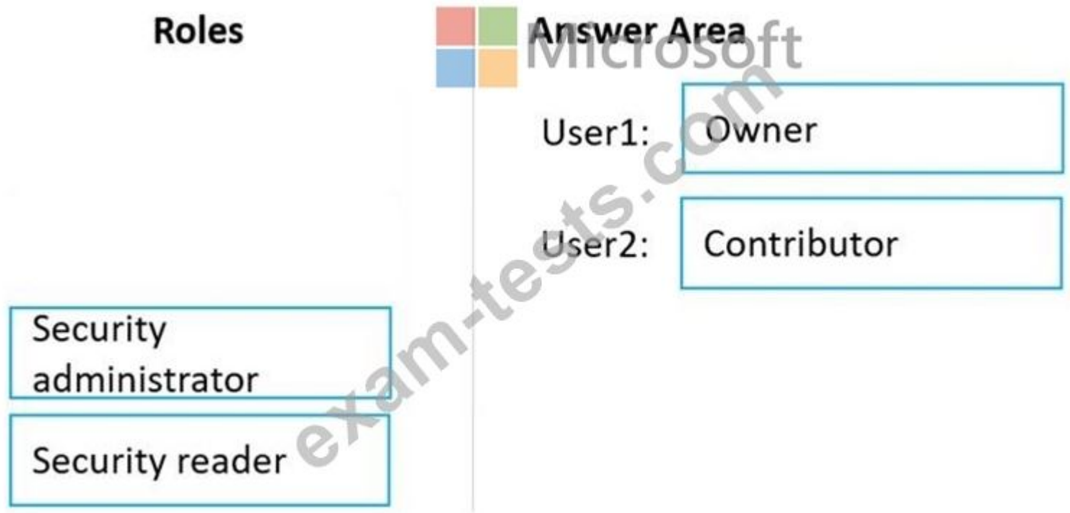
Roles

- Contributor
- Owner
- Security administrator
- Security reader

Answer Area

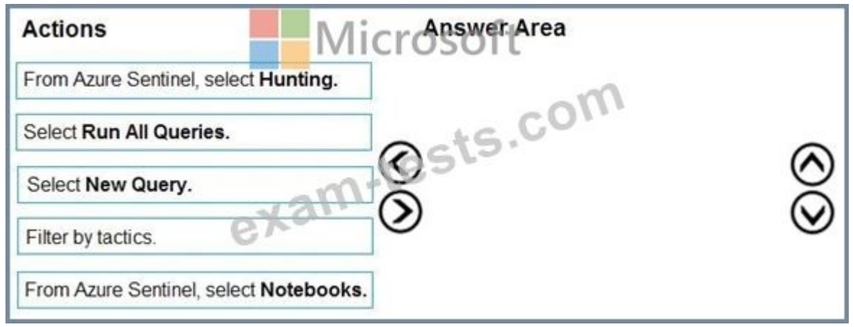
User1: [ ]

User2: [ ]

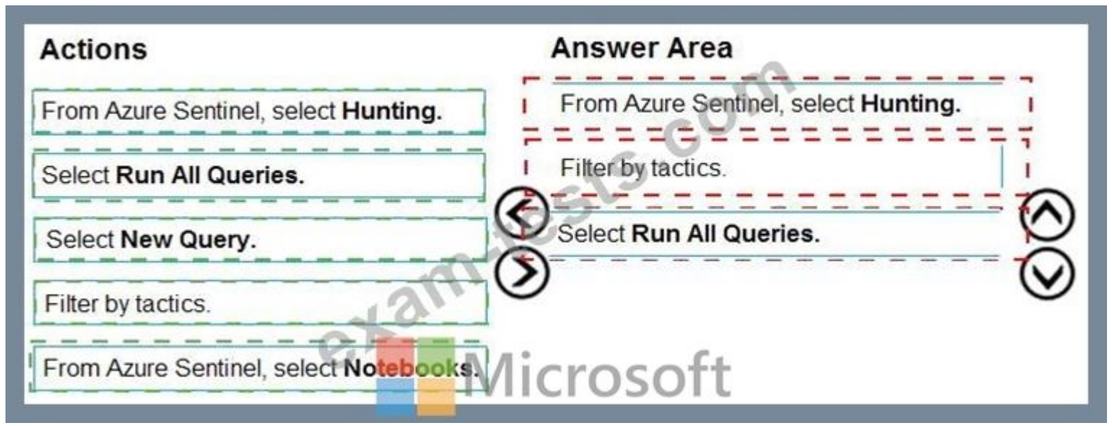


Explanation:
Box 1: Owner
At the Subscription Level, only Contributor and Owner can :
- Apply security recommendations
- Add/Assign initiatives
- Edit security policy
- Dismiss alerts
However, only the Owner can 'Enable auto provisioning'... to be the owner of the extension you're deploying. "For auto provisioning, the specific role required depends on the extension you're deploying." Box 2: Contributor Only the Contributor or the Owner can apply security recommendations.
Reference:
https://docs.microsoft.com/en-us/azure/defender-for-cloud/permissions
https://learn.microsoft.com/en-us/azure/defender-for-cloud/enable-data- collection?tabs=autoprovision-loganalytic#availability

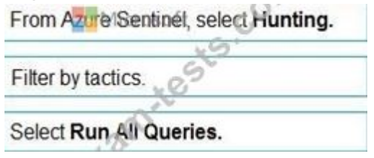
NEW QUESTION: 143
You have an Azure Sentinel deployment.
You need to query for all suspicious credential access activities.
Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.



Answer:



Explanation



NEW QUESTION: 144

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

You need to configure the continuous export of high-severity alerts to enable their retrieval from a third-party security information and event management (SIEM) solution.

To which service should you export the alerts?

A. Azure Cosmos DB

B. Azure Event Grid

C. Azure Event Hubs

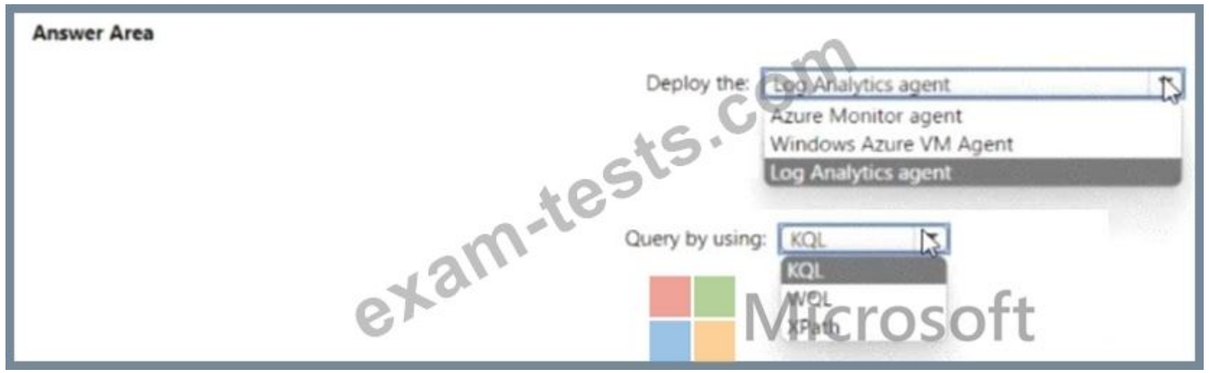
D. Azure Data Lake

Answer: C (LEAVE A REPLY)

Reference: https://docsmicrosoftcom/en-us/azure/security-center/continuous-export?tabs=azure-portal

NEW QUESTION: 145

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:

Explanation:

NEW QUESTION: 146

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.

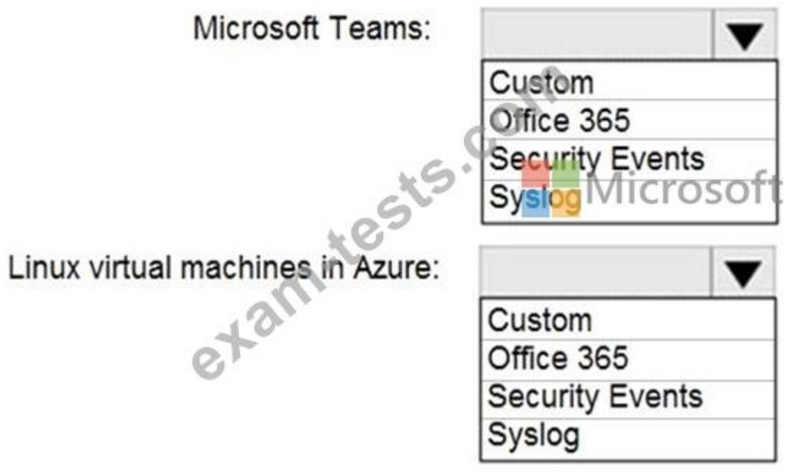
Does this meet the goal?
A. Yes
B. No
Answer: (SHOW ANSWER)
A machine with Azure Arc-enabled servers becomes an Azure resource and - when you've installed the Log Analytics agent on it - appears in Defender for Cloud with recommendations like your other Azure resources.
Install Log Analytics manually or when you enable auto provisioning of Log Analytics in
"Autoprovisioning" tag, auto provisioning is already turned on.
Reference:
https://docs.microsoft.com/en-us/azure/defender-for-cloud/quickstart-onboard- machines?pivots=azure-arc
https://docs.microsoft.com/en-us/azure/defender-for-cloud/enable-data-collection?tabs=autoprovision-feature

NEW QUESTION: 147
You have an Azure subscription.
You need to delegate permissions to meet the following requirements:
* Enable and disable advanced features of Microsoft Defender for Cloud.
* Apply security recommendations to a resource.
The solution must use the principle of least privilege.
Which Microsoft Defender for Cloud role should you use for each requirement? To answer, drag the appropriate roles to the correct requirements. Each role may be used once, mote 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.

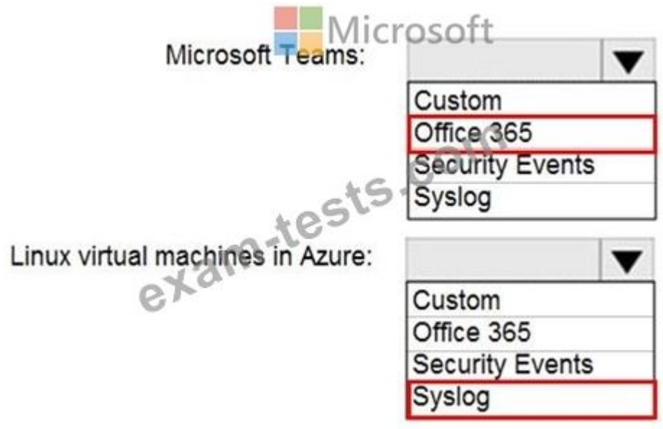
Answer:

Explanation:

NEW QUESTION: 148
You deploy Azure Sentinel.
You need to implement connectors in Azure Sentinel to monitor Microsoft Teams and Linux virtual machines in Azure. The solution must minimize administrative effort.
Which data connector type should you use for each workload? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



Answer:



Reference:
https://docs.microsoft.com/en-us/azure/sentinel/connect-office-365
https://docs.microsoft.com/en-us/azure/sentinel/connect-syslog

NEW QUESTION: 149
You need to configure Microsoft Cloud App Security to generate alerts and trigger remediation actions in response to external sharing of confidential files.
Which two actions should you perform in the Cloud App Security portal? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.
A. From Settings, select Information Protection, select Azure Information Protection, and then select Only scan files for Azure Information Protection classification labels and content inspection warnings from this tenant.
B. Select Investigate files, and then filter App to Office 365.
C. Select Investigate files, and then select New policy from search.
D. From Settings, select Information Protection, select Azure Information Protection, and then select Automatically scan new files for Azure Information Protection classification labels and content inspection warnings.
E. From Settings, select Information Protection, select Files, and then enable file monitoring.
F. Select Investigate files, and then filter File Type to Document.
Answer: D,E (LEAVE A REPLY)
In Defender for Cloud Apps, under the settings cog, select the Settings page under the System heading.
Under Microsoft Information Protection, select Automatically scan new files for Microsoft Information Protection sensitivity labels.
https://docs.microsoft.com/en-us/defender-cloud-apps/tutorial-dlp
https://www.microsoft.com/en-us/videoplayer/embed/RE4CMYG?postJsllMsg=true

NEW QUESTION: 150
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. The number of alerts exceeded 10,000 within two minutes.
B. The rule query takes too long to run and times out.
C. There are connectivity issues between the data sources and Log Analytics.
D. Permissions to one of the data sources of the rule query were modified.
Answer: (SHOW ANSWER)

NEW QUESTION: 151
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 (LEAVE A REPLY)
Reference:
https://docs.microsoft.com/en-us/azure/sentinel/investigate-cases

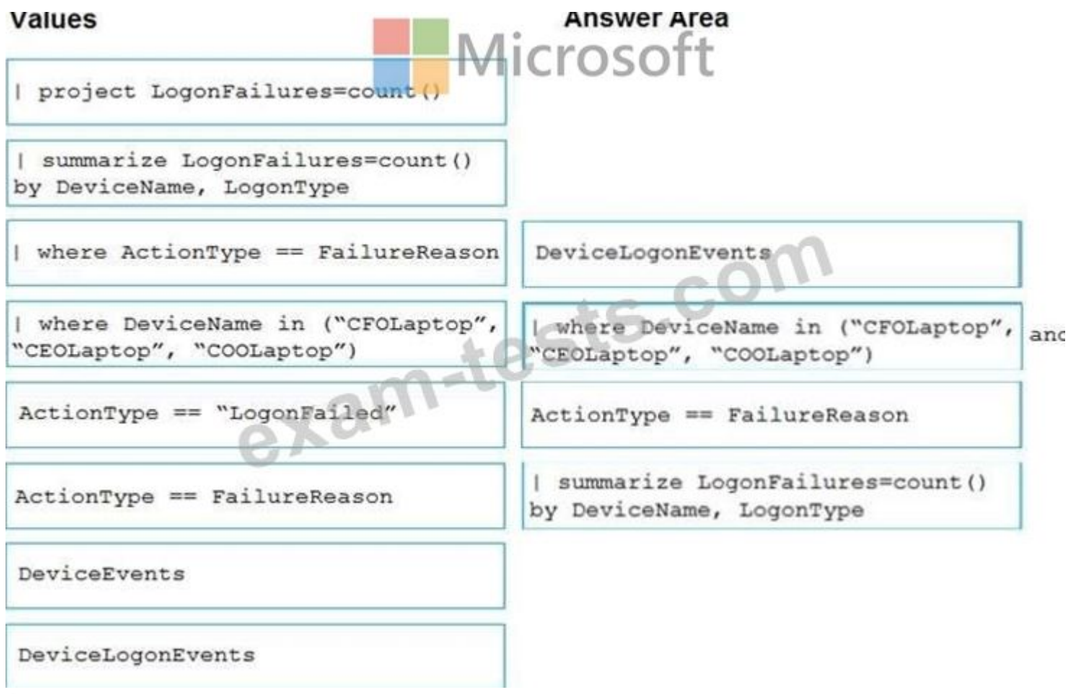
NEW QUESTION: 152
DRAG DROP
You are investigating an incident by using Microsoft 365 Defender.
You need to create an advanced hunting query to count failed sign-in authentications on three devices named CFOLaptop, CEOLaptop, and COOLaptop.
How should you complete the query? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.
Select and Place:

Values

- `| project LogonFailures=count()`
- `| summarize LogonFailures=count() by DeviceName, LogonType`
- `| where ActionType == FailureReason`
- `| where DeviceName in ("CFOLaptop", "CEOLaptop", "COOLaptop")`
- `ActionType == "LogonFailed"`
- `ActionType == FailureReason`
- `DeviceEvents`
- `DeviceLogonEvents`

Answer Area

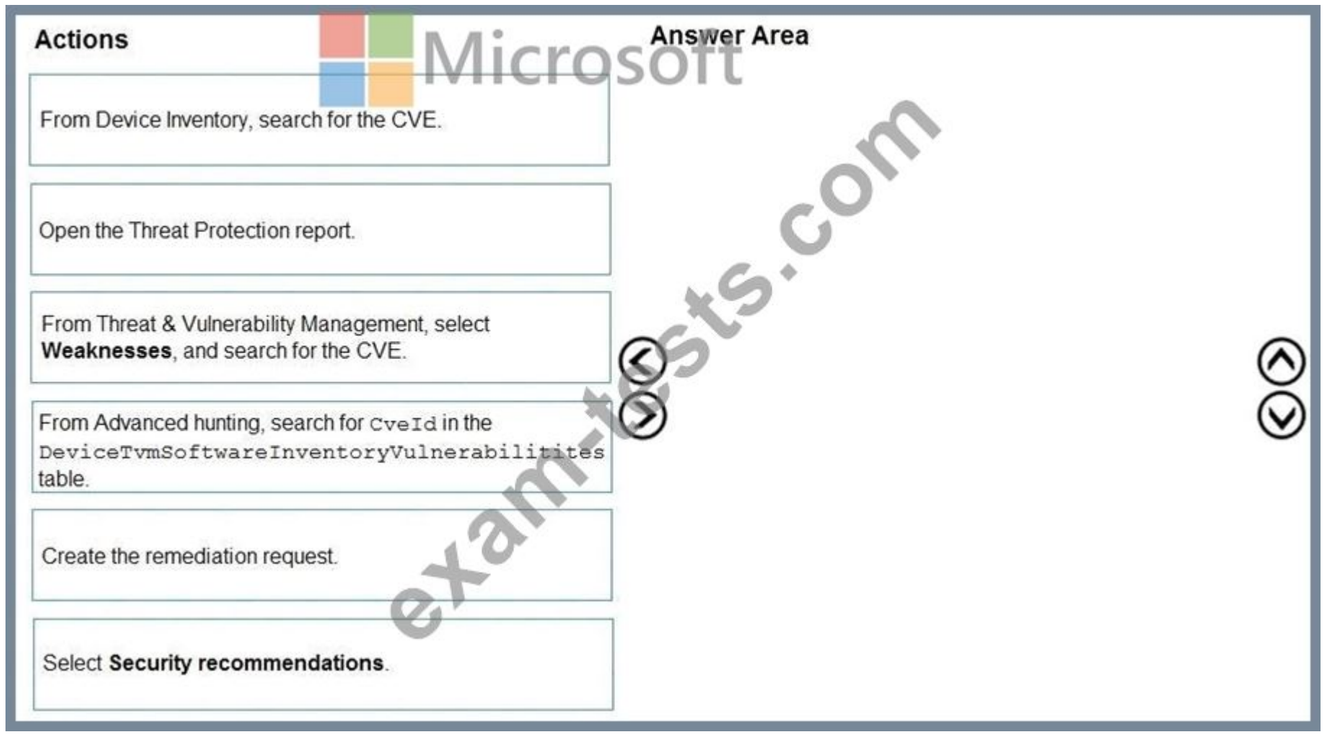
Answer:



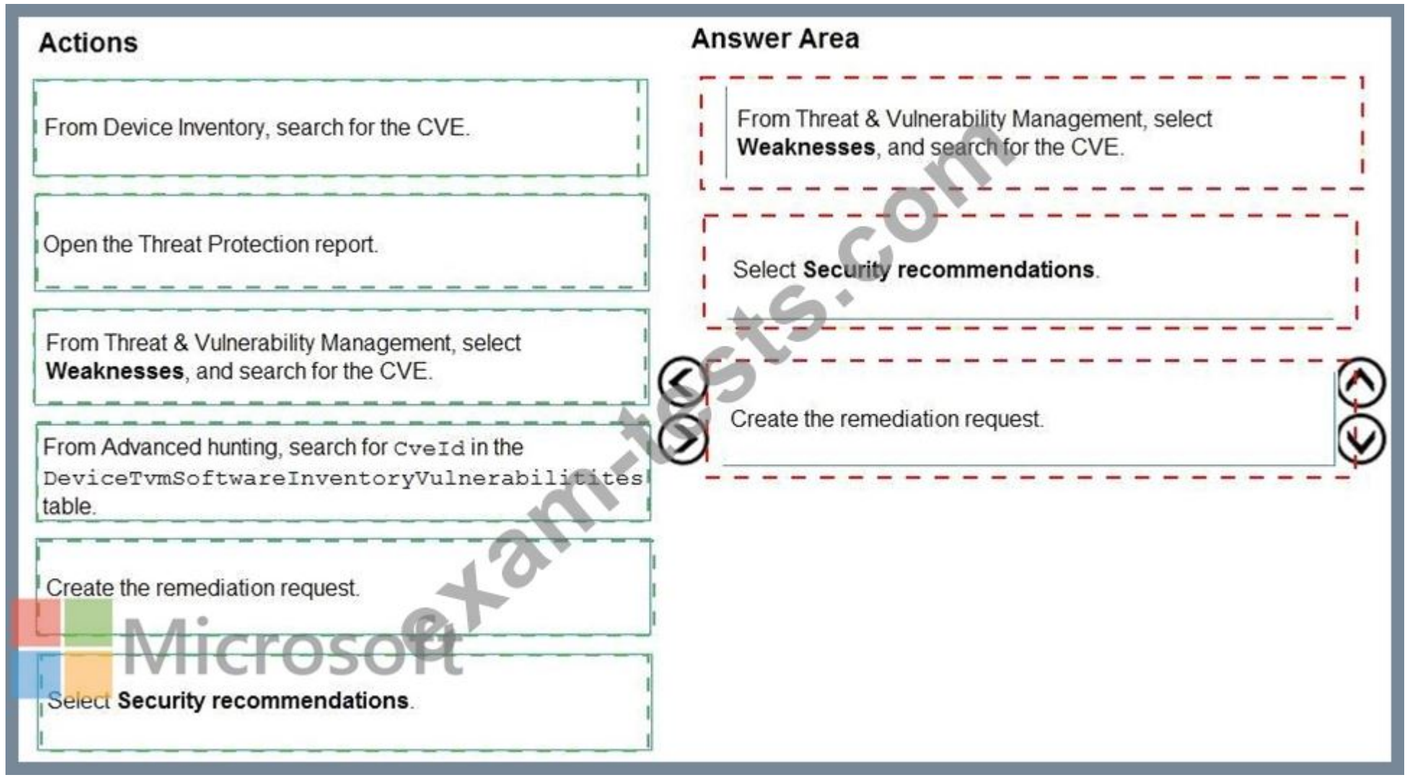
Section: [none]

NEW QUESTION: 153
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: (SHOW ANSWER)
Explanation (concise): To send a Microsoft Teams message when a suspicious sign-in is detected, create a playbook (Logic App) that posts to Teams (A) and associate the playbook so it runs when the corresponding alert/incident is created (B)-typically via an automation rule or by attaching the playbook to the analytics rule/incident. Entity behavior analytics, workbooks, or Fusion aren't required for sending Teams notifications.

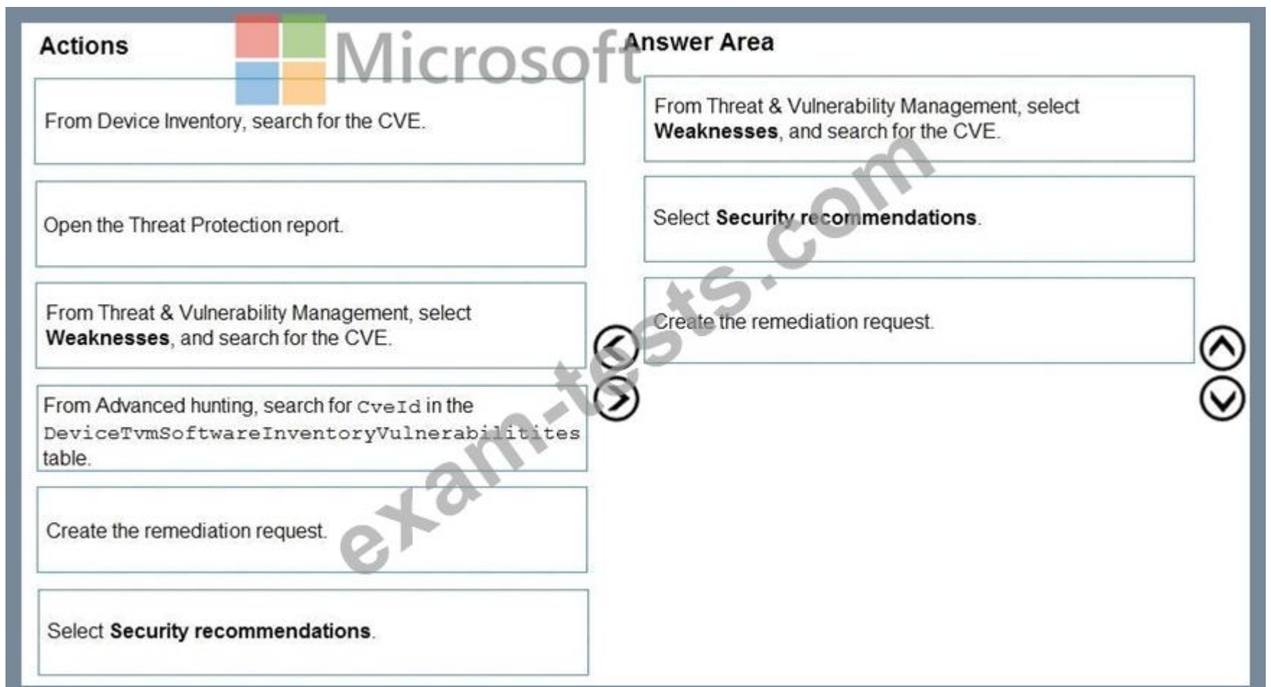
NEW QUESTION: 154
You are informed of a new common vulnerabilities and exposures (CVE) vulnerability that affects your environment.
You need to use Microsoft Defender Security Center to request remediation from the team responsible for the affected systems if there is a documented active exploit available.
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.



Answer:



Explanation



Reference:

https://techcommunity.microsoft.com/t5/core-infrastructure-and-security/microsoft-defender-atp-remediate-apps

NEW QUESTION: 155

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: (SHOW ANSWER)

In Microsoft Defender for Cloud's role-based access model, specific Azure built-in roles define what users can view and configure:

* Security Reader: View-only access to Defender for Cloud recommendations and alerts.
* Security Operator: Can view and dismiss alerts but cannot modify security policies.
* Security Admin: Can view everything a reader can and additionally edit security policies, manage recommendations, and configure settings across Defender for Cloud.
* Owner/Contributor: Have broader Azure resource management rights, exceeding what's required to manage Defender for Cloud policies-violating the principle of least privilege.

The principle of least privilege dictates assigning the narrowest role that allows performing the required tasks.

In this case, the Security Admin role is explicitly documented by Microsoft as granting permission to modify security policies and settings in Defender for Cloud, without granting full subscription ownership rights.

Therefore, to allow User1 to modify Defender for Cloud security policies while maintaining least privilege:

Assign the Security Admin role.

NEW QUESTION: 156
You receive a security bulletin about a potential attack that uses an image file.
You need to create an indicator of compromise (IoC) in Microsoft Defender for Endpoint to prevent the attack.
Which indicator type should you use?
A. a URL/domain indicator that has Action set to
B. a URL/domain indicator that has Action set to
C. a file hash indicator that has Action set to Alert and block
D. a certificate indicator that has Action set to Alert and block
Answer: C (LEAVE A REPLY)
Reference:
https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/indicator-file?view=o365-worldwide

NEW QUESTION: 157
You need to configure the Microsoft Sentinel integration to 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:

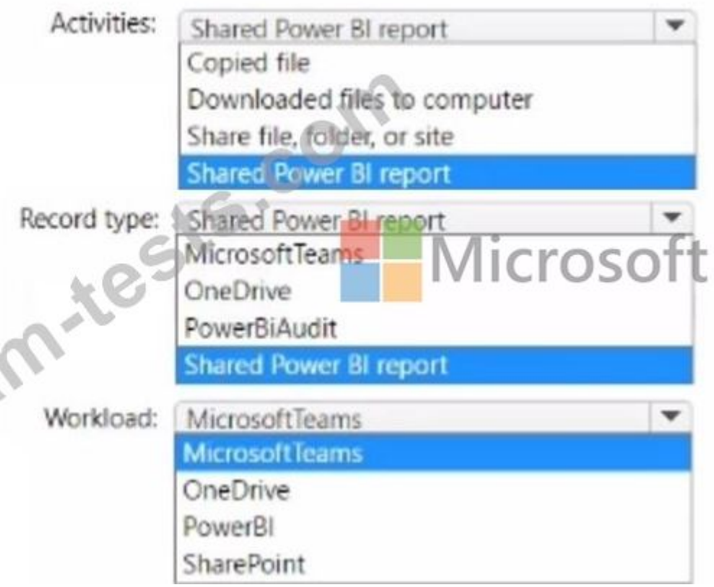
Explanation:

NEW QUESTION: 158
You have an Azure subscription that has Microsoft Defender for Cloud enabled.
You have a virtual machine named Server! 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: (SHOW ANSWER)
When a server is hosted outside of Azure (for example, in AWS , GCP , or on-premises), it must first be connected to Azure via Azure Arc before Microsoft Defender for Cloud can onboard it for protection and monitoring.
The Azure Arc agent (also known as the Connected Machine agent) establishes that connection between the non-Azure resource and Azure. Once connected, Defender for C loud can then deploy the necessary security extensions and agents (such as the Defender for Endpoint sensor or vulnerability scanner) automatically.
Why not the other options:
* Microsoft Monitoring Agent (MMA): Legacy; replaced by the Azure Monitor Agent (A MA) and no longer required for new Defender deployments.
* Azure Monitor Agent (AMA): Used after Arc onboarding for data collection but cannot onboard non- Azure servers by itself.
* Azure Pipelines Agent: Used for Azure DevOps CI/CD, not for Defender for Cloud .
# Correct Answer: B. the Azure Arc agent

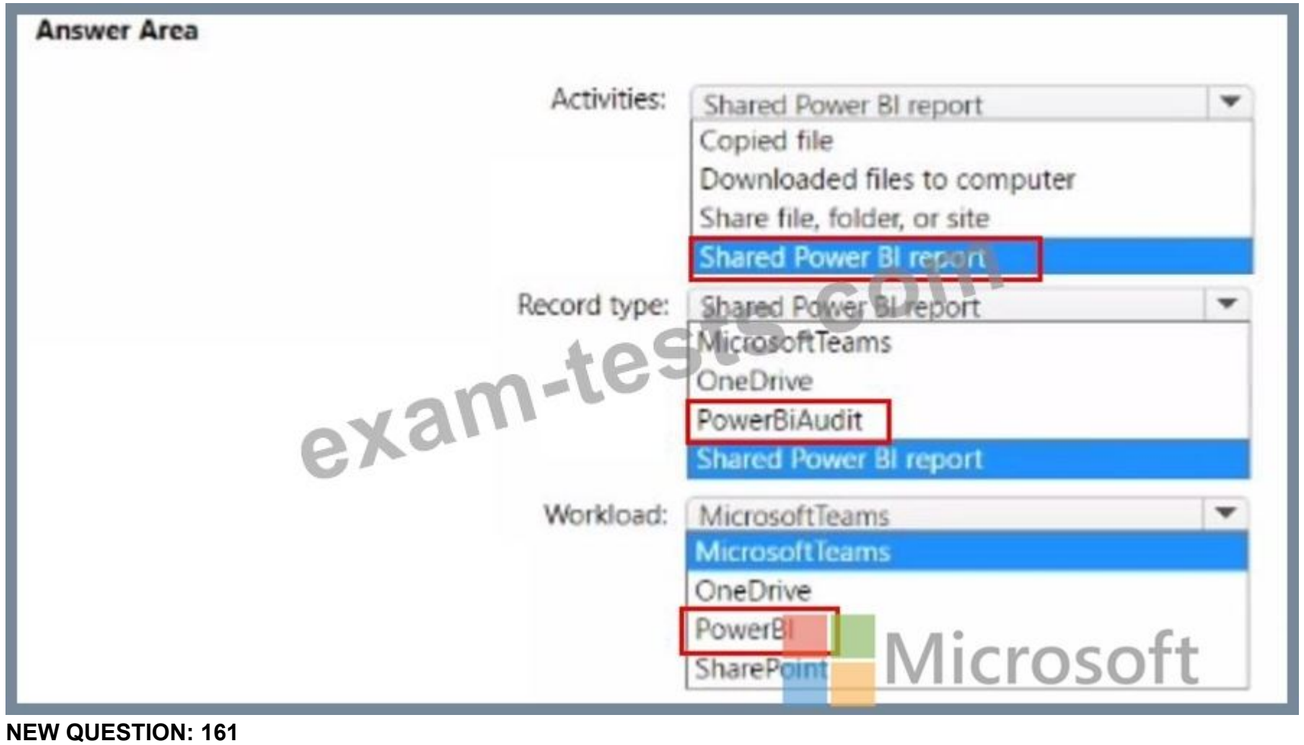
NEW QUESTION: 159
You have a Microsoft 365 E5 subscription that contains a database server named DB1. DB1 is onboarded to Microsoft Defender XDR.
You need to ensure that DB1 appears on the attack surface map.
What should you configure?
A. a sensitive entity tag
B. a honeytoken entity tag
C. an asset rule
D. a critical asset rule
Answer: D (LEAVE A REPLY)

NEW QUESTION: 160
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 identity which Power BI report file was shared.
How should you configure the search? To answer, select the appropriate options in the answer area.

Answer Area



Answer:



NEW QUESTION: 161

You need to visualize Azure Sentinel data and enrich the data by using third-party data sources to identify indicators of compromise (IoC).
What should you use?
A. notebooks in Azure Sentinel
B. Microsoft Cloud App Security
C. Azure Monitor
D. hunting queries in Azure Sentinel
Answer: A (LEAVE A REPLY)
According to Microsoft Sentinel documentation, notebooks integrate with Azure Machine Learning and Jupyter to allow advanced data visualization, enrichment, and correlation with third-party data sources.
Notebooks are used by security analysts and threat hunters to perform deep investigations by combining Sentinel data (such as logs, alerts, and incidents) with external threat intelligence feeds, indicators of compromise (IoCs), and custom datasets.
Microsoft describes notebooks as:
"A powerful tool built on Jupyter and Azure Machine Learning that allows you to use Python code to enrich Microsoft Sentinel data with external data sources, visualize data, and identify patterns and IoCs." They allow analysts to query, visualize, and correlate data interactively, going beyond the built-in dashboards and KQL-based analytics.
Thus, to visualize Sentinel data and enrich it with third-party IoC data, Notebooks in Azure Sentinel is the correct solution

NEW QUESTION: 162
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

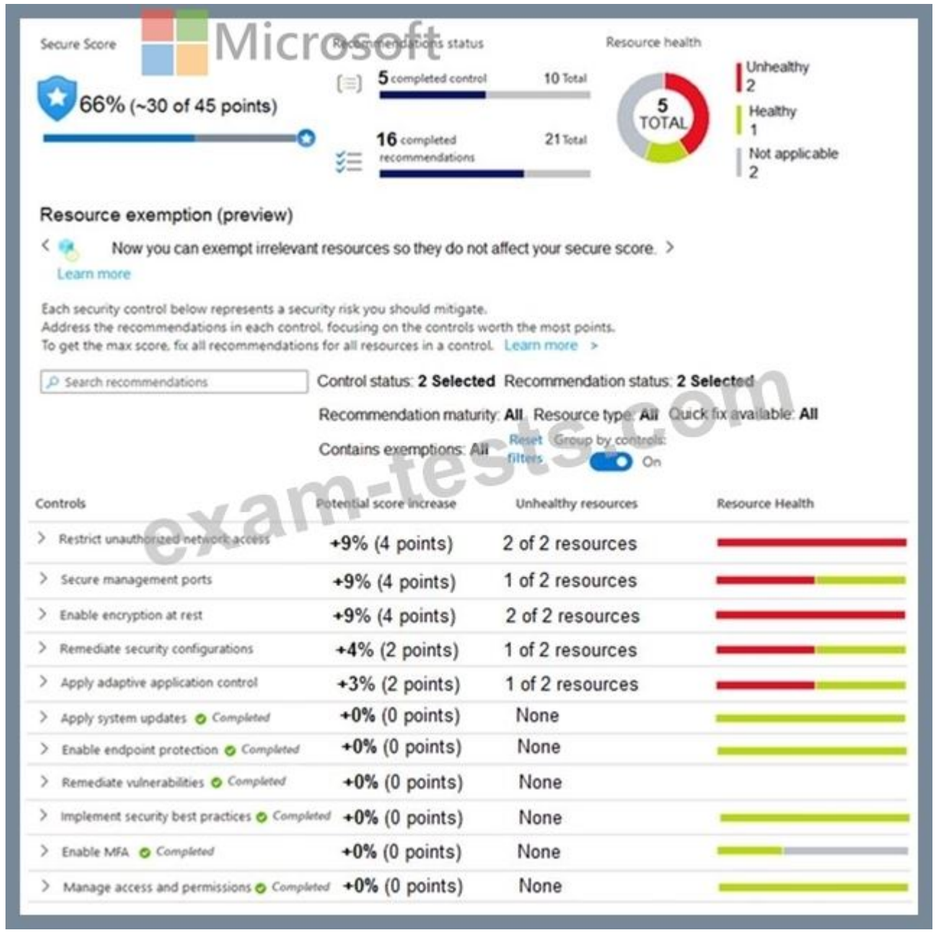
Answer:

Explanation:

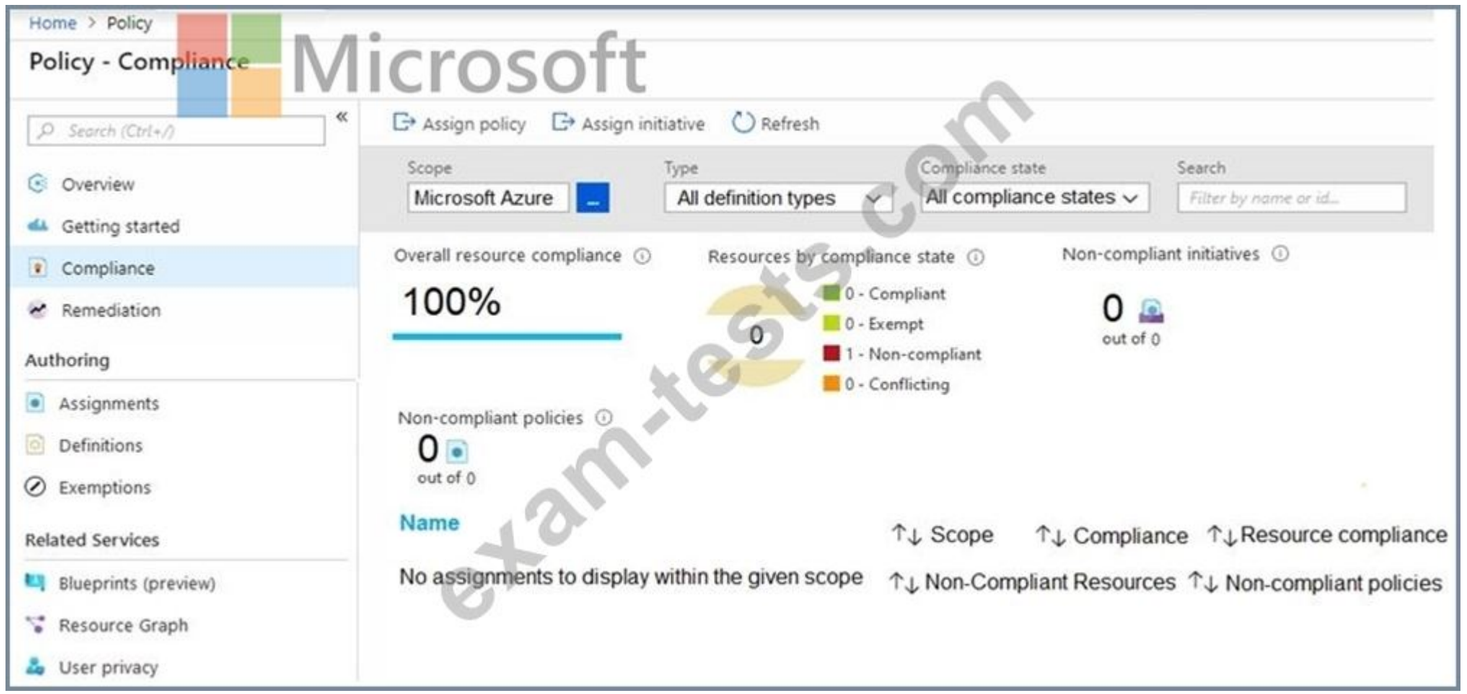
NEW QUESTION: 163

You manage the security posture of an Azure subscription that contains two virtual machines name vm1 and vm2.

The secure score in Azure Security Center is shown in the Security Center exhibit. (Click the Security Center tab.)



Azure Policy assignments are configured as shown in the Policies exhibit. (Click the Policies tab.)



For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

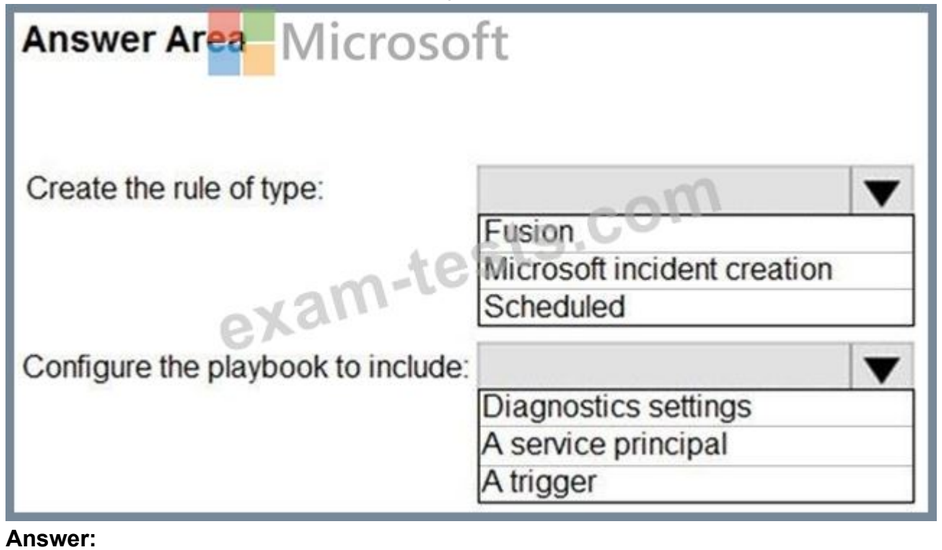
Answer Area

Statements	Yes	No
Both virtual machines have inbound rules that allow access from either Any or Internet ranges.	○	○
Both virtual machines have management ports exposed directly to the internet.	○	○
If you enable just-in-time network access controls on all virtual machines, you will increase the secure score by four point.	○	○

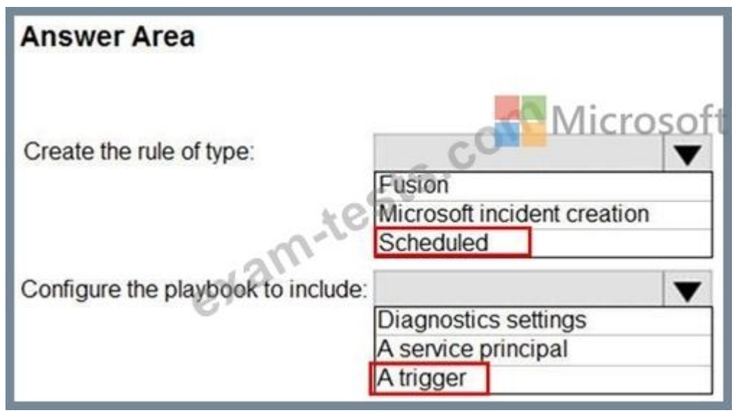
Answer:

Reference:
https://techcommunity.microsoft.com/t5/azure-security-center/security-control-restrict-unauthorized-network-access/ba-p/1593833
https://techcommunity.microsoft.com/t5/azure-security-center/security-control-secure-management-ports/ba-p/1505770

NEW QUESTION: 164
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:



NEW QUESTION: 165

You have a Microsoft 365 E5 subscription that uses Microsoft Copilot for Security. You plan to run the following code to create a custom Copilot for Security plugin.

```
<code segment>
SkillGroups:
- Format: <target>
Skills:
```

You need to specify a format and complete the code segment. Which format should you use for the <target> variable?

A. API

B. GPT

C. KQL

D. SQL

Answer: C (LEAVE A REPLY)

When authoring a custom plugin for Copilot for Security that queries security telemetry and returns structured results, the expected query/target format is Kusto Query Language (KQL). Copilot for Security integrates with Microsoft security data platforms (Microsoft Sentinel/Log Analytics and Defender tables) where investigative and hunting queries are expressed in KQL. Official plugin examples and guidance show the plugin invoking a KQL query against a workspace or a Defender table and returning the results in the plugin response payload. KQL is the language used to interrogate event, alert, and entity tables (for example, DeviceProcessEvents, SecurityAlert, MicrosoftGraphActivityLogs) and is the supported format when a plugin's purpose is to retrieve and return telemetry to Copilot for Security. Other formats listed (API, GPT, SQL) are not the standard query language for Defender/Sentinel data: APIs are endpoints for programmatic access, GPT is a model format, and SQL is not used for Azure Monitor / Sentinel tables. Therefore when the plugin's <target> must specify the query format against security telemetry, KQL is the correct choice.

NEW QUESTION: 166

You recently deployed Azure Sentinel.

You discover that the default Fusion rule does not generate any alerts. You verify that the rule is enabled.

You need to ensure that the Fusion rule can generate alerts.

What should you do?

A. Disable, and then enable the rule.

B. Add data connectors

C. Create a new machine learning analytics rule.

D. Add a hunting bookmark.

Answer: (SHOW ANSWER)

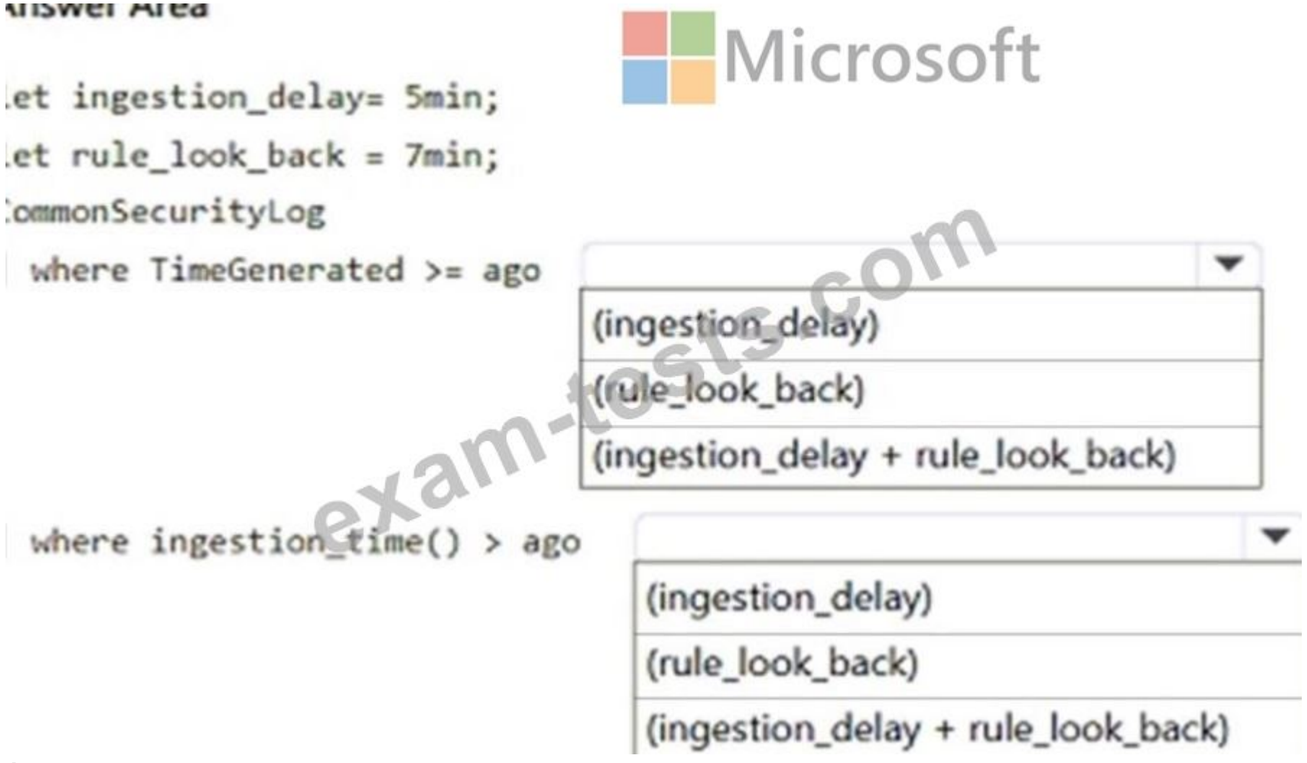
The built-in Fusion correlation rule in Microsoft Sentinel generates incidents only when it has sufficient telemetry from connected sources (e.g., Microsoft 365 Defender products, Azure AD sign-in logs, Cloud App, etc.). If no relevant data connectors are connected or sending data, Fusion will remain silent even if the rule is enabled. Connecting and authorizing the required data connectors provides the multi-signal input Fusion needs to produce incidents.

NEW QUESTION: 167
You need to visualize Azure Sentinel data and enrich the data by using third-party data sources to identify indicators of compromise (IoC).
What should you use?
A. notebooks in Azure Sentinel
B. Microsoft Cloud App Security
C. Azure Monitor
D. hunting queries in Azure Sentinel
Answer: A (LEAVE A REPLY)
Section: [none]
Explanation/Reference:
https://docs.microsoft.com/en-us/azure/sentinel/notebooks

NEW QUESTION: 168
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: (SHOW ANSWER)
According to Microsoft Entra (formerly Azure Active Directory) and Microsoft Security Operations documentation, when integrating Azure AD sign-in logs and audit logs with third-party SIEM systems, the supported and recommended method is to stream the logs to Azure Event Hubs through Diagnostic Settings
.
Event Hubs act as a real-time data ingestion service that can integrate directly with external SIEM tools such as Splunk, QRadar, ArcSight, or Sumo Logic. This allows for near real-time alerting and analysis of Azure AD sign-in events.
Official Microsoft guidance states:
"To integrate Azure AD logs with third-party SIEMs, configure Azure AD Diagnostic Settings to send sign-in and audit logs to Azure Event Hubs. Event Hubs can then stream the data to your SIEM for near real-time monitoring."
Other options do not meet the scenario's requirement:
* (A) and (C) involve Azure Sentinel, Microsoft's native SIEM solution. Since the question specifies a third-party SIEM, Sentinel is not required.
* (D) Archiving to a Storage account provides long-term retention and offline analysis but does not support near real-time alerting.
Therefore, the correct approach to route Azure AD sign-in events for near real-time monitoring in a third- party SIEM is to configure Azure AD Diagnostic Settings to stream logs to an Azure Event Hub.

Correct answer: B. Configure the Diagnostics settings in Azure AD to stream to an event hub

NEW QUESTION: 169
Hotspot Question
You have a Microsoft Sentinel workspace named Workspace1 that contains a table named CommonSecurityLog.
You ingest logs into CommonSecurityLog. CommonSecurityLog has an average log ingestion time of five minutes.
You need to create an analytics rule that has a lookback period of seven minutes and uses the data in the CommonSecurityLog table. The solution must meet the following requirements:
- Prevent the same event from being processed twice.
- Minimize the number of missed events due to log ingestion delays.
How should you complete the KQL query that defines the rule? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



Answer:

Answer Area

```
let ingestion_delay= 5min;
let rule_look_back = 7min;
CommonSecurityLog
| where TimeGenerated >= ago
```

(ingestion_delay)
(rule_look_back)
(ingestion_delay + rule_look_back)

```
| where ingestion_time() > ago
```

(ingestion_delay)
(rule_look_back)
(ingestion_delay + rule_look_back)

NEW QUESTION: 170
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.

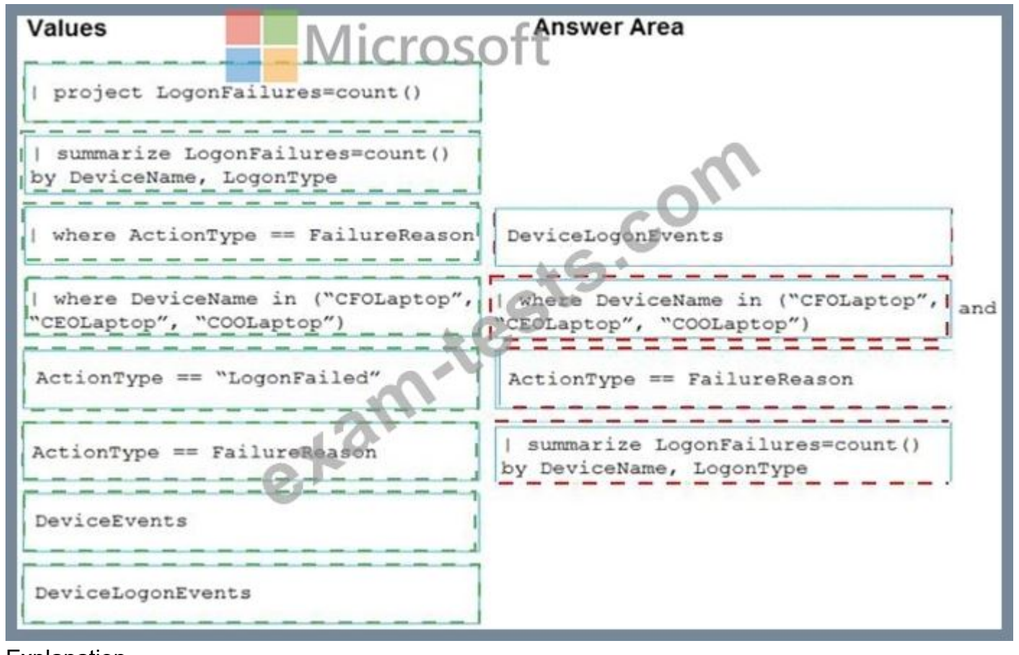
Answer:

Reference:
https://techcommunity.microsoft.com/t5/azure-security-center/suppression-rules-for-azure-security-center-alerts-are-now/ba-p/1404920

NEW QUESTION: 171
You are investigating an incident by using Microsoft 365 Defender.

You need to create an advanced hunting query to count failed sign-in authentications on three devices named CFOLaptop. CEOLaptop, and COOLaptop.
How should you complete the query? To answer, select the appropriate options in the answer area.
NOTE Each correct selection is worth one point

Answer:



Explanation

NEW QUESTION: 172
Hotspot Question
You have a Microsoft 365 subscription that uses Microsoft Defender XDR and has automatic attack disruption enabled.
During an active ransomware incident, Microsoft Defender for Endpoint automatically contains a device to limit lateral movement.
You need to use advanced hunting to return the following information:
- Devices that are contained due to response actions
- The most recent isolation state per device
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

```
DeviceEvents
| where ActionType == "IsolateDevice"
|  DeviceId, DeviceName, Timestamp, AdditionalFields
| extend IsolationStatus = tostring(AdditionalFields.IsolationStatus)
|  arg_max(Timestamp, *) by DeviceId, DeviceName
| where IsolationStatus == Isolated
| project DeviceName, DeviceId, Timestamp, IsolationStatus
| sort by Timestamp desc
```

- order
- project
- sort
- summarize
- take

Answer:

Answer Area

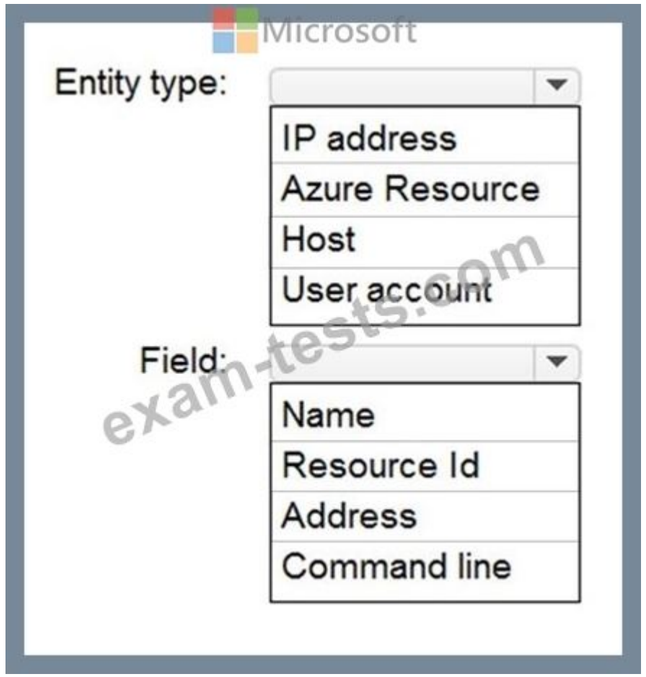
```
DeviceEvents
| where ActionType == "IsolateDevice"
|  DeviceId, DeviceName, Timestamp, AdditionalFields
| extend IsolationStatus = tostring(AdditionalFields.IsolationStatus)
|  arg_max(Timestamp, *) by DeviceId, DeviceName
| where IsolationStatus == Isolated
| project DeviceName, DeviceId, Timestamp, IsolationStatus
| sort by Timestamp desc
```

- order
- project
- sort
- summarize
- take

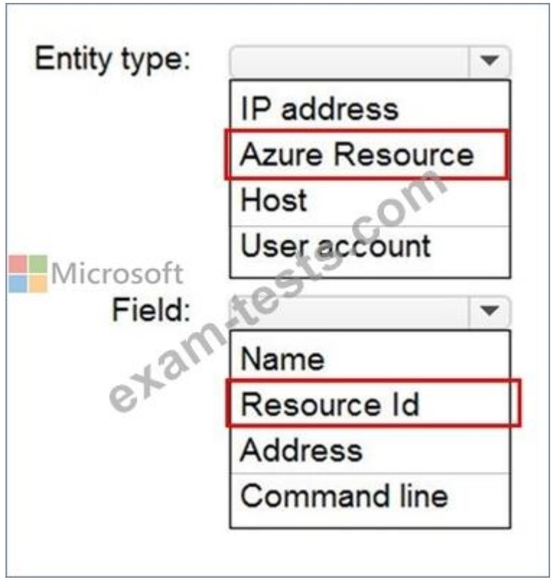
- order
- project
- sort
- summarize
- take

Explanation:
Box 1: project
The query needs to select specific columns (DeviceID, DeviceName, Timestamp, AdditionalFields) from the DeviceEvents table to pass to the next stage of the pipeline.
The project operator is used in KQL to select, rename, or extend columns in the result set.
Box 2: summarize
The query uses the aggregation function arg_max(Timestamp, *) grouped by unique identifiers (by DeviceId, DeviceName) to find the most recent isolation state record per device.
The summarize operator is the mandatory clause required to perform aggregations and group rows together in KQL.
Reference:
https://learn.microsoft.com/en-us/graph/api/resources/security-isolatedeviceresponseaction?view=graph-rest-beta

NEW QUESTION: 173
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.



Answer:



Reference:
https://techcommunity.microsoft.com/t5/azure-security-center/suppression-rules-for-azure-security-center-alerts-are-now/ba-p/1404920

NEW QUESTION: 174

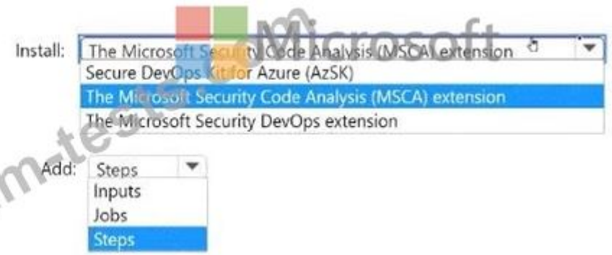
You have an Azure subscription that contains a Log Analytics workspace named Workspace1.
You configure Azure activity logs and Microsoft Entra ID logs to be forwarded to Workspace1.
You need to identify which Azure resources have been queried or modified by risky users.
How should you complete the KQL query? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Answer:

Explanation:

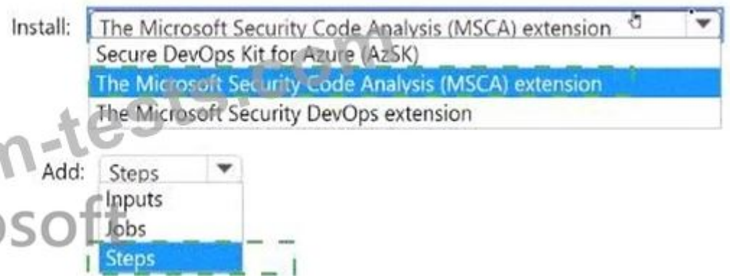
NEW QUESTION: 175
You have an Azure DevOps organization that uses Microsoft Defender for DevOps. The organization contains an Azure DevOps repository named Repo1 and an Azure Pipelines pipeline named Pipeline1.
Pipeline1 is used to build and deploy code stored in Repo1.
You need to ensure that when Pipeline1 runs, Microsoft Defender for Cloud can perform secret scanning of the code in Repo1.
What should you install in the organization, and what should you add to the YAML file of Pipeline"!? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Answer Area



Answer:

Answer Area



Explanation:

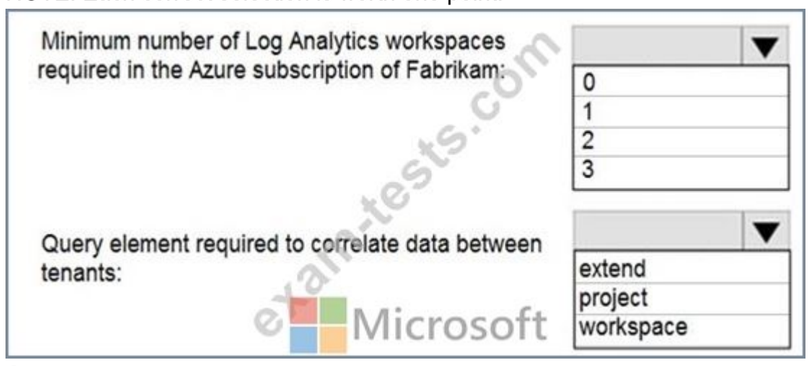
Answer Area

NEW QUESTION: 176

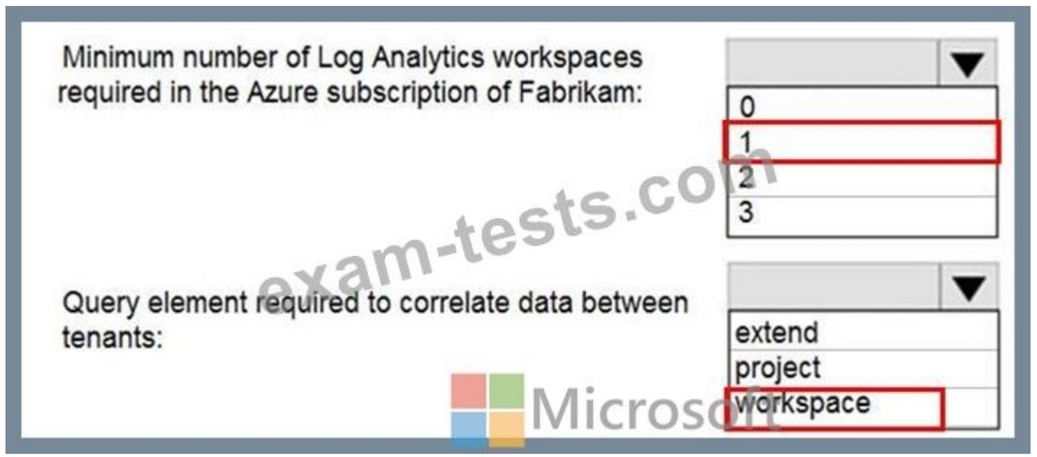
You need to implement Azure Sentinel queries for Contoso and Fabrikam to meet the technical requirements.

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:



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

Topic 1, Contoso Ltd

Overview

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

Overview

A company named Contoso Ltd. has a main office and five branch offices located throughout North America. The main office is in Seattle. The branch offices are in Toronto, Miami, Houston, Los Angeles, and Vancouver.

Contoso has a subsidiary named Fabrikam, Ltd. that has offices in New York and San Francisco.

Existing Environment

End-User Environment

All users at Contoso use Windows 10 devices. Each user is licensed for Microsoft 365. In addition, iOS devices are distributed to the members of the sales team at Contoso.

Cloud and Hybrid Infrastructure

All Contoso applications are deployed to Azure.

You enable Microsoft Cloud App Security.

Contoso and Fabrikam have different Azure Active Directory (Azure AD) tenants. Fabrikam recently purchased an Azure subscription and enabled Azure Defender for all supported resource types.

Current Problems

The security team at Contoso receives a large number of cybersecurity alerts. The security team spends too much time identifying which cybersecurity alerts are legitimate threats, and which are not.

The Contoso sales team uses only iOS devices. The sales team members exchange files with customers by using a variety of third-party tools. In the past, the sales team experienced various attacks on their devices.

The marketing team at Contoso has several Microsoft SharePoint Online sites for collaborating with external vendors. The marketing team has had several incidents in which vendors uploaded files that contain malware.

The executive team at Contoso suspects a security breach. The executive team requests that you identify which files had more than five activities during the past 48 hours, including data access, download, or deletion for Microsoft Cloud App Security-protected applications.
Requirements
Planned Changes
Contoso plans to integrate the security operations of both companies and manage all security operations centrally.
Technical Requirements
Contoso identifies the following technical requirements:
Receive alerts if an Azure virtual machine is under brute force attack.
Use Azure Sentinel to reduce organizational risk by rapidly remediating active attacks on the environment.
Implement Azure Sentinel queries that correlate data across the Azure AD tenants of Contoso and Fabrikam.
Develop a procedure to remediate Azure Defender for Key Vault alerts for Fabrikam in case of external attackers and a potential compromise of its own Azure AD applications.
Identify all cases of users who failed to sign in to an Azure resource for the first time from a given country. A junior security administrator provides you with the following incomplete query.
BehaviorAnalytics
| where ActivityType == "FailedLogOn"
| where _____ == True

NEW QUESTION: 177
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

Answer:

Actions

- From Workflow automation in Defender for Cloud, change the status of the workflow automati
- 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

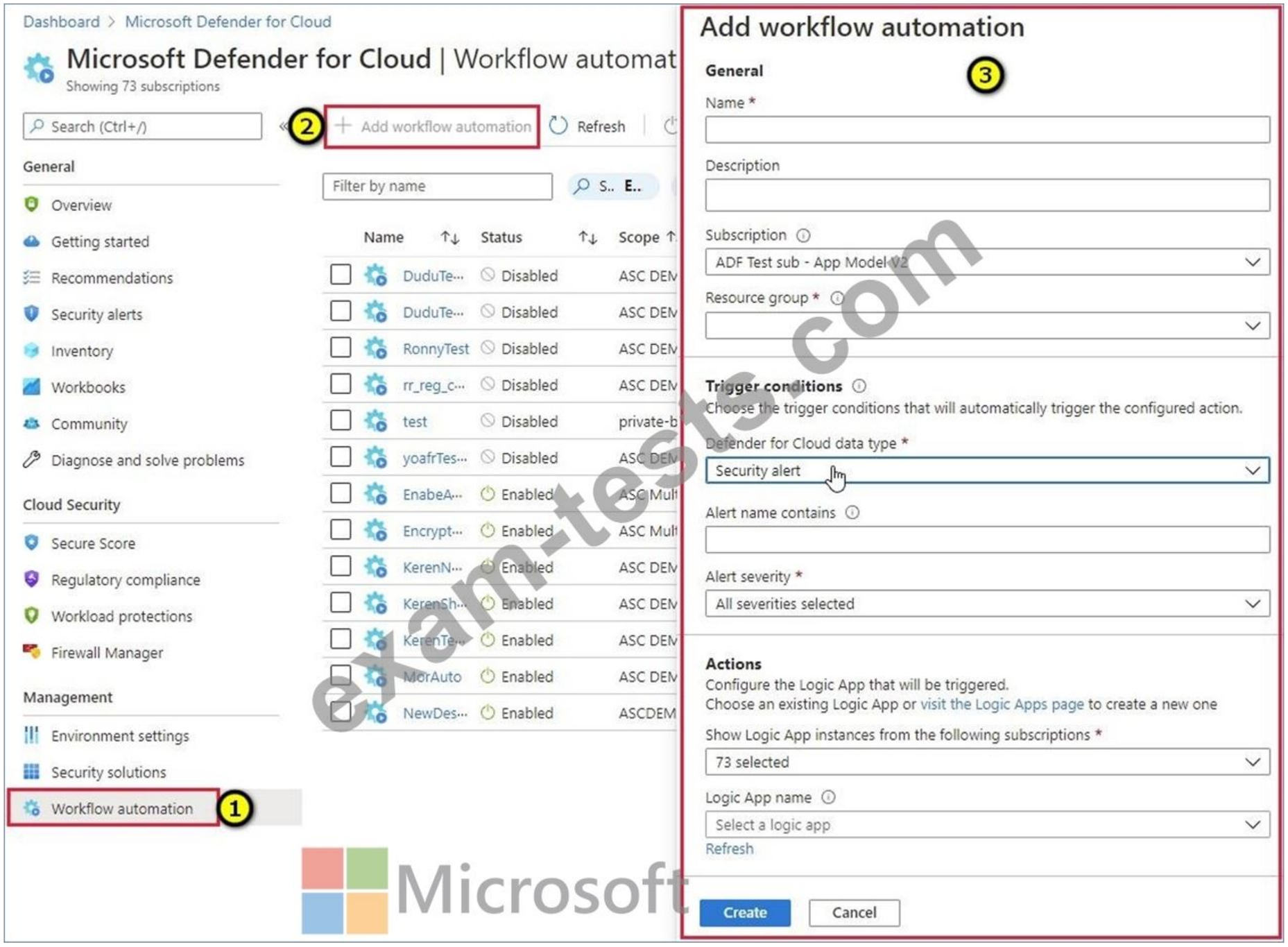
- From Logic App Designer, create a logic app.
- From Logic App Designer, run a trigger.
- From Workflow automation in Defender for Cloud, add a workflow automation.

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.



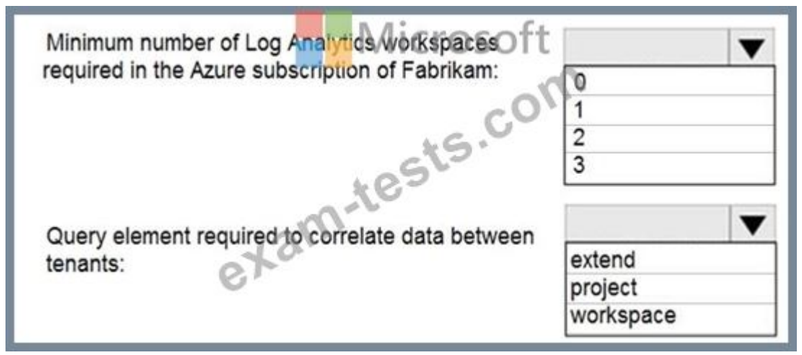
Here you can enter:

A name and description for the automation.

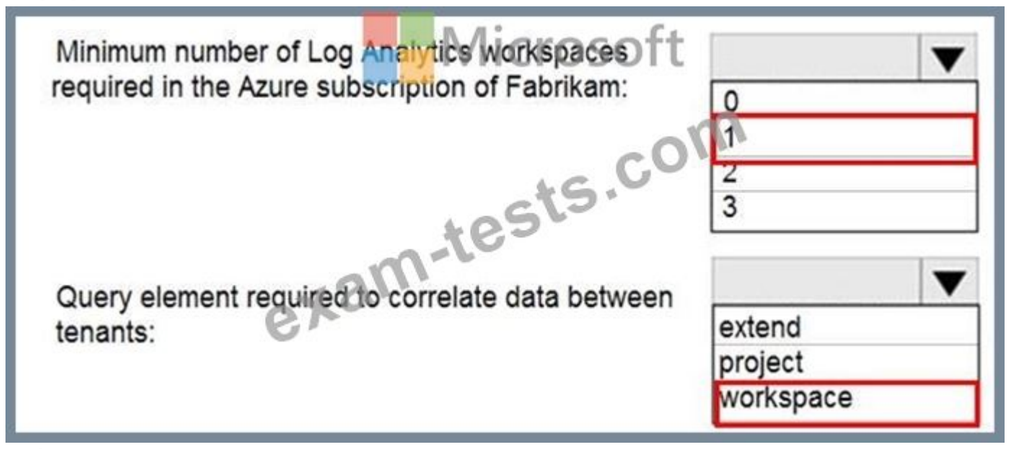
The triggers that will initiate this automatic workflow. For example, you might want your Logic App to run when a security alert that contains "SQL" is generated.
The Logic App that will run when your trigger conditions are met.
3. From the Actions section, select visit the Logic Apps page to begin the 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.

Reference: https://docs.microsoft.com/en-us/azure/defender-for-cloud/workflow-automation

NEW QUESTION: 178
You need to implement Azure 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:



Reference:

https://docs.microsoft.com/en-us/azure/sentinel/extend-sentinel-across-workspaces-tenants This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

Overview

Litware Inc. is a renewable company.

Litware has offices in Boston and Seattle. Litware also has remote users located across the United States. To access Litware resources, including cloud resources, the remote users establish a VPN connection to either office.

NEW QUESTION: 179

Hotspot Question

You have a Microsoft Sentinel workspace that is connected to the Microsoft Sentinel data lake.
Newly ingested data can take up to 15 minutes to become queryable in the data lake.
You need to schedule a KQL job that runs daily at 12:10 AM and populates a summary table used by threat hunters. The solution must meet the following requirements:
- Each run must query a fixed 24-hour window that ends 15 minutes
before the job runtime.
- Double-counting must be prevented across the daily runs.
- late-arriving records must be included in the summary.
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

```
let lookback = 1d;
let delay = 15m;
let endTime = [ now() + delay; | now() – delay; | now() – lookback; ]
let startTime = [ endTime – lookback; | ago(lookback); | endTime + lookback; | endTime – lookback; ]
SignInLogs
| where TimeGenerated between (startTime .. endTime)
| summarize SigninCount=count() by UserPrincipalName
| project UserPrincipalName, SigninCount
```


Answer:

Answer Area

```
let lookback = 1d;
let delay = 15m;
let endTime =
let startTime =
SignInLogs
| where TimeGenerated between (startTime .. endTime)
| summarize SigninCount=count() by UserPrincipalName
| project UserPrincipalName, SigninCount
```

now() + delay;
now() – delay;
now() – lookback;

endTime – lookback;
ago(lookback);
endTime + lookback;
endTime – lookback;

NEW QUESTION: 180
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 machines.
B. Add the device users to the admin role.
C. Create a new device group that has a rank of 4.
D. Create a new admin role.
E. Create a new device group that has a rank of 1.
F. Add a tag to the device group.
Answer: (SHOW ANSWER)

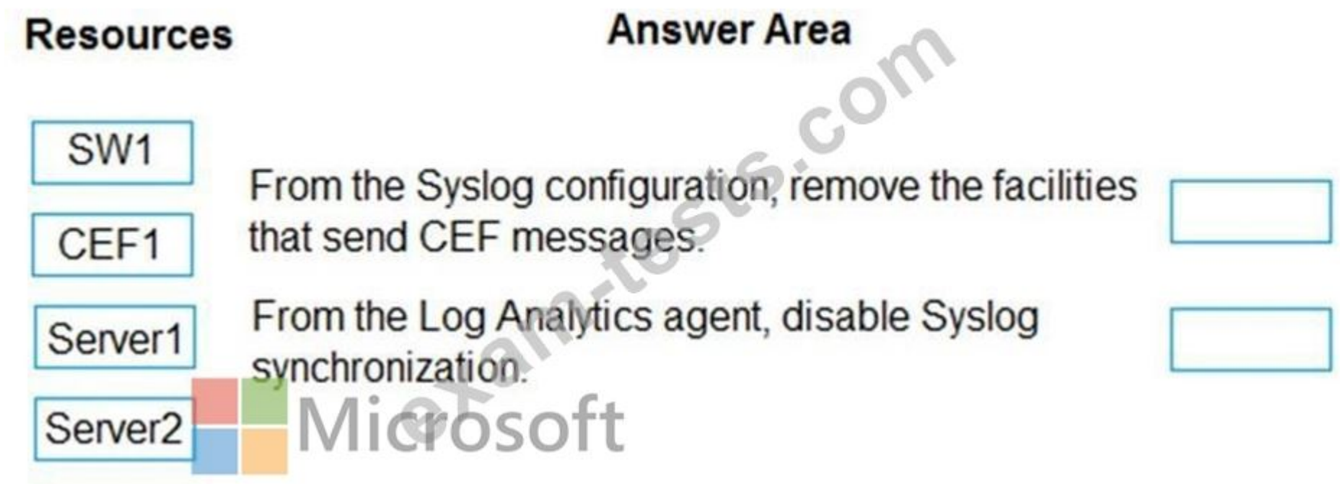
NEW QUESTION: 181
Drag and Drop Question
You have the resources shown in the following table.

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

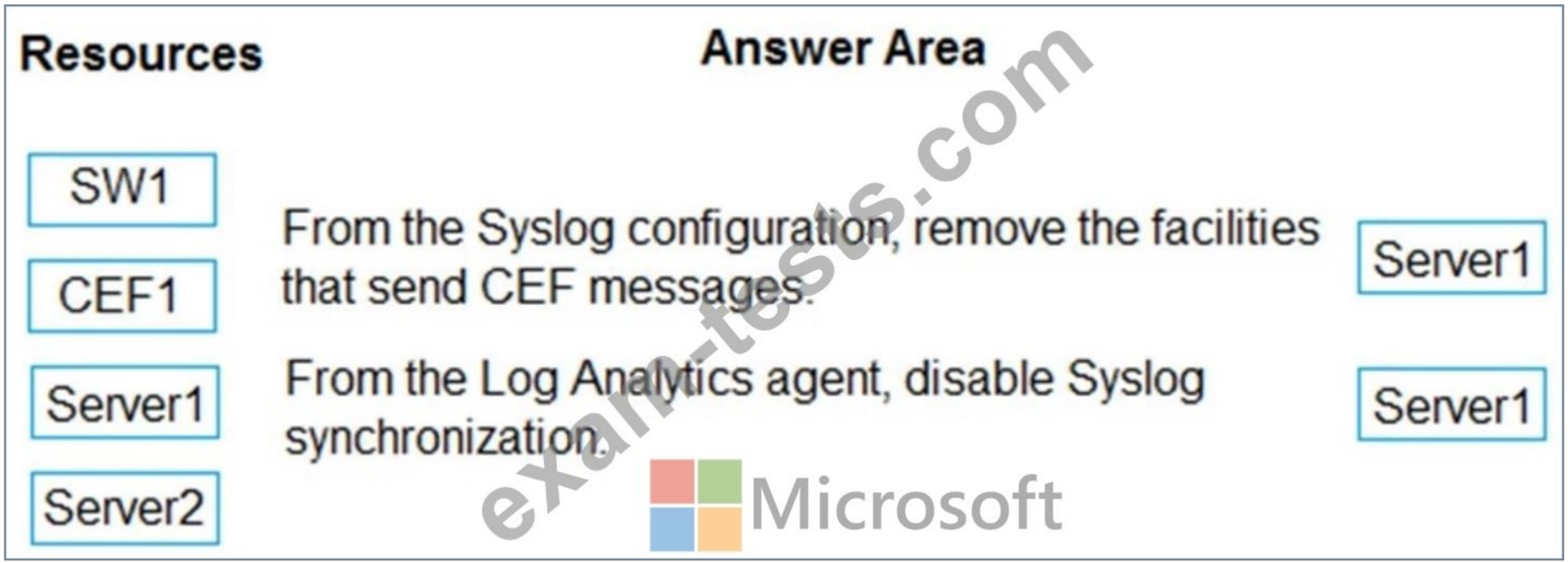
You need to prevent duplicate events from occurring in SW1.

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.



Answer:



Explanation:
Box 1: Server1
On each source machine that sends logs to the forwarder in CEF format (SERVER1), you must edit the Syslog configuration file to remove the facilities that are being used to send CEF messages. This way, the facilities that are sent in CEF won't also be sent in Syslog.
Box 2: Server1
You must run the following command on those machines (the ones you ran it previously, i.e SERVER1) to disable the synchronization of the agent with the Syslog configuration in Microsoft Sentinel. This ensures that the configuration change you made in the previous step does not get overwritten Reference:
https://docs.microsoft.com/en-us/azure/sentinel/connect-log-forwarder?tabs=rsyslog#run-the- deployment-script

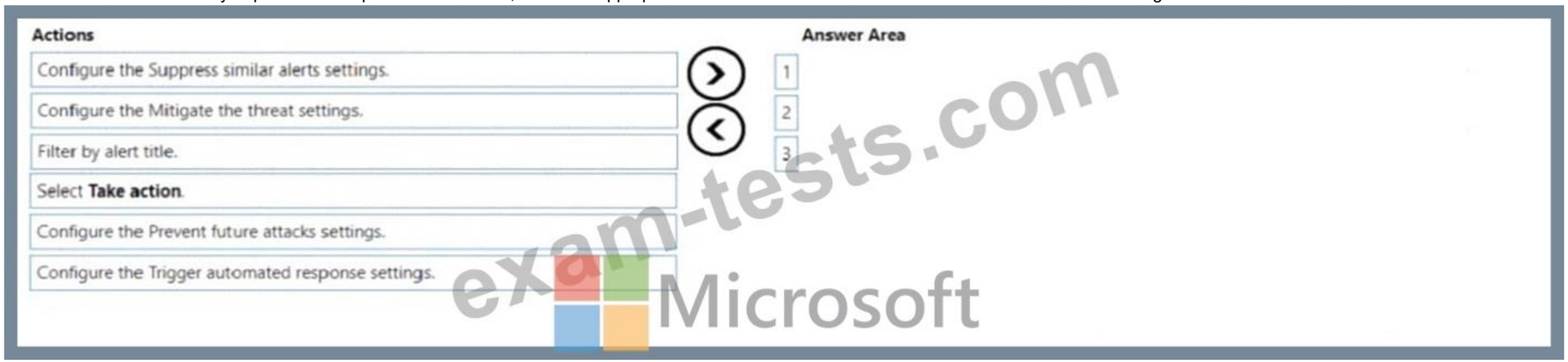
NEW QUESTION: 182
You have a Microsoft subscription that has Microsoft Defender for Cloud enabled You configure the Azure logic apps shown in the following table.

Name	Trigger	Action
LogicApp1	When a Defender for Cloud recommendation is created or triggered	Send an email
LogicApp2	When a Defender for Cloud alert is created or triggered	Send an email

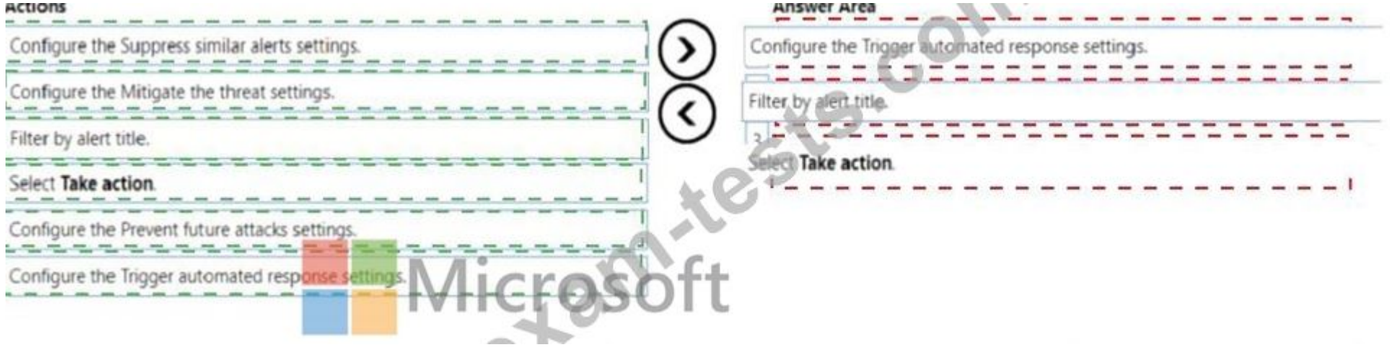
You need to configure an automatic action that will run if a Suspicious process executed alert is triggered.

The solution must minimize administrative effort.

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.



Answer:



Explanation:

A. Configure the Trigger automated response settings in the Azure Security Center or Azure Logic App,

B. Filter by alert title (e.g. "Suspicious process executed").

C. Select "Take action" (e.g. "Mitigate the threat").

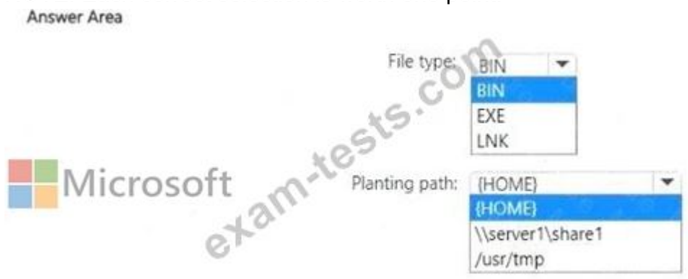
NEW QUESTION: 183

You have a Microsoft 365 E5 subscription that contains Windows 11 and Linux CentOS devices.

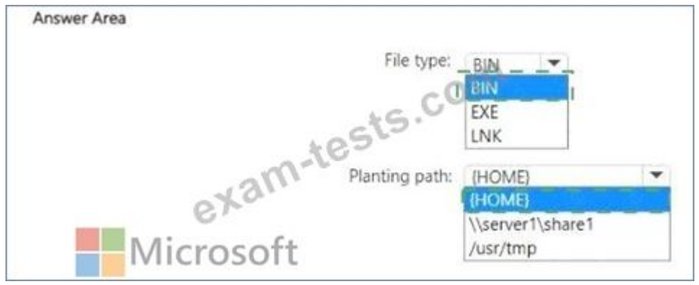
In Microsoft Defender XDR, Deception is set to On.

You plan to create a deception rule that will use a custom lure.

You need to specify the type of file, and the planting path for for the custom lure, What should you specify? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

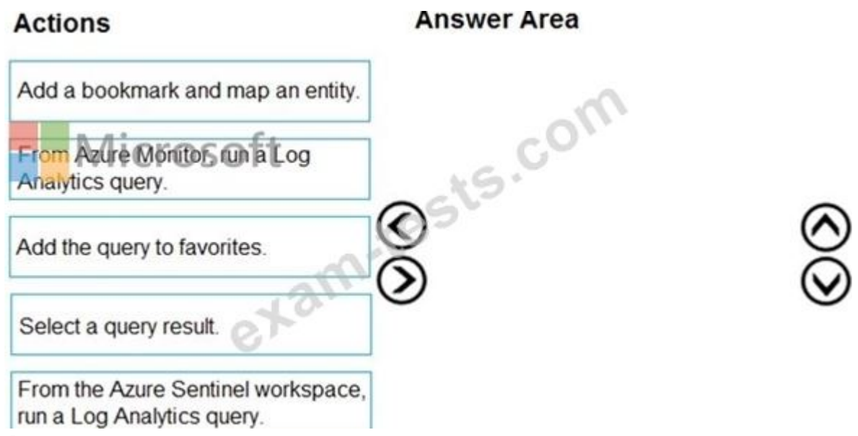


Answer:

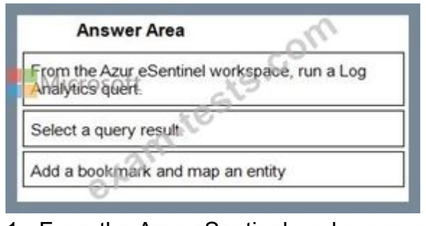


Explanation:

NEW QUESTION: 184
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.



Answer:



1 - From the Azur eSentinel workspace, run a Log Analytics quert.
2 - Select a query result.
3 - Add a bookmark and map an entity
Reference:
https://docs.microsoft.com/en-us/azure/sentinel/bookmarks

NEW QUESTION: 185
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: A,B (LEAVE A REPLY)
Explanation (concise): To send a Microsoft Teams message when a suspicious sign-in is detected, create a playbook (Logic App) that posts to Teams (A) and associate the playbook so it runs when the corresponding alert/incident is created (B)-typically via an automation rule or by attaching the playbook to the analytics rule/incident. Entity behavior analytics, workbooks, or Fusion aren't required for sending Teams notifications.

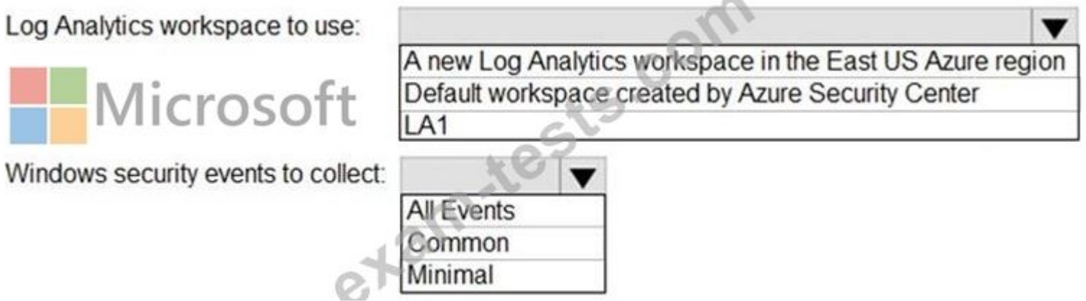
NEW QUESTION: 186
You have a playbook in Azure Sentinel.
When you trigger the playbook, it sends an email to a distribution group.

You need to modify the playbook to send the email to the owner of the resource instead of the distribution group.
What should you do?
A. Add a parameter and modify the trigger.
B. Add a custom data connector and modify the trigger.
C. Add a condition and modify the action.
D. Add a parameter and modify the action.
Answer: D (LEAVE A REPLY)
You need to add a new parameter in Send email action. That parameter specifies who you want to send to.
https://docs.microsoft.com/en-us/azure/sentinel/tutorial-respond-threats-playbook#run-a-playbook-on-demand

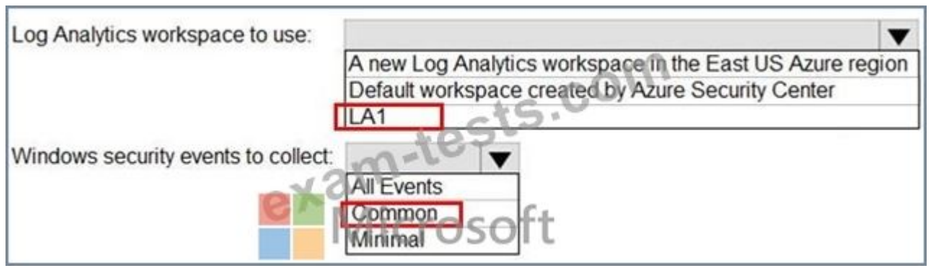
NEW QUESTION: 187
You have a Microsoft Sentinel workspace that uses the Microsoft 365 Defender data connector.
From Microsoft Sentinel, you investigate a Microsoft 365 incident.
You need to update the incident to include an alert generated by Microsoft Defender for Cloud Apps.
What should you use?
A. the investigation graph on the Incidents page of Microsoft Sentinel
B. the entity side panel of the Timeline card in Microsoft Sentinel
C. the Timeline tab on the Incidents page of Microsoft Sentinel
D. the Alerts page in the Microsoft 365 Defender portal
Answer: B (LEAVE A REPLY)

NEW QUESTION: 188
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. create a KQL query that will i create a KQL query that will i NOTE: Each correct selection is worth one point.
A. Create custom rule based on the Office 365 connector templates.
B. Create a Microsoft incident creation rule based on Azure Security Center.
C. Create a Microsoft Cloud App Security connector.
D. Create an Azure AD Identity Protection connector.
Answer: (SHOW ANSWER)
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: 189
You need to implement Azure Defender to meet the Azure Defender 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:



NEW QUESTION: 190

You have the following advanced hunting query in Microsoft 365 Defender.

```
DeviceProcessEvents
| where Timestamp > ago (24h)
and InitiatingProcessFileName =~ 'runsll32.exe'
and InitiatingProcessCommandLine !contains " " and InitiatingProcessCommandLine != ""
and FileName in~ ('schtasks.exe')
and ProcessCommandLine has 'Change' and ProcessCommandLine has 'SystemRestore'
and ProcessCommandLine has 'disable'
| project Timestamp, AccountName, ProcessCommandLine
```

You need to receive an alert when any process disables System Restore on a device managed by Microsoft Defender during the last 24 hours.

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 detection rule.

B. Create a suppression rule.

C. Add | order by Timestamp to the query.

D. Block DeviceProcessEvents with DeviceNetworkEvents.

E. Add DeviceId and ReportId to the output of the query.

Answer: A,E (LEAVE A REPLY)

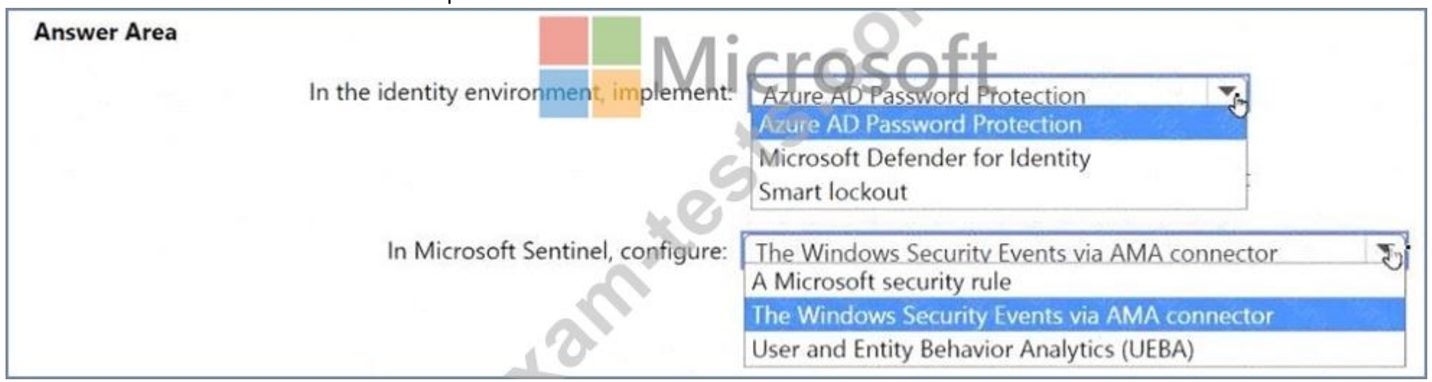
In Microsoft 365 Defender advanced hunting, if you want to automatically receive alerts based on a KQL query-such as detecting when a process disables System Restore-you must convert that query into a custom detection rule . According to Microsoft's official documentation, custom detection rules "run hunting queries on a schedule and create alerts and incidents when results are found." In order for the detection rule to function properly and correlate results across devices and incidents, the query must output DeviceId and ReportId . These fields are mandatory for any advanced hunting query that you want to convert into a detection rule be cause they uniquely identify the device and event instance. Without them, the rule cannot properly generate correlated alerts.

Therefore:

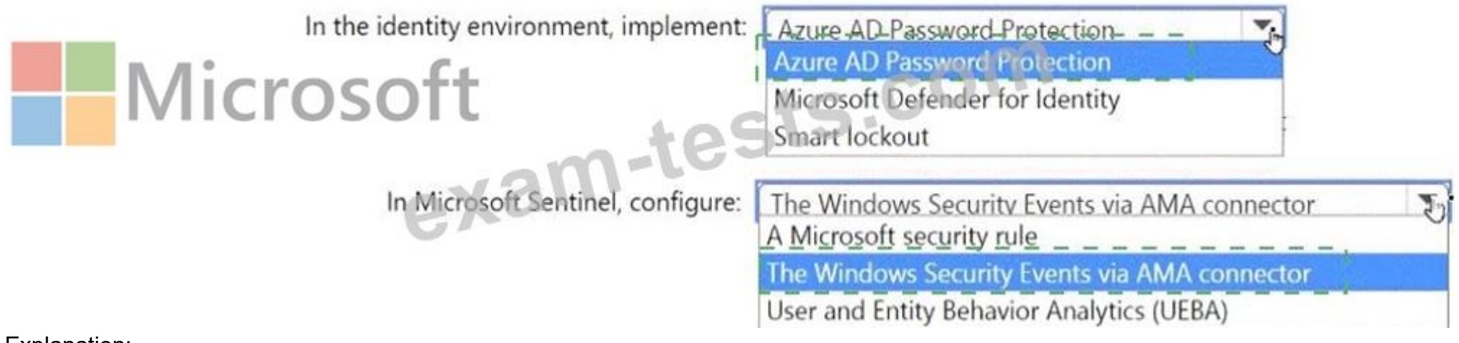
* Create a detection rule (A) - ensures the query runs automatically and alerts are generated.

* Add DeviceId and ReportId (E) - required for detection rule creation and accurate device/event correlation.
Other options are incorrect:
* Suppression rule (B) filters alerts, not generate them.
* Order by Timestamp (C) is optional for display, not alerting.
* DeviceNetworkEvents (D) is unrelated to this process query.

NEW QUESTION: 191
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:



Explanation:

NEW QUESTION: 192
You have an Azure subscription.
You need to delegate permissions to meet the following requirements:
* Enable and disable advanced features of Microsoft Defender for Cloud.
* Apply security recommendations to a resource.
The solution must use the principle of least privilege.
Which Microsoft Defender for Cloud role should you use for each requirement? To answer, drag the appropriate roles to the correct requirements. Each role may be used once, mote 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.

Answer:

Explanation:

NEW QUESTION: 193
You have a Microsoft 365 E5 subscription that uses Microsoft Defender XDR.
You have a Microsoft Sentinel workspace.

Microsoft Sentinel connectors are configured as shown in the following table.

Connector	Collected log
Microsoft Entra ID	• Audit logs • Microsoft Graph activity logs
Microsoft 365	• Microsoft Exchange Online • Microsoft SharePoint Online • Microsoft Teams

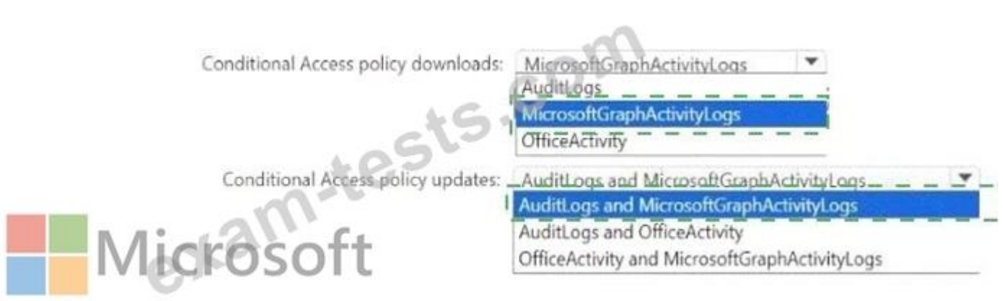
You use Microsoft Sentinel to investigate suspicious Microsoft Graph API activity related to Conditional Access policies. You need to search for the following activities:

* Downloads of the Conditional Access policies by using PowerShell

* Updates to the Conditional Access policies by using the Microsoft Entra admin center Which tables should you query for each activity? lo answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer:



Explanation:

For Conditional Access investigations in Microsoft Sentinel, the data source depends on the control plane used. When policies are downloaded via PowerShell , the cmdlets call the Microsoft Graph (e.g., Get-MgIdentityConditionalAccessPol icy). Those Graph requests are captured by the Microsoft Graph Activity Logs connector and land in the MicrosoftGraphActivityLogs table. This table records the app identity (such as PowerShell/Graph SDK), the API path (like /identity/conditionalAccess/policies), verb (GET), and result, which is ideal for spotting bulk reads/exports of policy definitions.

When policies are updated in the Microsoft Entra admin center , two streams provide visibility. First, directory auditing writes change events (create/update/delete of Conditional Access policies) to Microsoft Entra Audit logs , surfaced in Sentinel as the AuditLogs table, including the actor, target policy, operation (Update policy), and result. Second, the Entra admin center itself is a first-party application that performs the update by invoking Microsoft Graph ; those API calls are also recorded in MicrosoftGraphActivityLogs (with verb PATCH/POST and the policy resource path).

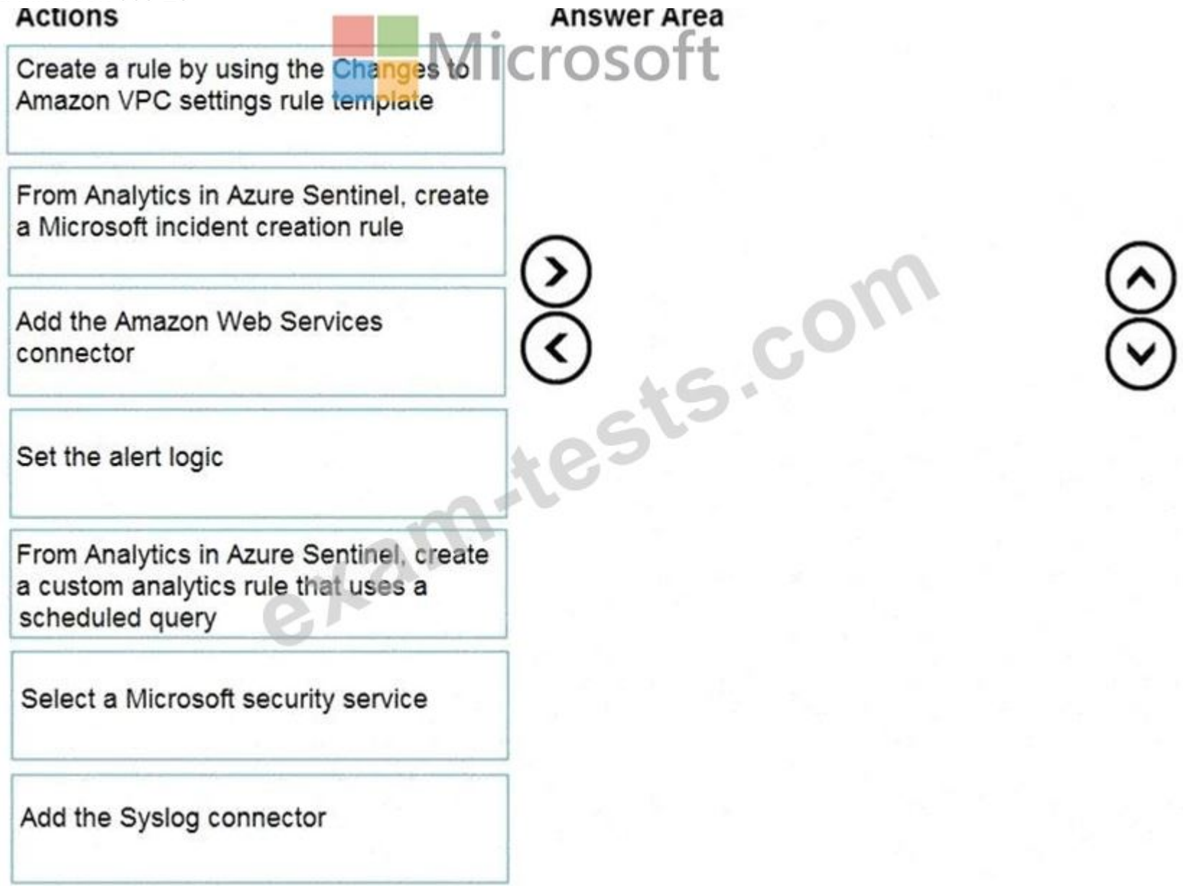
Therefore, to cover both perspectives- the authoritative audit record and the underlying API activity - you should query AuditLogs and MicrosoftGraphActivityLogs for updates, and MicrosoftGraphActivityLogs for downloads executed through PowerShell.

NEW QUESTION: 194

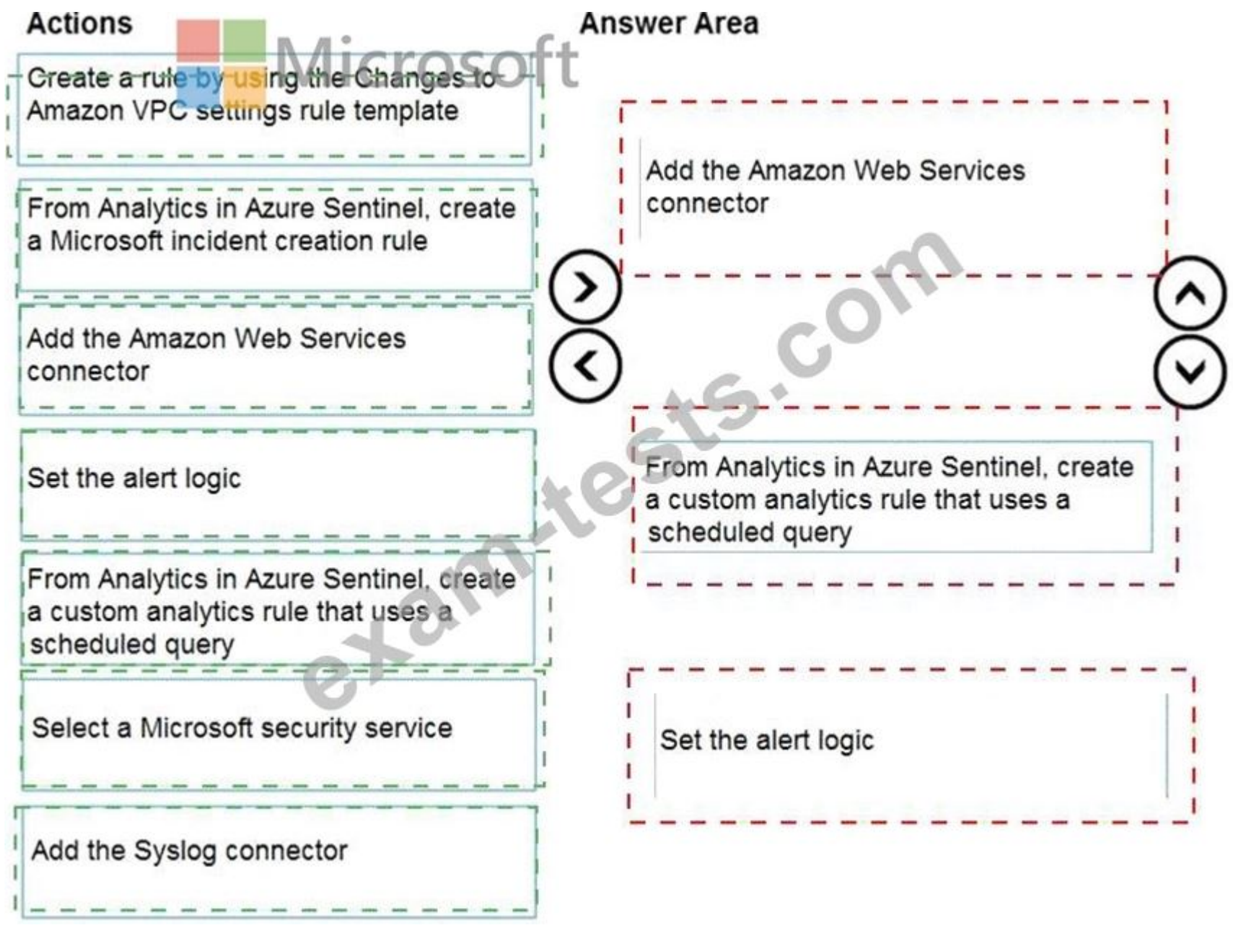
You need to use an Azure Sentinel analytics rule to search for specific criteria in Amazon Web Services (AWS) logs and to generate incidents.

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



Answer:



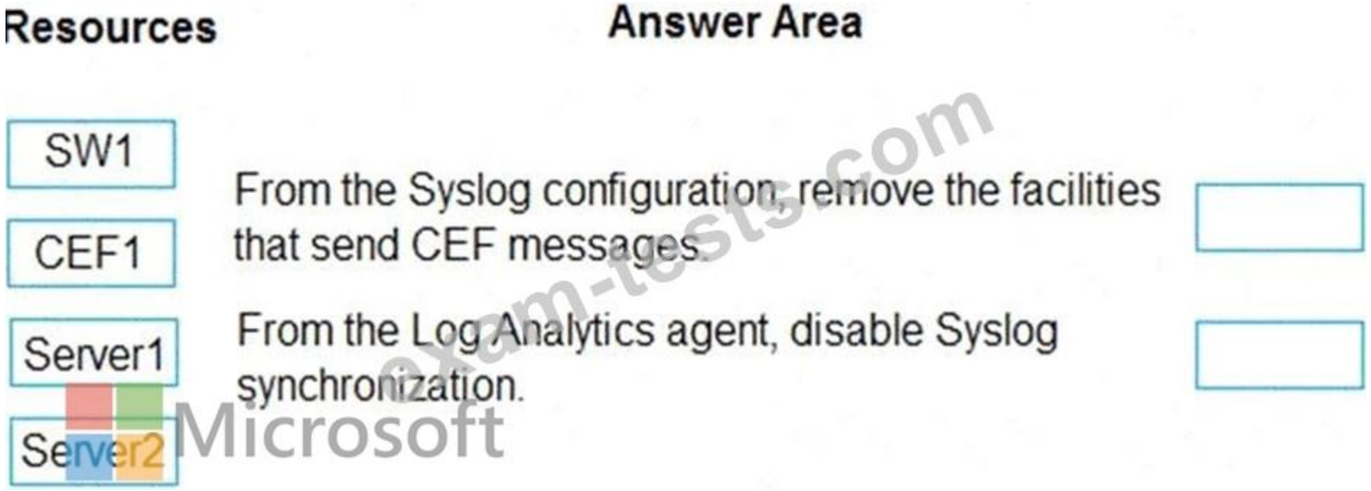
Explanation:

Comprehensive and Detailed Explanation with all Microsoft Security Operations (SecOps) documents :
=
To search for specific criteria in Amazon Web Services (AWS) logs and generate incidents using Microsoft Sentinel , the configuration process follows a structured sequence according to Microsoft Sentin el documentation and the Azure Sentinel playbook for AWS integration.
* Add the Amazon Web Services (AWS) connector
* Before Sentinel can analyze AWS data, you must integrate AWS logs using the Amazon Web Services data connector . This connector streams AWS Clo udTrail and other AWS log data into your Sentinel workspace. Microsoft's documentation states: "Use the Amazon Web Services (AWS) connector to stream CloudTrail events and security logs into Microsoft Sentinel for analysis and alerting."
* Without this conne ctor, Sentinel cannot query or detect AWS-specific activities.
* Create a custom analytics rule that uses a scheduled query
* Once data ingestion is established, you create an analytics rule in Sentinel using a scheduled query to continuously search for specif ic conditions (e.g., unauthorized access attempts, changes to VPC settings, etc.).
* Microsoft specifies: "Custom analytics rules run KQL queries on a schedule to detect specific patterns or anomalies across ingested data sources."
* Set the alert logic
* After defining your rule, you configure the alert logic to determine when Sentinel should trigger an alert or incident. This includes setting thresholds, event frequency, severity levels, and entity mappings.
* Microsoft Sentinel's official guidance notes: "Alert logic defines the conditions under which an alert is generated from the query results."

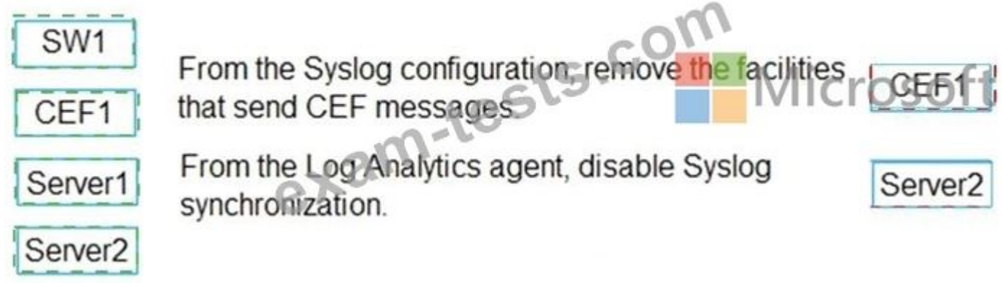
NEW QUESTION: 195
You have the resources shown in the following table.

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.



Answer:



Explanation:

| From the Syslog configuration, remove the facilities that send CEF messages. | CEF1 | | From the Log Analytics agent, disable Syslog synchronization. | Server2 | The goal is to eliminate duplicate events in the Azure Sentinel workspace (SW1). Duplication typically occurs when the same log source is sending data to Azure Sentinel via multiple collection methods.

Analysis of the Environment

* SW1 is the Azure Sentinel (now Microsoft Sentinel) workspace, which is the final destination for all logs.
* CEF1 is a Linux server configured as a log forwarder (often called a CEF collector) for Microsoft Sentinel. It uses the Log Analytics agent (or the newer Azure Monitor Agent) to ingest logs and is specifically configured to forward Common Event Format (CEF) logs to SW1.
* Server1 sends CEF logs to CEF1. This is the intended, single collection path for Server1's CEF logs:

Server1 CEF1 SW1. No duplication is inherent here.

* Server2 sends Syslog logs to CEF1. This path is: Server2 CEF1 SW1.
* Since CEF1 is running the Log Analytics agent (required to forward logs to SW1) and is configured to collect Syslog data (to receive Server2's logs), the Log Analytics agent on CEF1 will also attempt to ingest the Syslog messages it receives into SW1.
* However, the Log Analytics agent itself can also be used to collect Syslog/CEF logs directly from the source server.

Addressing Duplication

Duplication is most likely to occur if a server is sending the same logs to a forwarder AND also has the Log Analytics agent configured to send the same logs directly to SW1.

Action 1: From the Syslog configuration, remove the facilities that send CEF messages.

* Resource: CEF1
* Reasoning: CEF1 is a Linux server running the Log Analytics agent and is acting as the collector.
Server1 sends CEF logs to CEF1. These CEF logs are transmitted using Syslog (specifically, a custom Syslog format). If the Log Analytics agent on CEF1 is configured to collect all Syslog facilities, it will ingest the raw CEF Syslog messages it receives from Server1 AND also ingest the parsed CEF messages via its custom forwarding logic. To prevent the Syslog collector on CEF1 from ingesting the raw CEF messages that it is supposed to be forwarding, you must modify its Syslog configuration (e.g., in /etc/rsyslog.conf or equivalent) to ignore the facilities/log files used by the incoming CEF messages from Server1. The primary purpose of CEF1 is to receive and forward CEF, not to have its Log Analytics agent ingest the raw Syslog that transports the CEF payload.
Action 2: From the Log Analytics agent, disable Syslog synchronization.
* Resource: Server2
* Reasoning: Server2 is configured to send Syslog logs to CEF1 (Server2 CEF1 SW1). Since Server2 is a Linux server, it may also have the Log Analytics agent installed for other monitoring purposes. If the Log Analytics agent on Server2 is installed, it is configured by default to collect Syslog logs directly and send them to SW1 (Server2 SW1). This creates a duplicate path for the Syslog data:
* Path A (Intended): Server2 Syslog CEF1 SW1
* Path B (Duplication): Server2 Log Analytics Agent Syslog SW1
* According to Microsoft Sentinel documentation on log ingestion, when using a dedicated forwarder (like CEF1) for Syslog/CEF, you must disable the Syslog collection on the Log Analytics agent of the source machine (Server2) to prevent this duplication. This is typically done by disabling Syslog synchronization in the Log Analytics agent configuration or removing the Syslog entry from the agent's data sources.
References: Microsoft Sentinel documentation on data connectors for Syslog and CEF, specifically the sections discussing the deployment of the Log Analytics agent and forwarders, which repeatedly warn about the need to prevent dual-ingestion of the same log type (Syslog or CEF) from both the source server's agent and a dedicated collector/forwarder.

NEW QUESTION: 196
You have a Microsoft Sentinel workspace that contains a custom workbook.
You need to query for a summary of security events. The solution must meet the following requirements:
* Identify the number of security events ingested during the past week.
* Display the count of events by day in a chart.
How should you complete the query? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

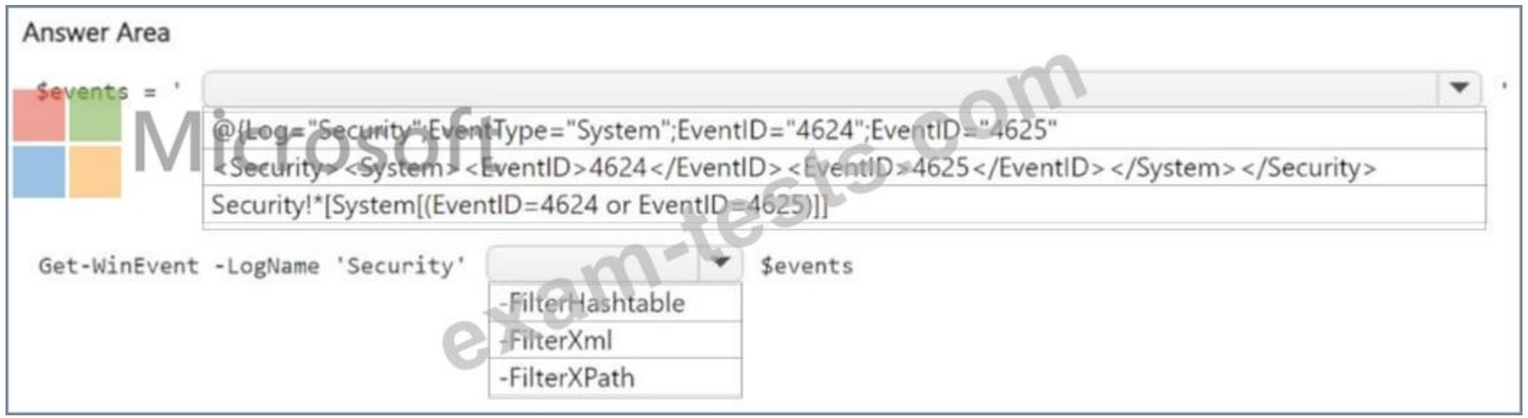
Answer:
Answer Area

Explanation:

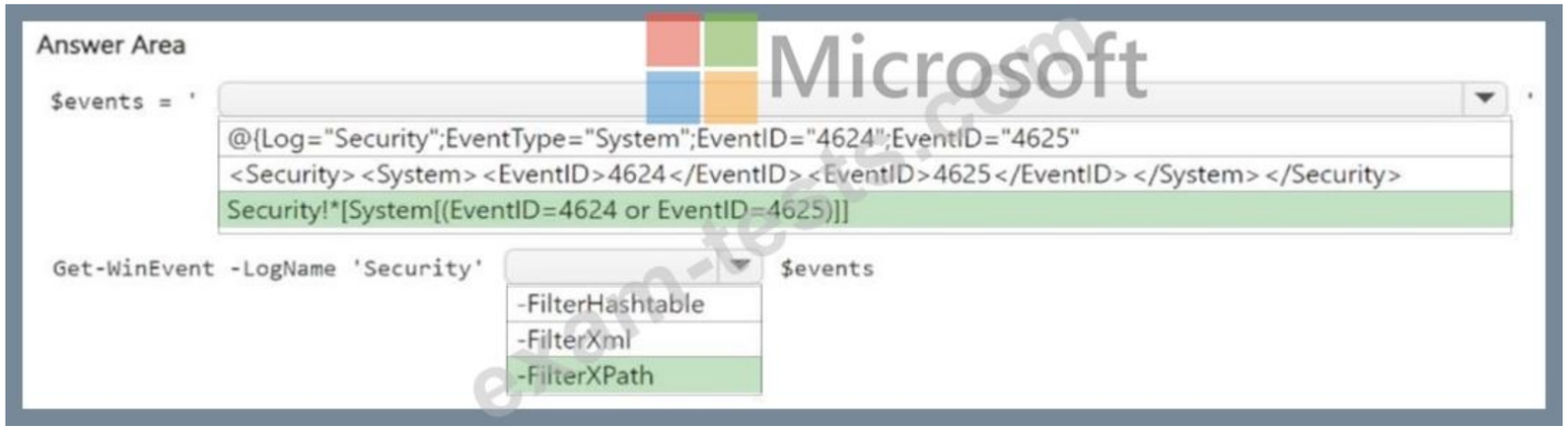
Answer Area

NEW QUESTION: 197
You have a Microsoft Sentinel workspace named Workspace1 that contains the AzureActivity table.
You need to configure the retention period for the AzureActivity table. The solution must meet the following requirements:
- Maximize the period during which you can run interactive queries.
- Minimize retention costs.
To what should you set the retention period? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.
A. 30 days
B. 90 days
C. 180 days
D. 2 years
Answer: B (LEAVE A REPLY)
You should set the interactive (Analytics) retention period for the AzureActivity table to 90 days.
Maximizes Free Interactive Queries: Microsoft Sentinel includes up to 90 days of interactive (Analytics tier) retention at no extra cost for workspaces and solution tables.
Minimizes Costs: Data retained in the interactive state for up to 90 days does not incur a retention charge. Any interactive retention period set beyond 90 days (up to 2 years) will incur extra standard Azure Monitor storage fees High-Performance KQL: Setting it to 90 days allows security analysts to perform immediate, real- time Kusto Query Language (KQL) searches, threat hunting, and dashboard visualizations across
3 months of historical data without query or restoration penalties.
Reference:
https://practical365.com/choosing-an-appropriate-retention-period-for-microsoft-sentinel-workspaces/

NEW QUESTION: 198
Hotspot Question
You have on-premises servers that run Windows Server.
You have a Microsoft Sentinel workspace named SW1. SW1 is configured to collect Windows Security log entries from the servers by using the Azure Monitor Agent data connector.
You plan to limit the scope of collected events to events 4624 and 4625 only.
You need to use a PowerShell script to validate the syntax of the filter applied to the connector.
How should you complete the script? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



Answer:

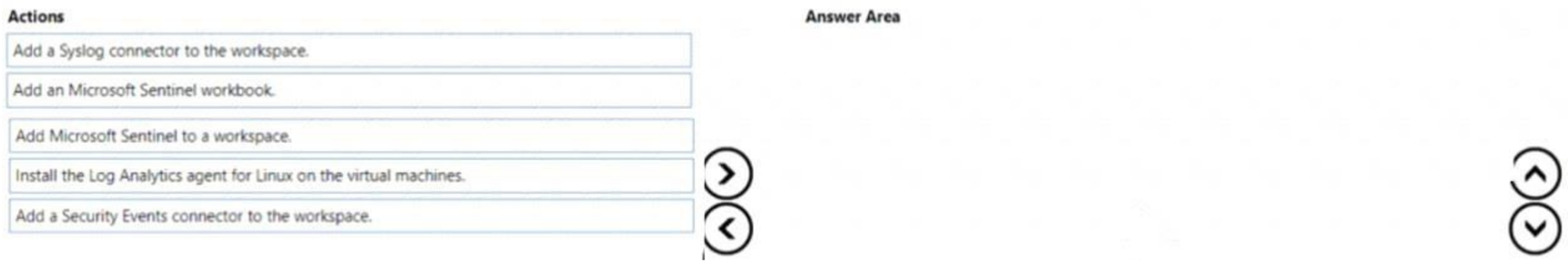


NEW QUESTION: 199

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

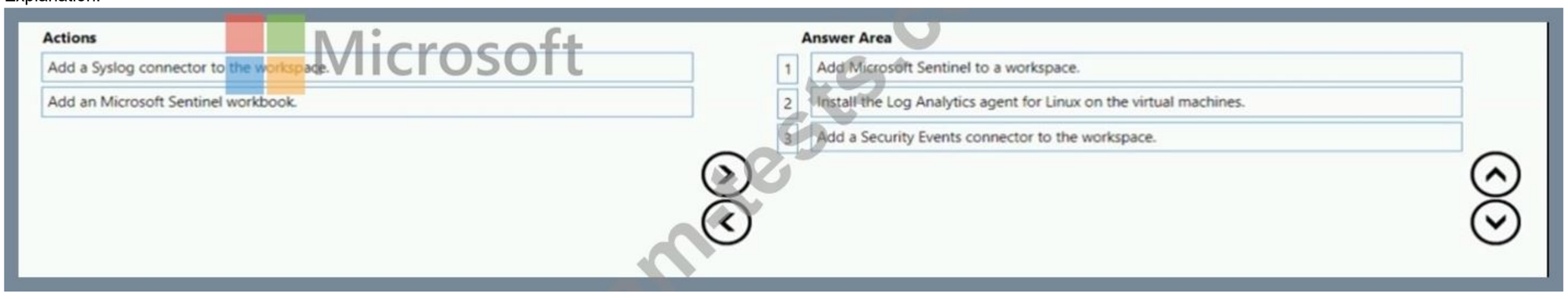
You need to configure Microsoft Sentinel to collect event logs from the virtual machines.

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.



Answer:

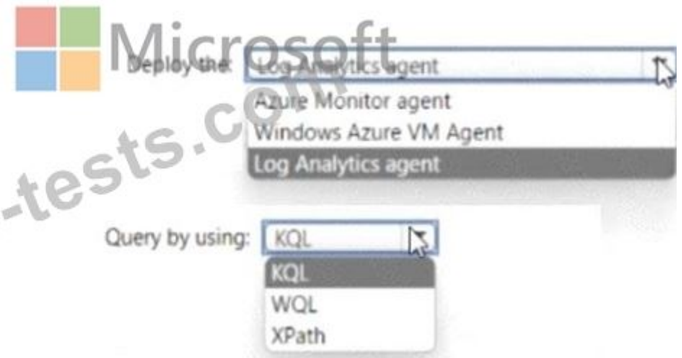
Explanation:



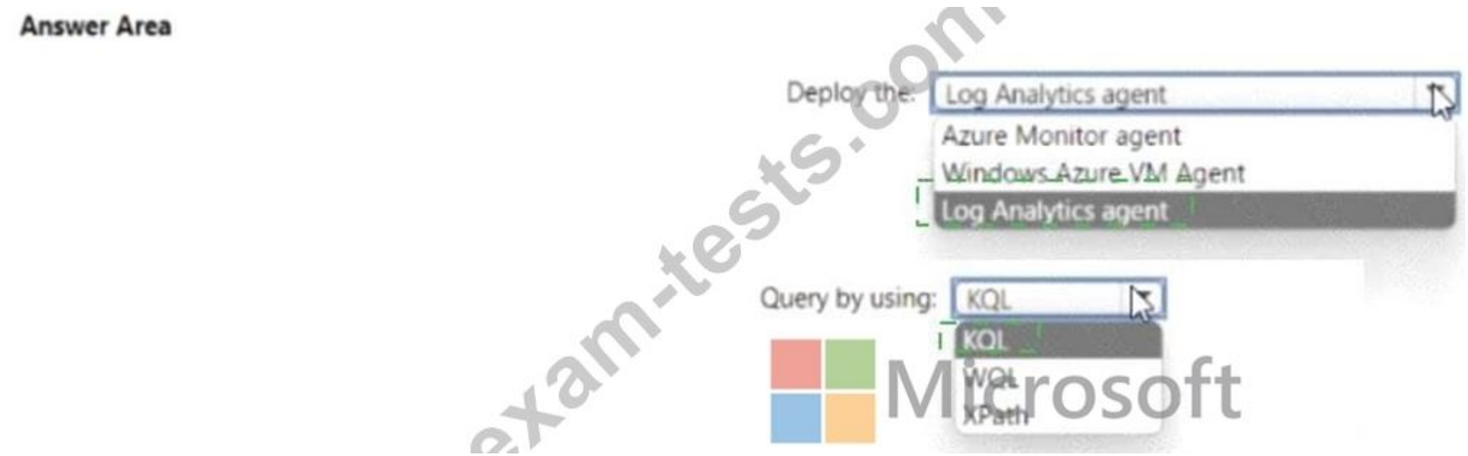
NEW QUESTION: 200

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



Answer:



Explanation:

To collect Windows Security event logs in Microsoft Sentinel , each monitored server or virtual machine must send its logs to a Log Analytics workspace , which Sentinel uses as its data foundation. This requires deploying the Log Analytics agent (formerly OMS agent) to the Windows systems.

The Log Analytics agent collects data such as event lo gs (including Security, Application, and System logs) and forwards them to the connected Log Analytics workspace. Once the agent is installed and configured, the data becomes available for analysis and correlation in Microsoft Sentinel.

Why not the other a gents:

* The Azure Monitor agent (AMA) is newer but, at this time, some Sentinel connectors and data collection rules still rely on the Log Analytics agent for Windows event collection.
* The Windows Azure VM Agent is only responsible for enabling Azure manage ment extensions, not log collection.

Once the data is ingested into Sentinel, analysts use KQL (Kusto Query Language) to query, investigate, and create analytics rules or workbooks. KQL is the native query language for both Azure Monitor Logs and Microsoft Sentinel .

Therefore, the correct configuration is:

Deploy the Log Analytics agent

Query by using KQL

NEW QUESTION: 201

Hotspot Question

Your on-premises network contains a Hyper-V cluster. The cluster contains the virtual machines shown in the following table.

Name	Operating system	Azure Connected Machine agent	Azure Monitoring Agent
Server1	Windows Server 2019	Not installed	Installed
Server2	Windows Server 2016	Installed	Not installed
Server3	Linux Ubuntu 20.04	Not installed	Installed

You have a Microsoft Sentinel workspace named SW1.

You have a data collection rule (DCR) that has the following configurations:

- Name: DCR1
- Destination: SW1
- Platform type: All
- Data collection endpoint: None
- Data source: Windows event logs, Linux syslog

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
Server1 can be added to DCR1 as a resource and all the Windows event logs can be gathered.	○	○
Server2 can be added to DCR1 as a resource and specific Windows event log events can be gathered.	○	○
Server3 can be added to DCR1 as a resource and all the Linux syslog data can be gathered.	○	○

Answer:

Answer Area

Statements	Yes	No
Server1 can be added to DCR1 as a resource and all the Windows event logs can be gathered.	○	○
Server2 can be added to DCR1 as a resource and specific Windows event log events can be gathered.	○	○
Server3 can be added to DCR1 as a resource and all the Linux syslog data can be gathered.	○	○

NEW QUESTION: 202

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

User1

User2

User3

Answer Area

Enable Microsoft Defender for Servers on virtual machines: [ ]

Review security recommendations and enable server vulnerability scans: [ ]

Answer:

Explanation:

Task

User

Enable Microsoft Defender for Servers on virtual machines:

User1

Review security recommendations and enable server vulnerability scans:

User1

* Query successful

This is a role-based access control (RBAC) question using the principle of least privilege.

The table of users and roles is:

Name

Role

User1

Security administrator

User2

Security reader

User3

Contributor

Export to Sheets

* Action: This is a management/configuration task at the subscription level, often related to enabling Defender plans and installing extensions on VMs.

* Required Permissions: The ability to modify security policies and settings in Microsoft Defender for Cloud and the permission to install extensions on VMs.

* The Security Administrator role is explicitly designed for this, granting permissions to manage the security features, policies, and program enrollment (like enabling Defender plans).

* The Contributor role can also perform this by installing the necessary agents and extensions, but it grants broad access to manage all resources, violating the principle of least privilege for a purely security-focused task.

* Least Privilege User: User1 (Security administrator)

* Action: This task has two parts:

* Review security recommendations: This is a read-only action. The Security Reader role is sufficient.

* Enable server vulnerability scans: This means configuring a security feature (Vulnerability Assessment), which requires write access to the security configuration or the resource itself.

* The Security Reader role cannot perform the "enable" action.

* The Security Administrator role has the permissions required to modify security policy and configuration to enable scanning features.

* The Contributor role can also do this, but again, the Security Administrator role is the least privileged for a security-specific configuration change.

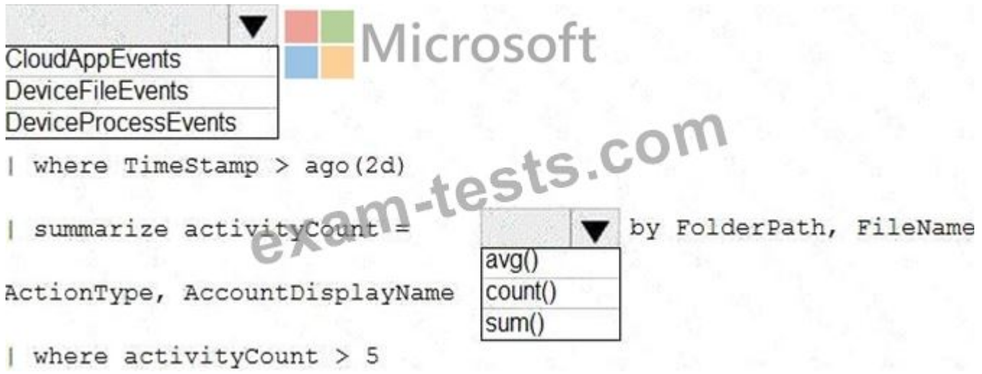
* Least Privilege User: Since the entire task includes an "enable" (write) action, we must use the role that can perform both read and write security actions. User1 (Security administrator) is the appropriate choice.

Task

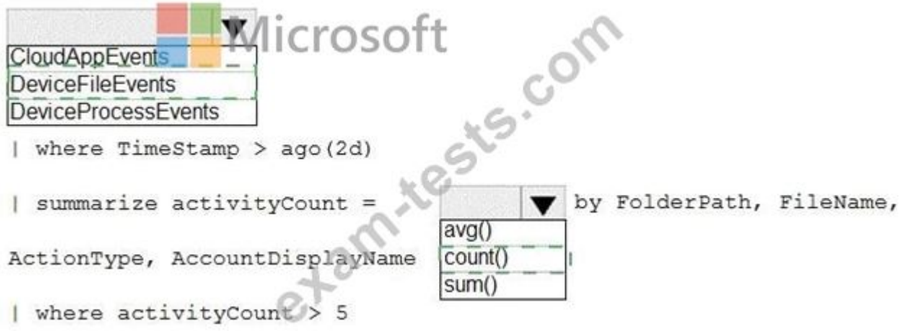
User

Enable Microsoft Defender for Servers on virtual machines:
User1
Review security recommendations and enable server vulnerability scans:
User1

NEW QUESTION: 203
You need to create an advanced hunting query to i nvestigate 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.



Answer:



Explanation:
Table: DeviceFileEvents
Aggregation function: count()
In Microsoft Defender XDR advanced hunting, data tables such as DeviceFileEvents , DeviceProcessEvents
, and CloudAppEvents are used to investigate various types of activities. Since this query aims to investigate an issue related to file activity-specifically identifying when files have been accessed, modified, or created repeatedly-the correct data source table is DeviceFileEvents . This table contains information about file- level activities recorded by Defender for Endpoint sensors, including file path, file name, action type, and user account involved.
The KQL structure shown in the image follows standard hunting query syntax:
DeviceFileEvents
| where Timestamp > ago(2d)
| summarize activityCount = count() by FolderPath, FileName, ActionType, AccountDisplayName
| where activityCount > 5

Here's why:
* The where Timestamp > ago(2d) clause filters results from the last 2 days, a typi cal timeframe for immediate investigations.
* The summarize operator groups events by FolderPath, FileName, ActionType, and AccountDisplayName, then uses count() to determine how many times each file was acted upon.
* Finally, where activityCount > 5 filters t o show only unusually high-frequency activity, which might indicate suspicious or automated file manipulation.
Microsoft Defender XDR documentation highlights that DeviceFileEvents is the correct schema for file activity investigations, while DeviceProcess Events focuses on process creation and execution, and CloudAppEvents targets cloud application usage.
Thus, the verified and documented correct completions are:
Table: DeviceFileEvents
Aggregation function: count()

NEW QUESTION: 204
You have a Microsoft Sentinel workspace that has Microsoft Sentinel data lake enabled for long- term retention.
You have a Microsoft Security Operations Center (SOC) that uses Jupyter notebooks for advanced investigations.
You run a weekly, hypothesis-driven hunting query to detect potential lateral movement. The query looks for multiple failed sign-ins followed by a successful sign-in.
You need to offload heavy computation for the query and persist the processed results to the data lake.
What should you do?
A. Create an analytics rule.
B. Create a scheduled notebook job.
C. Use livestream to continuously append the results of a second hunting query.
D. Every hour, create a watchlist from raw events.
Answer: (SHOW ANSWER)
The best action is to create a scheduled notebook job. This approach uses the underlying Apache Spark compute in your Jupyter notebook environment to offload heavy computations from the SOC, and it automatically persists the processed results directly back to the Microsoft Sentinel data lake for long-term retention and future review.
Jupyter notebooks integrated with Microsoft Sentinel allow you to offload heavy, complex computation (like the multi-stage logic of correlating weekly failed-to-successful sign-ins) outside of the main Log Analytics engine.
Furthermore, notebooks can natively write and persist processed results directly back to your long-term data lake using Azure Storage APIs or Synapse integration.
Reference:
https://strategic-cyber.co.uk/2024/06/19/microsoft-sentinel-part-2-deploying-a-sentinel-workspace-and-onboarding-free-data-sources/

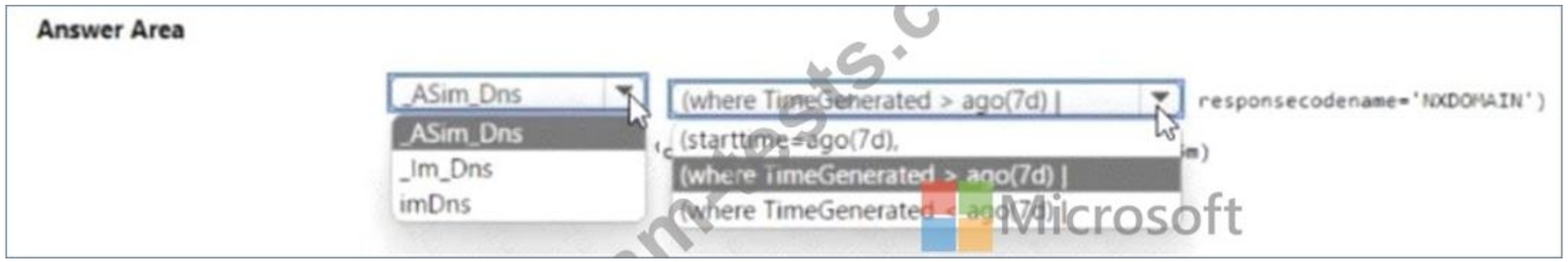
NEW QUESTION: 205
You have a Microsoft 365 subscription that has Microsoft 365 Defender enabled.
You need to identify all the changes made to sensitivity labels during the past seven days.
What should you use?
A. the Incidents blade of the Microsoft 365 Defender portal
B. the Alerts settings on the Data 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 (LEAVE A REPLY)
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

NEW QUESTION: 206
You implement Safe Attachments policies in Microsoft Defender for Office 365.
Users report that email messages containing attachment s take longer than expected to be received.
You need to reduce the amount of time it takes to deliver messages that contain attachments without compromising security. The attachments must be scanned for malware, and any messages that contain malware must be blocked.
What should you configure in the Safe Attachments policies?
A. Dynamic Delivery
B. Replace
C. Block and Enable redirect
D. Monitor and Enable redirect
Answer: (SHOW ANSWER)
In Microsoft Defender for Office 365 Safe Attachments, Dynamic Delivery is specifically designed to shorten perceived delivery time while keeping full detonation scanning in place. Microsoft explains that with Dynamic Delivery, the service "delivers the message body right away and replaces attachments with a placeholder while scanning" ; once the sandbox verdict is clean, the original file is reinserted automatically
. If malware is found, the attachment is blocked/removed and the message is handled per policy (for example, quarantined) . This option meets both requirements in the question: (1) users get messages quickly (no long wait for full message delivery) and (2) security isn't reduced because attachments are still detonated before users can open them.
By contrast, Block delays or stops delivery when malicious; Replace swaps detected-malicious attachments with a .txt summary but doesn't reduce the initial delivery time for clean items; Monitor only logs without enforcing protection. Therefore, to reduce delivery latency without compromising protection and still block malware , configure Dynamic Delivery in your Safe Attachments policy.

NEW QUESTION: 207
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 (LEAVE A REPLY)
Explanation (concise): In Azure Sentinel (Microsoft Sentinel) KQL, to display a time chart aggregated by day, you bucket timestamps using bin(TimeGenerated, 1d) (often after a summarize), which is what the timechart visual expects. extend adds columns, makeset aggregates values into a set, and workspace is for cross-workspace queries-not for time bucketing.

NEW QUESTION: 208
You need to create a query to investigate DNS-related activity. 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.

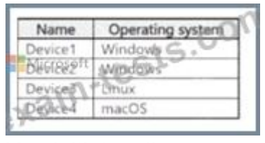


Answer:

Explanation

NEW QUESTION: 209

You have a Microsoft 365 subscription that uses Microsoft Defender for Endpoint and contains the devices shown in the following table.



Name	Operating system
Device1	Windows
Device2	Windows
Device3	Linux
Device4	macOS

You initiate a live response session on each device.

You need to collect a Defender for Endpoint investigation package from each device.

On which devices can you collect the package by running advanced live response commands from the command-line interface (CLI)?

A. Device1, Device2, and Device3 only

B. Device1 and Device2 only

C. Device1, Devke2, Device3, and Device4

D. Device3 and Device4 only

Answer: A (LEAVE A REPLY)

NEW QUESTION: 210

You have an Azure subscription named Sub1 that contains the resources shown in the following table.

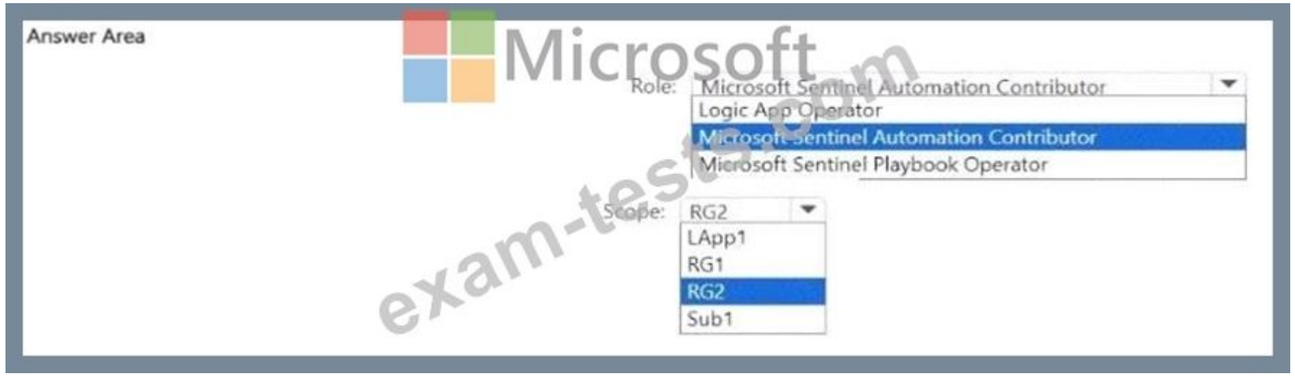
Name	Type	Resource group	Description
WS1	Microsoft Sentinel workspace	RG1	Contains a scheduled query rule named Rule1
LApp1	Azure logic app	RG2	Contains a Microsoft Sentinel incident trigger

You plan to configure Rule1 to trigger Lapp1 when an incident is generated.

You need to recommend the role-based access control (RBAC) role that you should assign to WS1, and the scope at which should you assign the role. The solution must follow the principle of least privilege.

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

NOTE: Each correct selection is worth one point.



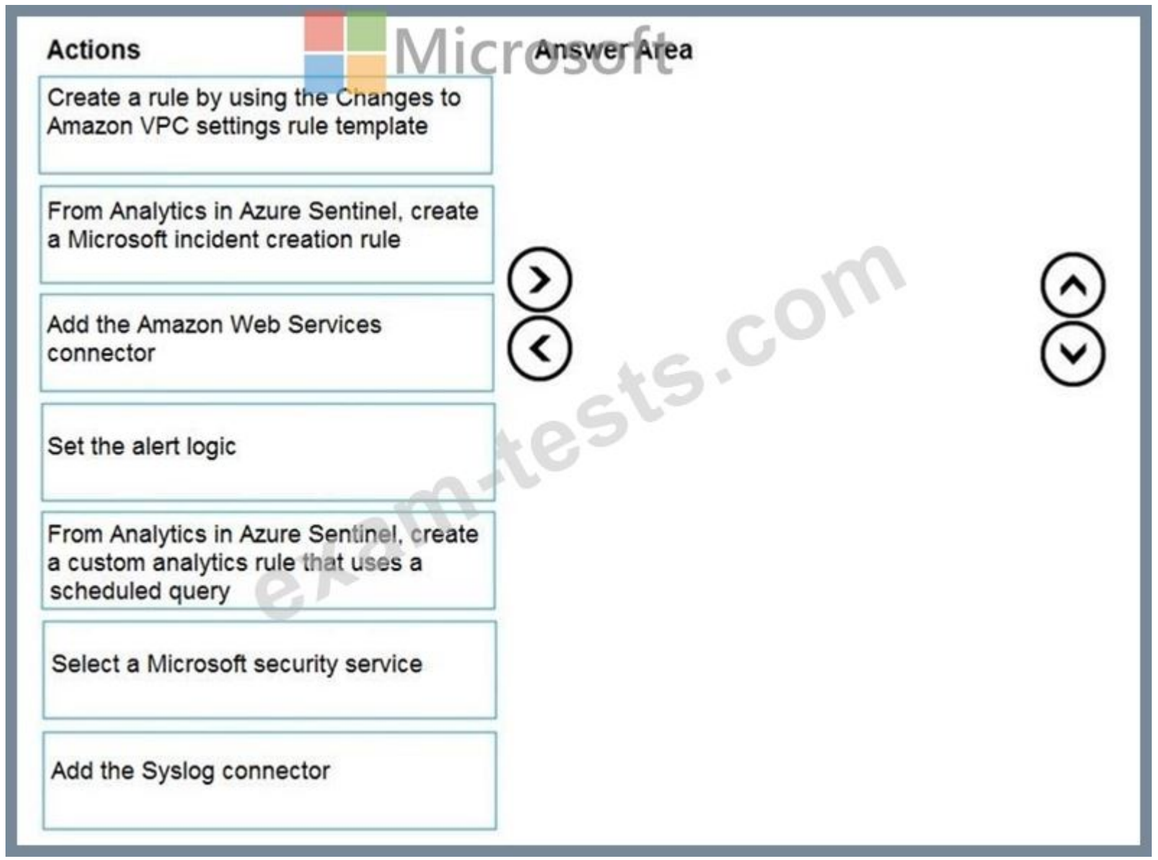
Answer:

NEW QUESTION: 211

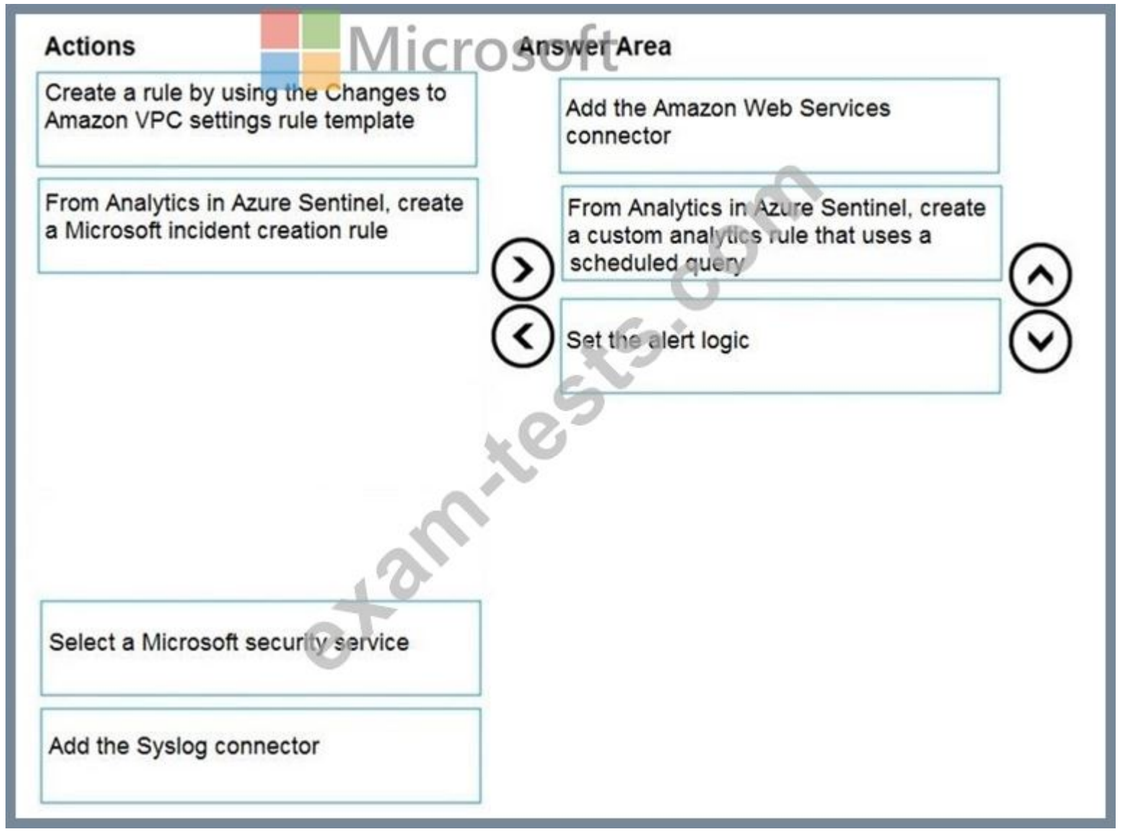
Drag and Drop Question

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.


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

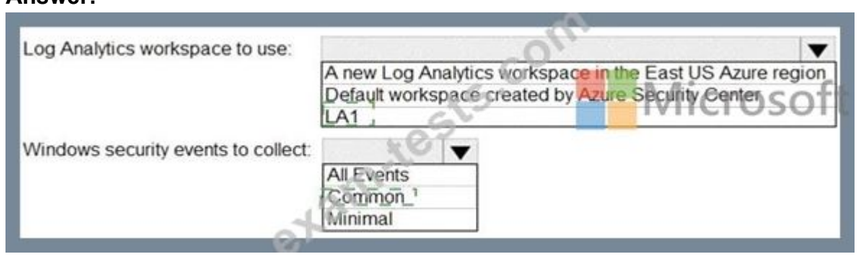
Answer:



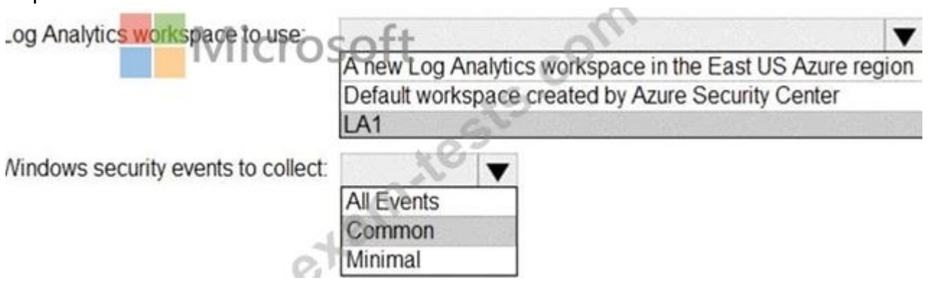
Explanation:
https://docs.microsoft.com/en-us/azure/sentinel/detect-threats-custom

NEW QUESTION: 212
You need to implement Azure Defender to meet the Azure Defender 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:



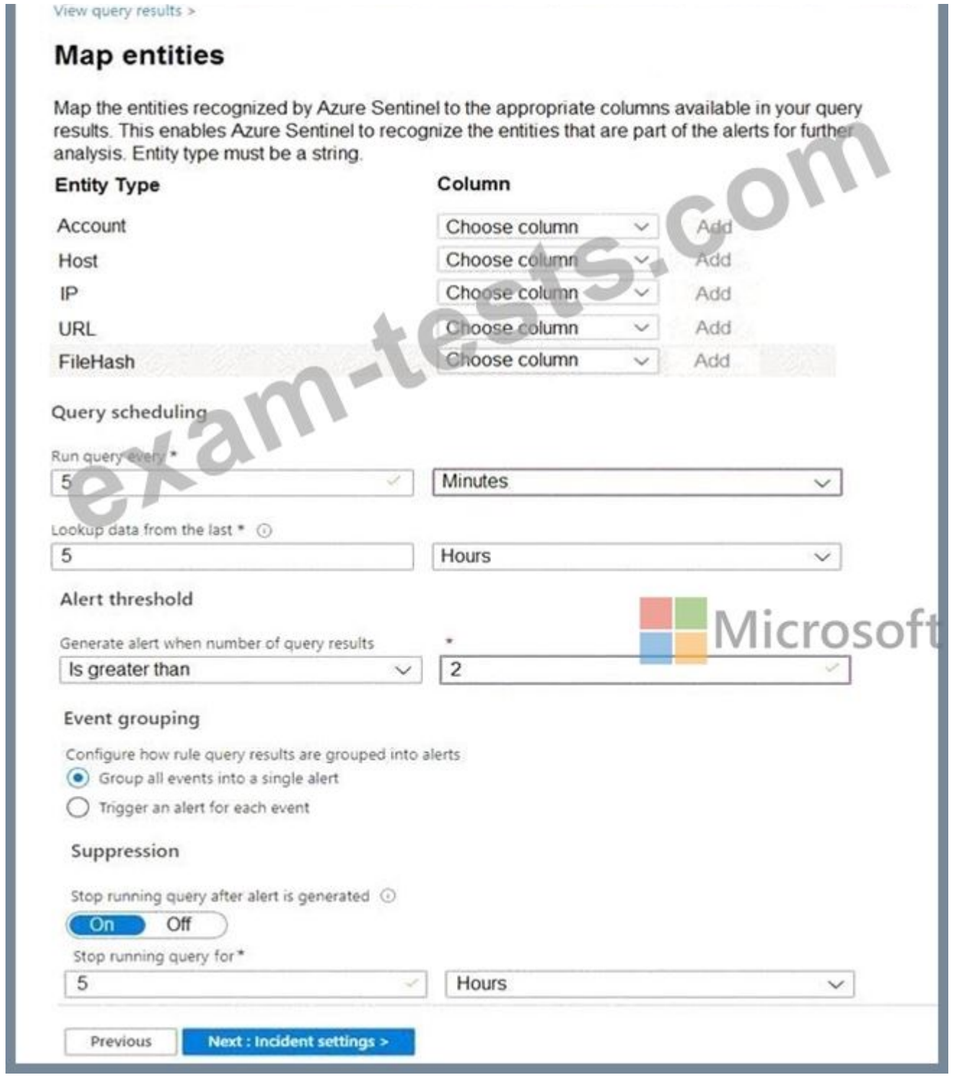
Explanation:



NEW QUESTION: 213

You use Azure Sentinel to monitor irregular Azure activity.

You create custom analytics rules to detect threats as shown in the following exhibit.



You do NOT define any incident settings as part of the rule definition.

Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.

NOTE: Each correct selection is worth one point.

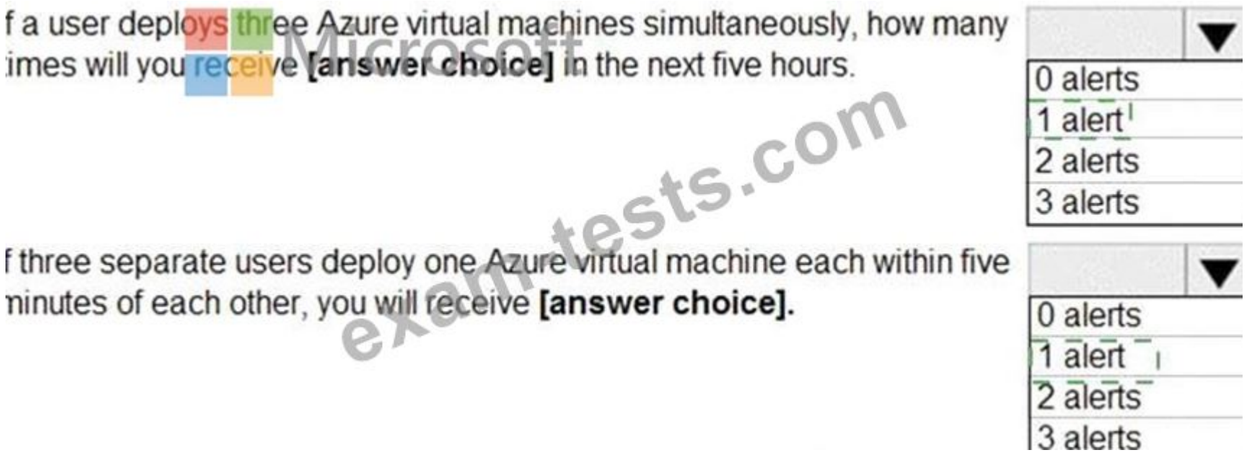
If a user deploys three Azure virtual machines simultaneously, how many times will you receive **[answer choice]** in the next five hours.

- 0 alerts
- 1 alert
- 2 alerts
- 3 alerts

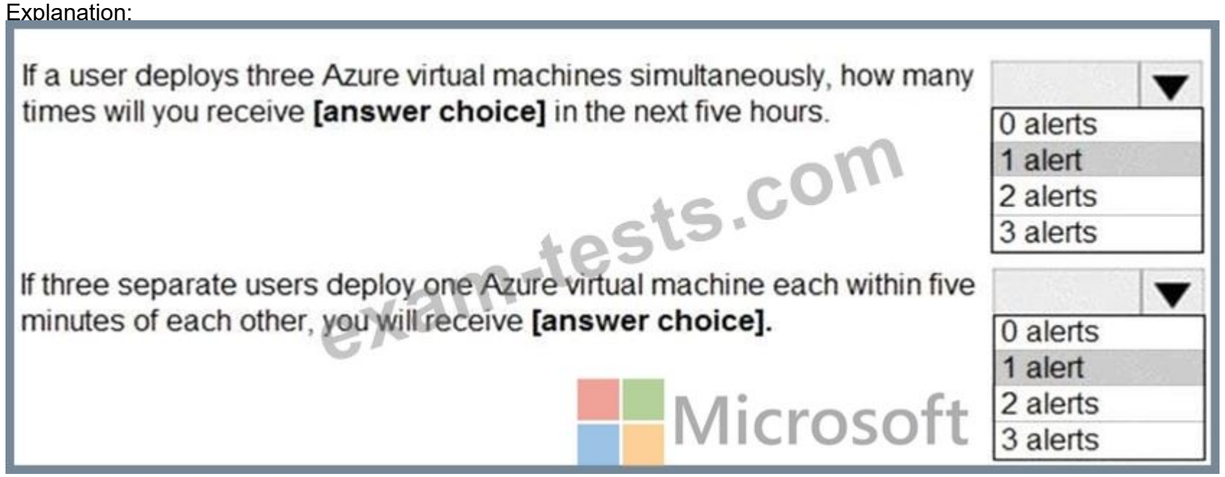
If three separate users deploy one Azure virtual machine each within five minutes of each other, you will receive **[answer choice].**

- 0 alerts
- 1 alert
- 2 alerts
- 3 alerts

Answer:



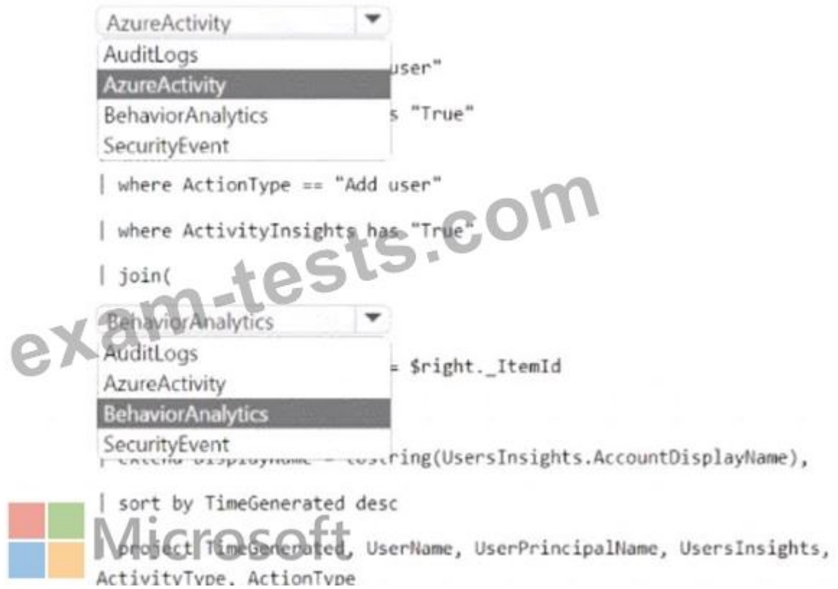
Explanation:



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

NEW QUESTION: 214
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: (SHOW ANSWER)
A suppression rule in Azure Security Center (Defender for Cloud) prevents specific alerts from appearing in the portal or triggering notifications. When a suppression rule is active, alerts that match its conditions are hidden from view, even though they still occur in the background.
If you need to temporarily view alerts from the suppressed virtual machines - for example, while troubleshooting or verifying detections - you can disable the suppression rule. Microsoft documentation states: "To temporarily resume visibility of alerts suppressed by a rule, change the rule state to Disabled.
When disabled, the rule no longer hides alerts that meet its conditions." Changing the expiration date (Option A) only controls when the rule automatically stops; it does not immediately restore visibility.
Modifying filters (Option C) won't reveal suppressed alerts, as those are already hidden from query results.
Viewing Windows event logs (Option D) provides raw OS data but not Security Center alert context.
Thus, to see the suppressed alerts for the last five days, you must disable the suppression rule, making B the correct answer.

NEW QUESTION: 215
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:

Answer Area

Explanation:

NEW QUESTION: 216

Hotspot Question

You have 100 on-premises servers that run Windows Server and do NOT have internet connectivity.

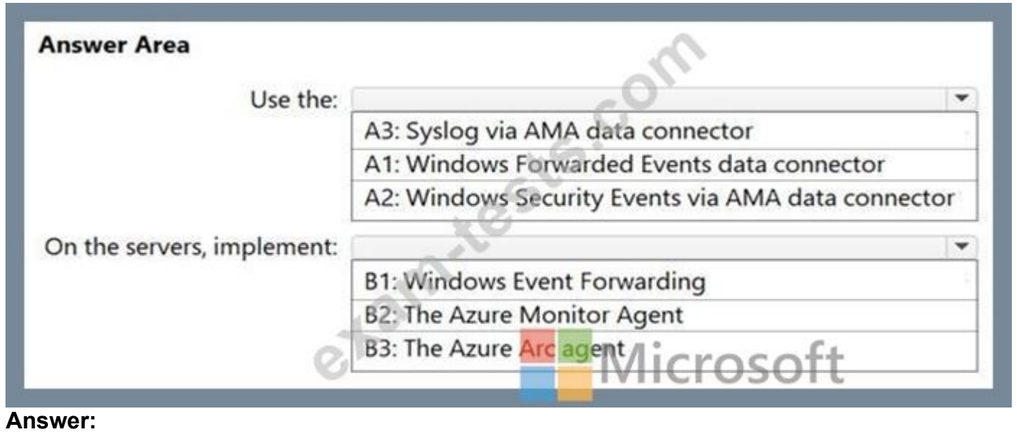
You have an Azure subscription that contains a dedicated monitoring server.

You have a Microsoft Sentinel workspace named Workspace1.

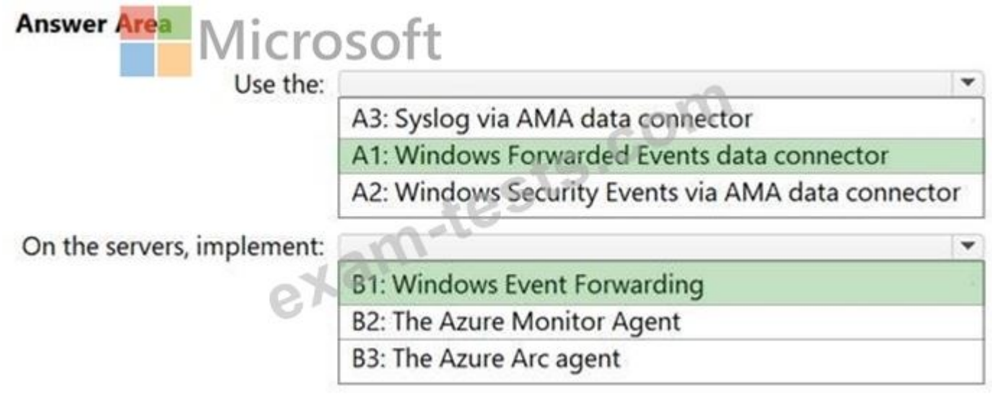
You need to ingest Windows event logs from the on-premises servers into Workspace1.

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

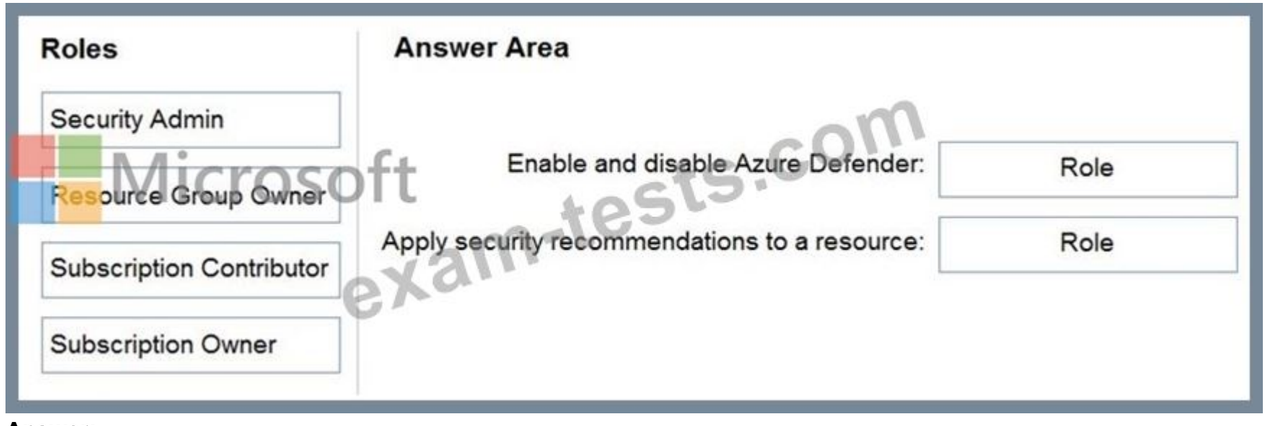
NOTE: Each correct selection is worth one point.



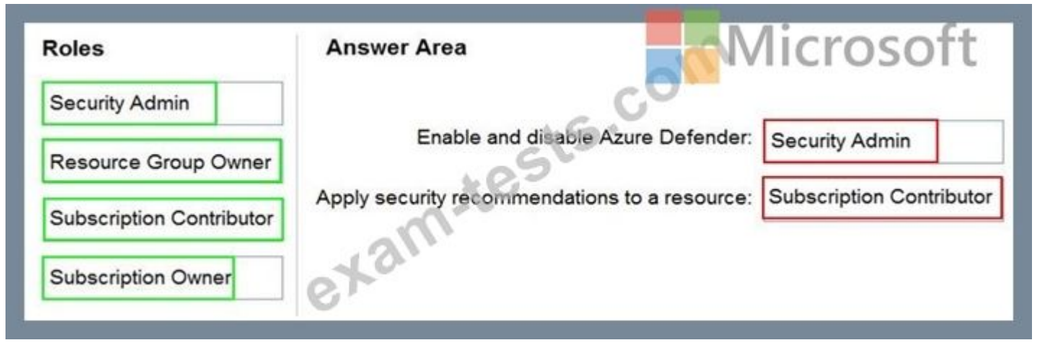
Answer:



NEW QUESTION: 217
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.



Answer:



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

NEW QUESTION: 218
You have an on-premises datacenter that contains a custom web app named Appl. App1 uses Active Directory Domain Services (AD DS) authentication and is accessible by using Microsoft Entra application proxy.
You have a Microsoft 365 E5 subscription that uses Microsoft Defender XDR.
You receive an alert that a user downloaded highly confidential documents.
You need to remediate the risk associated with the alert by requiring multi-factor authentication (MFA) when users use App1 to initiate the download of documents that have a Highly Confidential sensitivity label applied.
What should you do? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Answer:

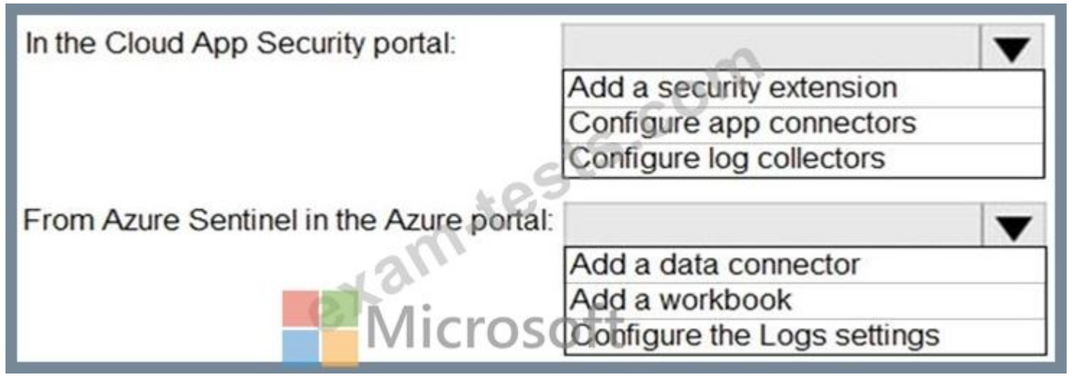
Explanation:

NEW QUESTION: 219

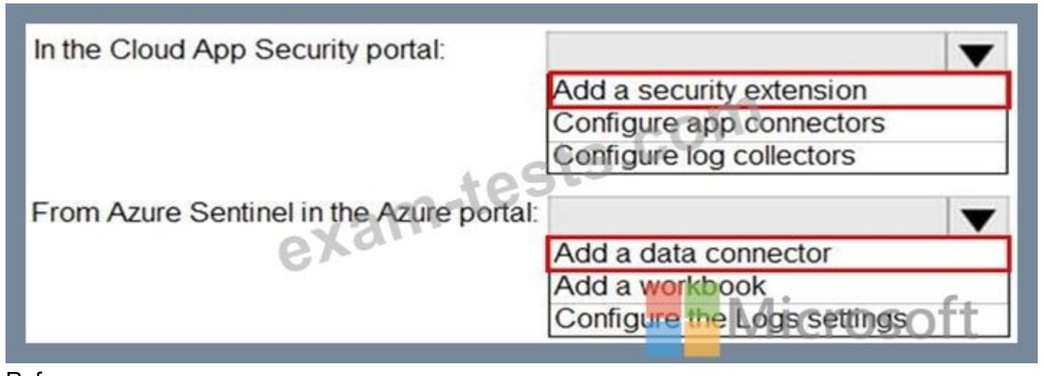
You need to configure the Azure Sentinel integration to meet the Azure Sentinel requirements.

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

NOTE: Each correct selection is worth one point.



Answer:



Reference:

https://docs.microsoft.com/en-us/cloud-app-security/siem-sentinel

NEW QUESTION: 220

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

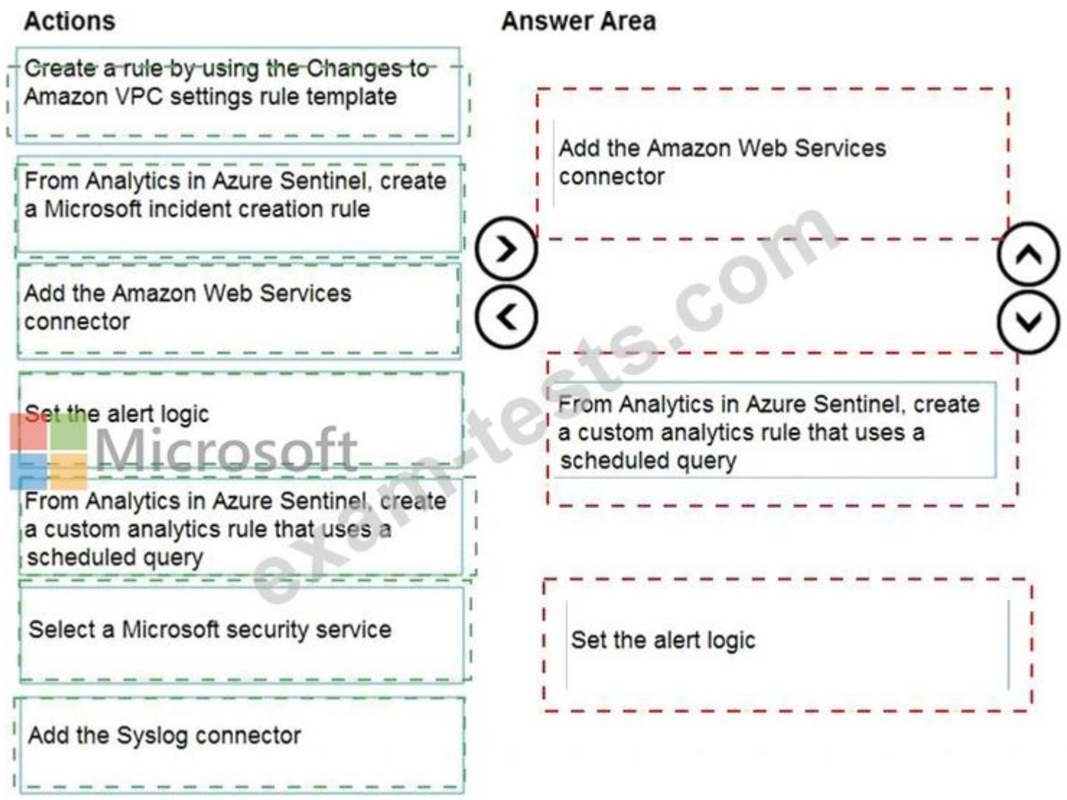
Set the alert logic

From Analytics in Azure Sentinel, create a custom analytics rule that uses a scheduled query

Select a Microsoft security service

Add the Syslog connector

Answer:



Explanation

Graphical user interface, text, application Description automatically generated

Reference:

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

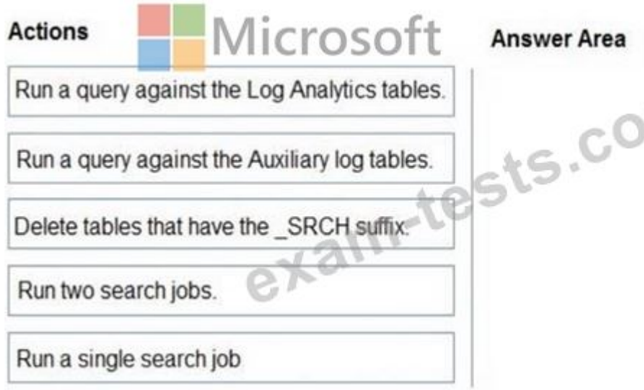
NEW QUESTION: 221

Drag and Drop Question

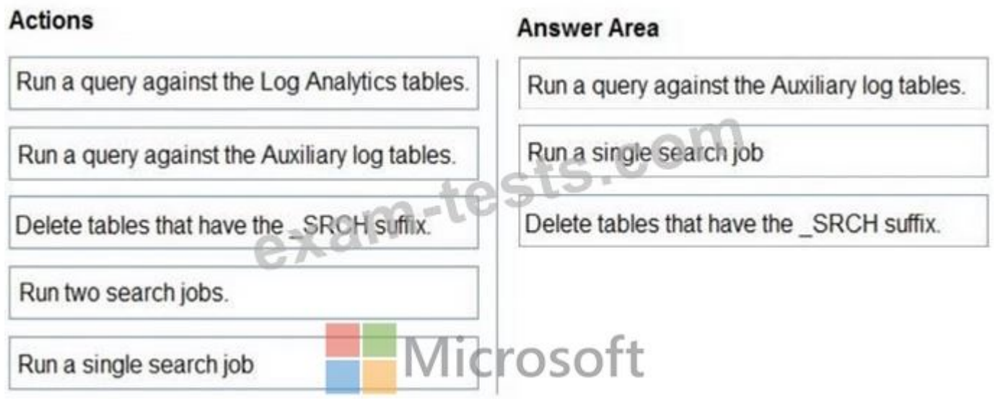
You have a Microsoft Sentinel workspace named Workspace1 that has a retention period of 12 years. Workspace1 contains two custom auxiliary tables named Table1 and Table2.

You need to correlate the data between Table1 and Table2 from the past six months by using a JOIN operation. The solution must minimize administrative effort and costs.

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.



Answer:



NEW QUESTION: 222

You have an Azure subscription that contains a user named User1 and a Microsoft Sentinel workspace named WS1. WS1 uses Microsoft Defender for Cloud.

You have the Microsoft security analytics rules shown in the following table.

Name	Service	Severity	Action
Rule1	Defender for Cloud	High	Create incident
Rule2	Defender for Cloud	High	Create incident
Rule3	Defender for Cloud	High	Create incident
Rule4	Defender for Cloud	High	Create incident

User1 performs an action that matches Rule1, Rule2, Rule3, and Rule4. How many incidents will be created in WS1?

A. 1
B. 2
C. 3

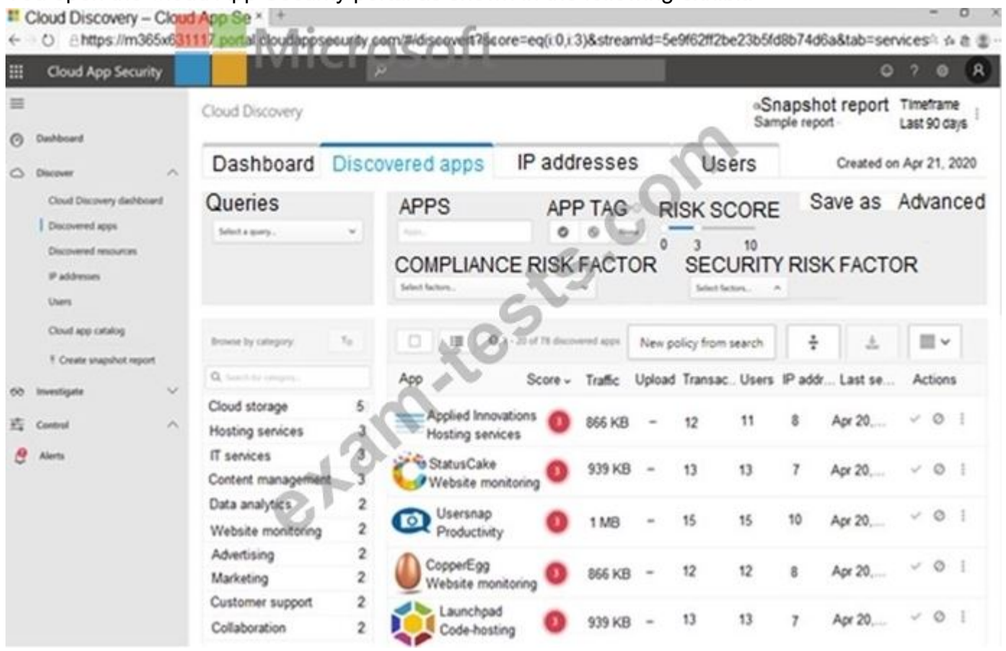
D. 4

Answer: (SHOW ANSWER)

Microsoft Sentinel "Microsoft security" analytics rules (for products like Defender for Cloud) create incidents from alerts generated by that product. Even if multiple identical Microsoft security rules exist for the same product, a single incoming alert will result in one incident in the workspace, not one per rule.

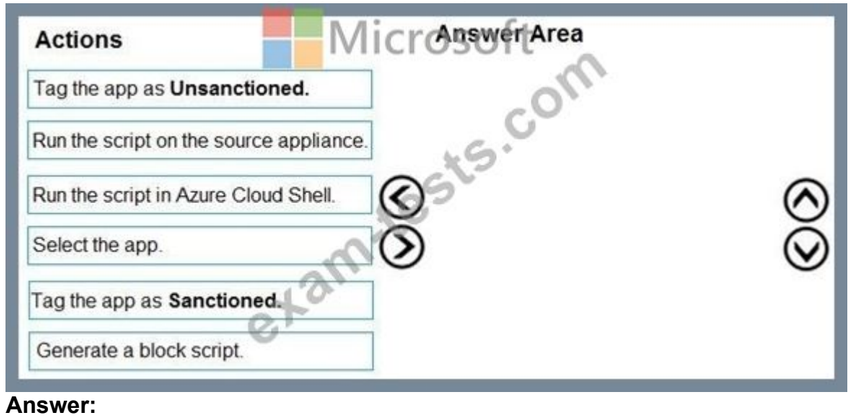
NEW QUESTION: 223

You open the Cloud App Security portal as shown in the following exhibit.

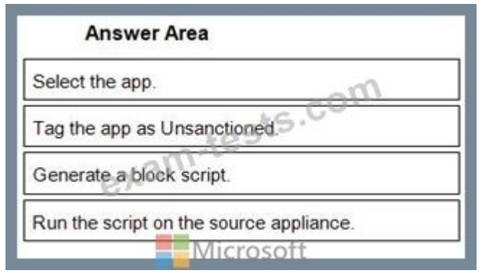


You need to remediate the risk for the Launchpad app.

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.



Answer:



1 - Select the app.
2 - Tag the app as Unsanctioned.
3 - Generate a block script.
4 - Run the script on the source appliance.
Reference:
https://docs.microsoft.com/en-us/cloud-app-security/governance-discovery

NEW QUESTION: 224
From Azure Sentinel, you open the Investigation pane for a high-severity incident as shown in the following exhibit.

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

If you hover over the virtual machine named vm1, you can view **[answer choice].**

- the inbound network security group (NSG) rules
- the last five Windows security log events
- the open ports on the host
- the running processes

If you select **[answer choice],** you can navigate to the bookmarks related to the incident.

- Entities
- Info
- Insights
- Timeline

Answer:

If you hover over the virtual machine named vm1, you can view **[answer choice].**

- the inbound network security group (NSG) rules
- the last five Windows security log events
- the open ports on the host
- the running processes

If you select **[answer choice],** you can navigate to the bookmarks related to the incident.

- Entities
- Info
- Insights
- Timeline

Reference:
https://docs.microsoft.com/en-us/azure/sentinel/tutorial-investigate-cases#use-the-investigation-graph-to-deep-dive

NEW QUESTION: 225
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: A,D (LEAVE A REPLY)
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: 226
Case Study 3 - Litware Inc
Overview
Fabrikam, Inc. is a financial services company.
The company has branch offices in New York, London, and Singapore. Fabrikam has remote users located across the globe. The remote users access company resources, including cloud resources, by using a VPN connection to a branch office.
Existing Environment
Identity Environment
The network contains an Active Directory Domain Services (AD DS) forest named fabrikam.com that syncs with an Azure AD tenant named fabrikam.com. To sync the forest, Fabrikam uses Azure AD Connect with pass-through authentication enabled and password hash synchronization disabled.
The fabrikam.com forest contains two global groups named Group1 and Group2.
Microsoft 365 Environment
All the users at Fabrikam are assigned a Microsoft 365 E5 license and an Azure Active Directory Premium Plan 2 license.
Fabrikam implements Microsoft Defender for Identity and Microsoft Defender for Cloud Apps and enables log collectors.
Azure Environment
Fabrikam has an Azure subscription that contains the resources shown in the following table.

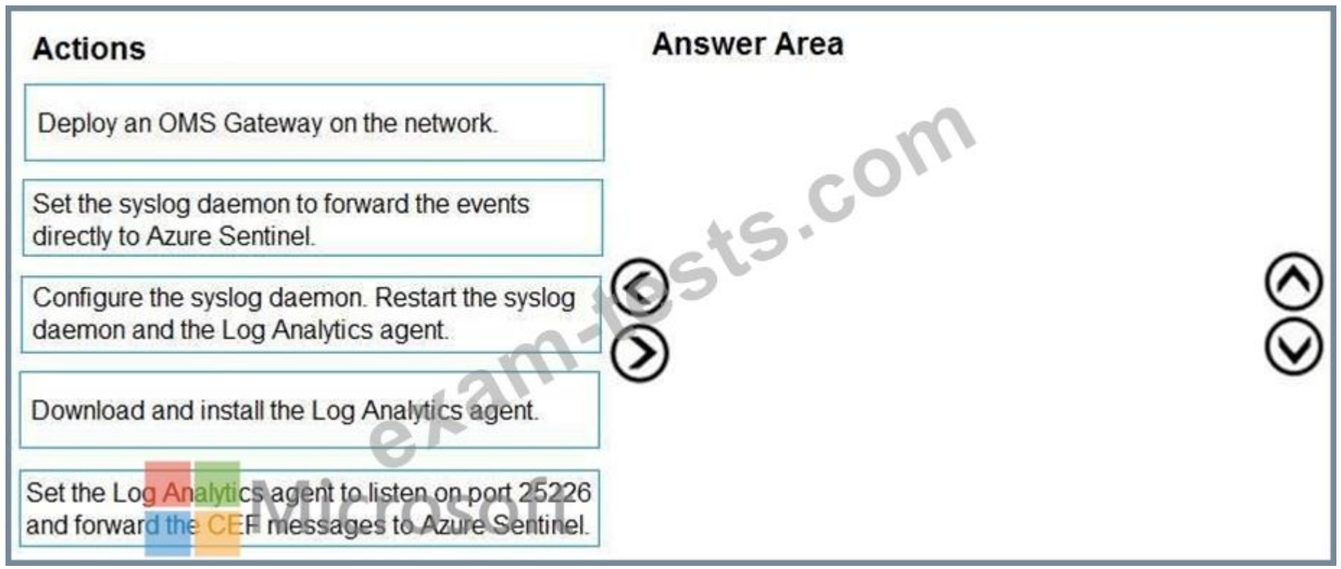
Name	Type	Description
App1	Azure logic app	To automate incident generation in an internal ticketing system, the security operations (SecOps) team invokes App1 by using an HTTP endpoint.
SAWkspc1	Azure Synapse Analytics workspace	SAWkspc1 hosts an Apache Spark pool named Pool1.
LAWkspc1	Log Analytics workspace	LAWkspc1 will be used in a planned Microsoft Sentinel implementation.

Amazon Web Services (AWS) Environment
Fabrikam has an Amazon Web Services (AWS) account named Account1. Account1 contains
100 Amazon Elastic Compute Cloud (EC2) instances that run a custom Windows Server 2022.
The image includes Microsoft SQL Server 2019 and does NOT have any agents installed.
Current Issues
When the users use the VPN connections, Microsoft 365 Defender raises a high volume of impossible travel alerts that are false positives.
Defender for Identity raises a high volume of Suspected DCSync attack alerts that are false positives.
Requirements

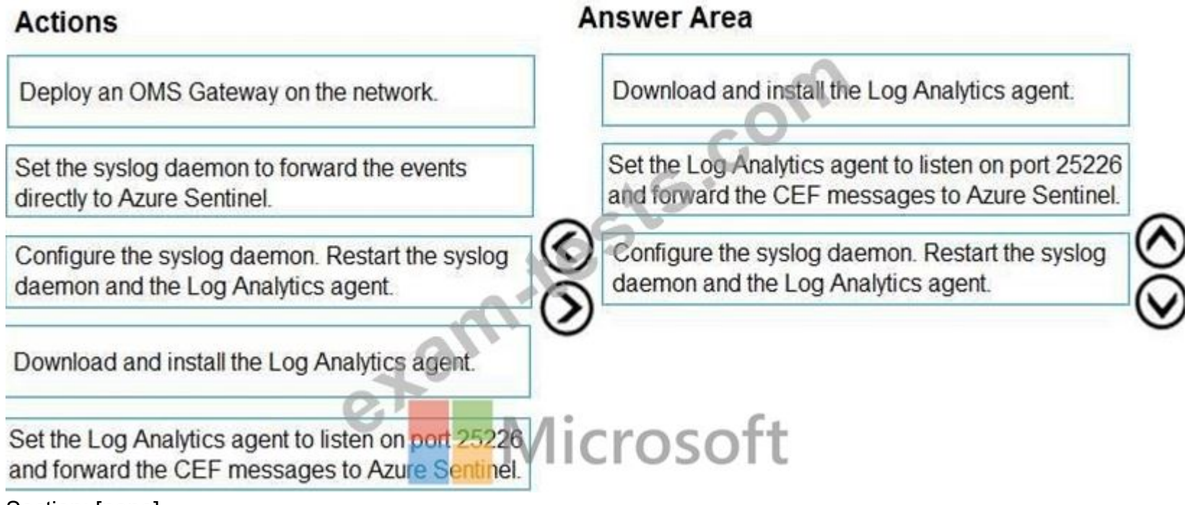
Planned changes
Fabrikam plans to implement the following services:
- Microsoft Defender for Cloud
- Microsoft Sentinel
Business Requirements
Fabrikam identifies the following business requirements:
- Use the principle of least privilege, whenever possible.
- Minimize administrative effort.
Microsoft Defender for Cloud Apps Requirements
Fabrikam identifies the following Microsoft Defender for Cloud Apps requirements:
- Ensure that impossible travel alert policies are based on the previous activities of each user.
- Reduce the amount of impossible travel alerts that are false positives.
Microsoft Defender for Identity Requirements
Minimize the administrative effort required to investigate the false positive alerts.
Microsoft Defender for Cloud Requirements
Fabrikam identifies the following Microsoft Defender for Cloud requirements:
- Ensure that the members of Group2 can modify security policies.
- Ensure that the members of Group1 can assign regulatory compliance policy initiatives at the Azure subscription level.
- Automate the deployment of the Azure Connected Machine agent for Azure Arc-enabled servers to the existing and future resources of Account1.
- Minimize the administrative effort required to investigate the false positive alerts.
Microsoft Sentinel Requirements
Fabrikam identifies the following Microsoft Sentinel requirements:
- Query for NXDOMAIN DNS requests from the last seven days by using built-in Advanced Security Information Model (ASIM) unifying parsers.
- From AWS EC2 instances, collect Windows Security event log entries that include local group membership changes.
- Identify anomalous activities of Azure AD users by using User and Entity Behavior Analytics (UEBA).
- Evaluate the potential impact of compromised Azure AD user credentials by using UEBA.
- Ensure that App1 is available for use in Microsoft Sentinel automation rules.
- Identify the mean time to triage for incidents generated during the last 30 days.
- Identify the mean time to close incidents generated during the last 30 days.
- Ensure that the members of Group1 can create and run playbooks.
- Ensure that the members of Group1 can manage analytics rules.
- Run hunting queries on Pool1 by using Jupyter notebooks.
- Ensure that the members of Group2 can manage incidents.
- Maximize the performance of data queries.
- Minimize the amount of collected data.
You need to correlate data from the SecurityEvent Log Analytics table to meet the Microsoft Sentinel requirements for using UEBA.
Which Log Analytics table should you use?
A. SentinelAudit
B. AADRiskyUsers
C. IdentityDirectoryEvents
D. IdentityInfo

Answer: (SHOW ANSWER)

NEW QUESTION: 227
DRAG DROP
You plan to connect an external solution that will send Common Event Format (CEF) messages to Azure Sentinel.
You need to deploy the log forwarder.
Which three actions should you perform in sequence? To answer, move the appropriate actions form the list of actions to the answer area and arrange them in the correct order.
Select and Place:



Answer:



Section: [none]

Explanation/Reference:

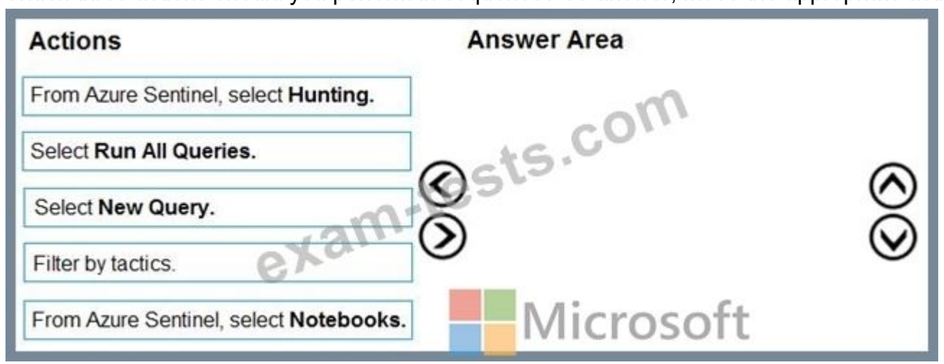
https://docs.microsoft.com/en-us/azure/sentinel/connect-cef-agent?tabs=rsyslog

NEW QUESTION: 228

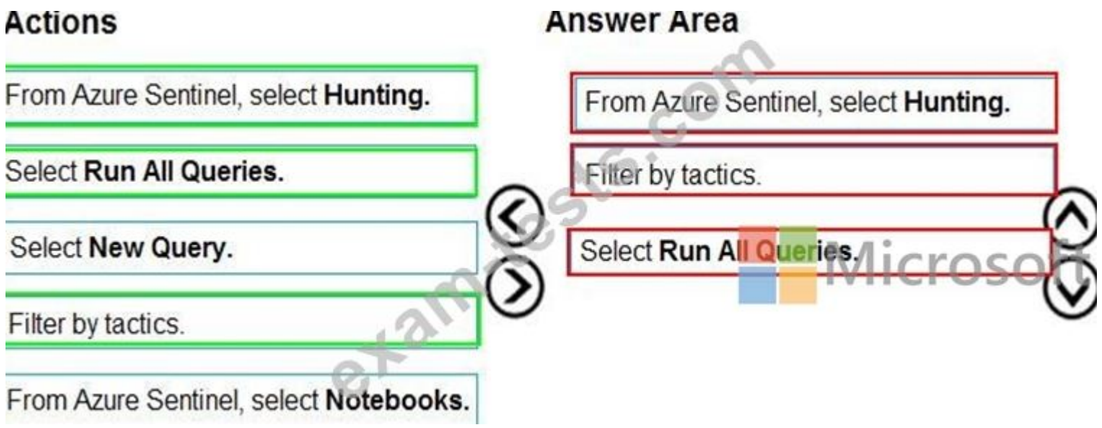
You have an Azure Sentinel deployment.

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.



Answer:



NEW QUESTION: 229

You have a Microsoft 365 E5 subscription that uses Microsoft Defender for Endpoint and contains a Windows device named Device1. You need to investigate a suspicious executable file detected on Device1.

The solution must meet the following requirements:

* Identify the image file path of the file.

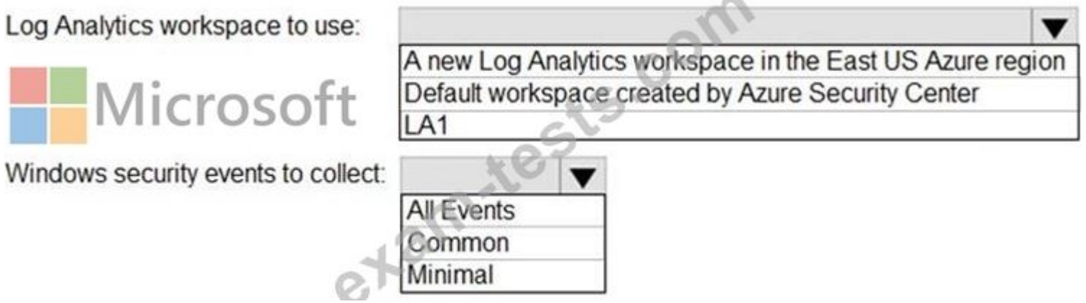
* Identify when the file was first detected on Device1.

What should you review from the timeline of the detection event? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

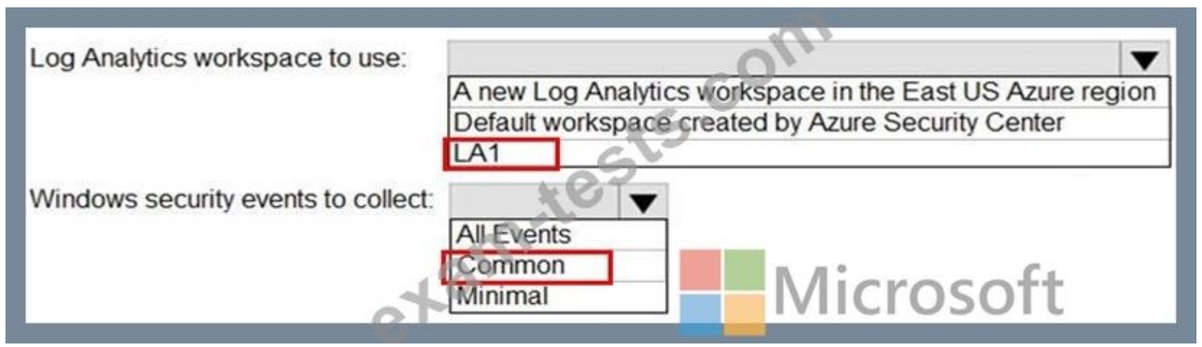
Answer:

Explanation:

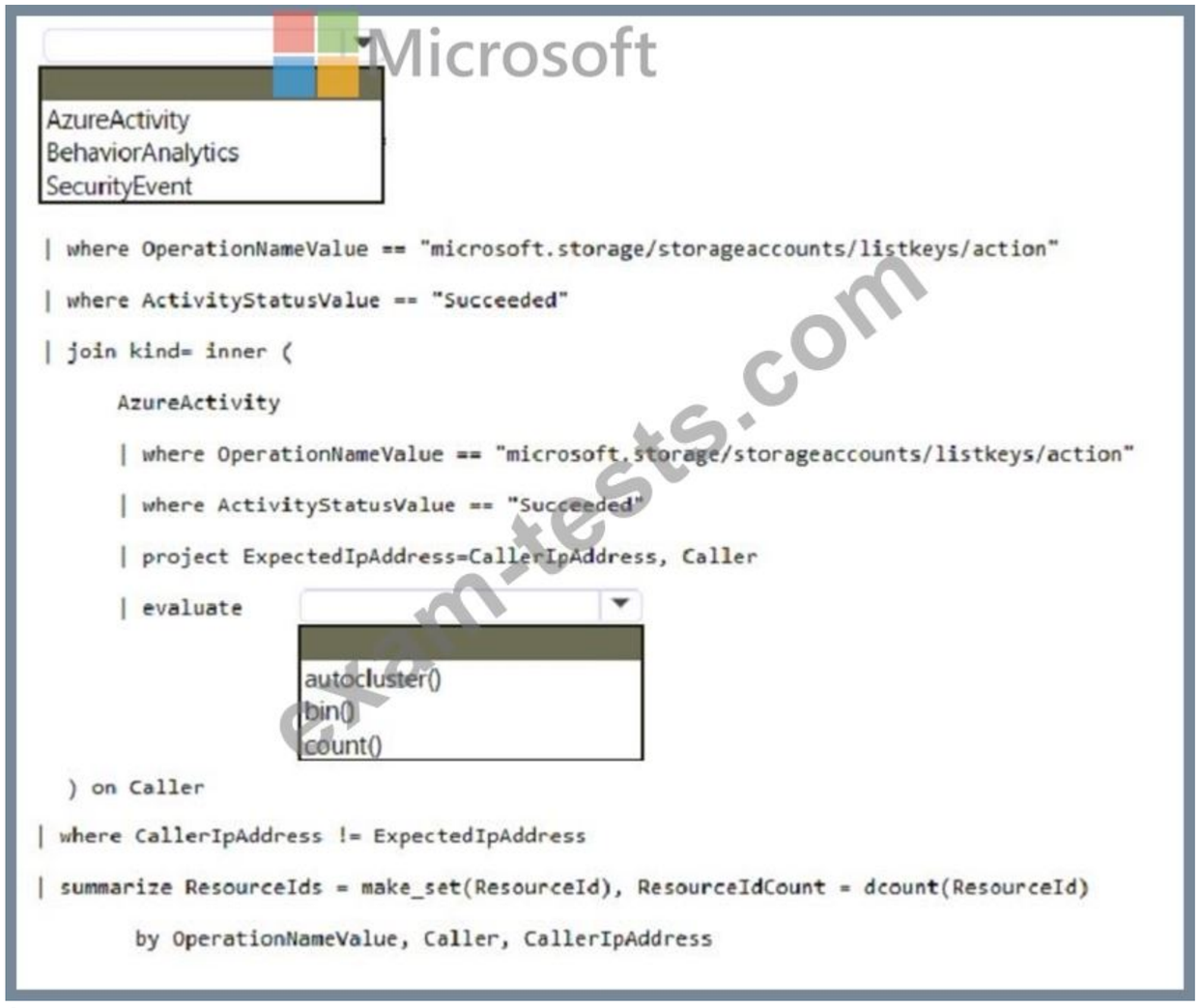
NEW QUESTION: 230
You need to implement Azure Defender to meet the Azure Defender requirements and the business requirements.
What should you include in the solution? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



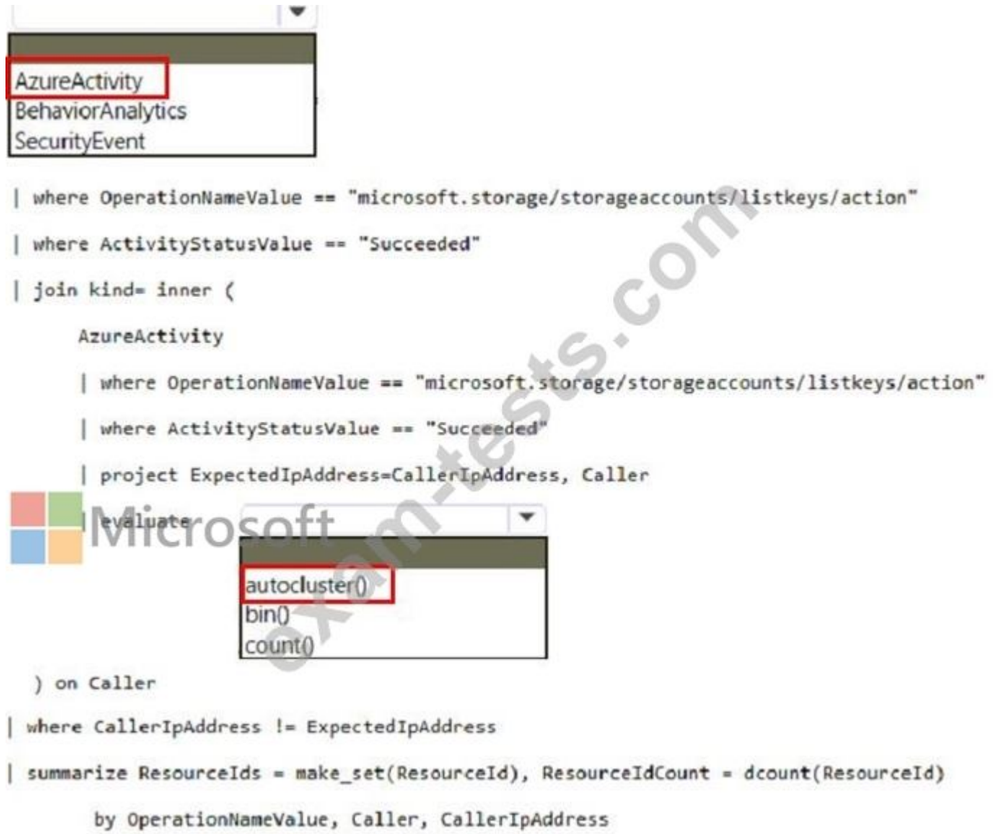
Answer:



NEW QUESTION: 231
You have a Microsoft Sentinel workspace named sws1.
You need to create a hunting query to identify users that list storage keys of multiple Azure Storage accounts. The solution must exclude users that list storage keys for a single storage account.
How should you complete the query? To answer, select the appropriate options in the answer area.



Answer:



NEW QUESTION: 232
Case Study 3 - Litware Inc
Overview
Fabrikam, Inc. is a financial services company.
The company has branch offices in New York, London, and Singapore. Fabrikam has remote users located across the globe. The remote users access company resources, including cloud resources, by using a VPN connection to a branch office.
Existing Environment
Identity Environment
The network contains an Active Directory Domain Services (AD DS) forest named fabrikam.com that syncs with an Azure AD tenant named fabrikam.com. To sync the forest, Fabrikam uses Azure AD Connect with pass-through authentication enabled and password hash synchronization disabled.
The fabrikam.com forest contains two global groups named Group1 and Group2.
Microsoft 365 Environment
All the users at Fabrikam are assigned a Microsoft 365 E5 license and an Azure Active Directory Premium Plan 2 license.
Fabrikam implements Microsoft Defender for Identity and Microsoft Defender for Cloud Apps and enables log collectors.
Azure Environment
Fabrikam has an Azure subscription that contains the resources shown in the following table.

Name	Type	Description
App1	Azure logic app	To automate incident generation in an internal ticketing system, the security operations (SecOps) team invokes App1 by using an HTTP endpoint.
SAWkspc1	Azure Synapse Analytics workspace	SAWkspc1 hosts an Apache Spark pool named Pool1.
LAWkspc1	Log Analytics workspace	LAWkspc1 will be used in a planned Microsoft Sentinel implementation.

Amazon Web Services (AWS) Environment

Fabrikam has an Amazon Web Services (AWS) account named Account1. Account1 contains 100 Amazon Elastic Compute Cloud (EC2) instances that run a custom Windows Server 2022. The image includes Microsoft SQL Server 2019 and does NOT have any agents installed.

Current Issues

When the users use the VPN connections, Microsoft 365 Defender raises a high volume of impossible travel alerts that are false positives.

Defender for Identity raises a high volume of Suspected DCSync attack alerts that are false positives.

Requirements

Planned changes

Fabrikam plans to implement the following services:

- Microsoft Defender for Cloud
- Microsoft Sentinel

Business Requirements

Fabrikam identifies the following business requirements:

- Use the principle of least privilege, whenever possible.
- Minimize administrative effort.

Microsoft Defender for Cloud Apps Requirements

Fabrikam identifies the following Microsoft Defender for Cloud Apps requirements:

- Ensure that impossible travel alert policies are based on the previous activities of each user.
- Reduce the amount of impossible travel alerts that are false positives.

Microsoft Defender for Identity Requirements

Minimize the administrative effort required to investigate the false positive alerts.

Microsoft Defender for Cloud Requirements

Fabrikam identifies the following Microsoft Defender for Cloud requirements:

- Ensure that the members of Group2 can modify security policies.
- Ensure that the members of Group1 can assign regulatory compliance policy initiatives at the Azure subscription level.
- Automate the deployment of the Azure Connected Machine agent for Azure Arc-enabled servers to the existing and future resources of Account1.
- Minimize the administrative effort required to investigate the false positive alerts.

Microsoft Sentinel Requirements

Fabrikam identifies the following Microsoft Sentinel requirements:

- Query for NXDOMAIN DNS requests from the last seven days by using built-in Advanced Security Information Model (ASIM) unifying parsers.

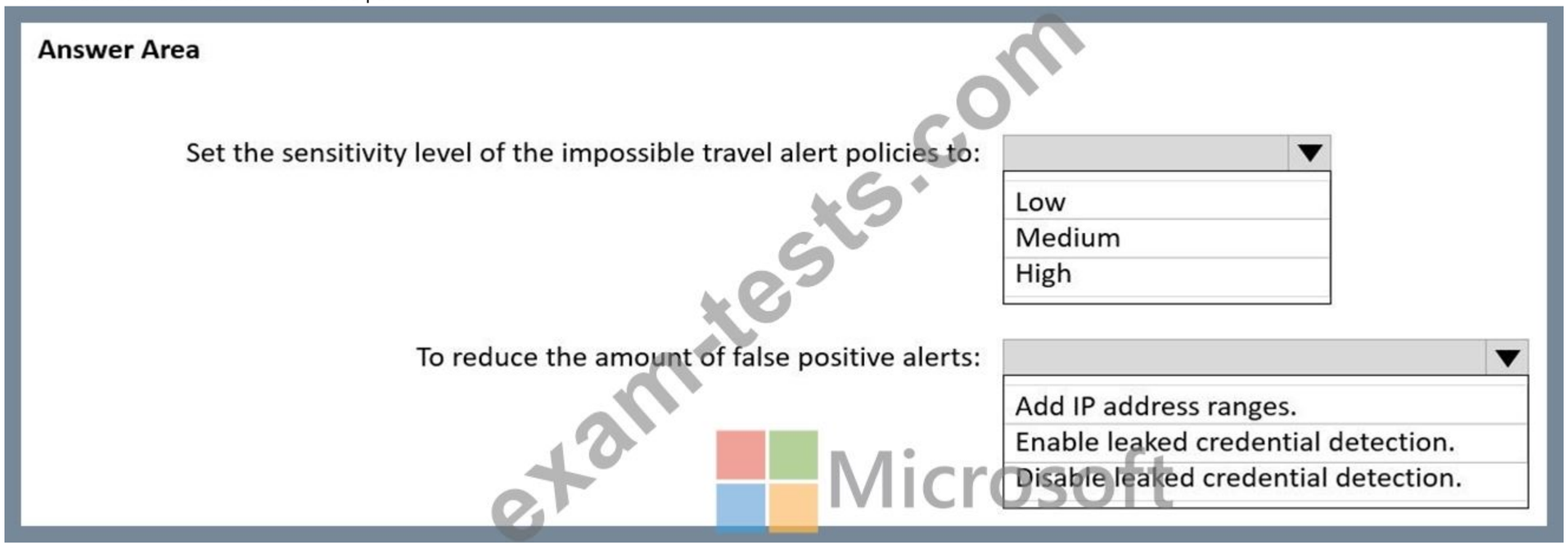
- From AWS EC2 instances, collect Windows Security event log entries that include local group membership changes.
- Identify anomalous activities of Azure AD users by using User and Entity Behavior Analytics (UEBA).
- Evaluate the potential impact of compromised Azure AD user credentials by using UEBA.
- Ensure that App1 is available for use in Microsoft Sentinel automation rules.
- Identify the mean time to triage for incidents generated during the last 30 days.
- Identify the mean time to close incidents generated during the last 30 days.
- Ensure that the members of Group1 can create and run playbooks.
- Ensure that the members of Group1 can manage analytics rules.
- Run hunting queries on Pool1 by using Jupyter notebooks.
- Ensure that the members of Group2 can manage incidents.
- Maximize the performance of data queries.
- Minimize the amount of collected data.

Hotspot Question

You need to meet the Microsoft Defender for Cloud Apps requirements.

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

NOTE: Each correct selection is worth one point.



Answer:

Answer Area

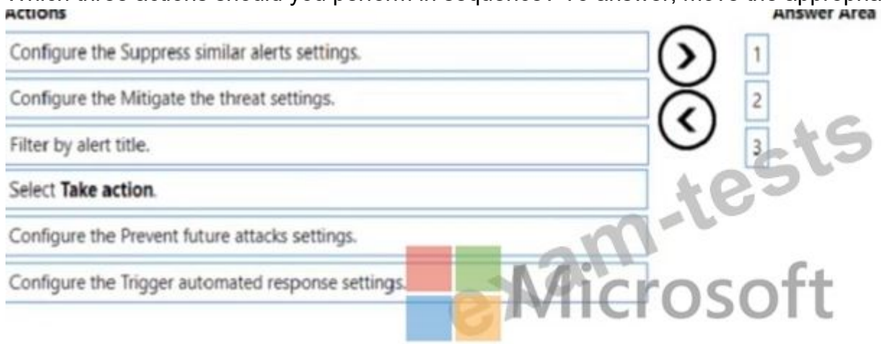
NEW QUESTION: 233

You have a Microsoft subscription that has Microsoft Defender for Cloud enabled You configure the Azure logic apps shown in the following table.

Name	Trigger	Action
LogicApp1	When a Defender for Cloud recommendation is created or triggered	Send an email
LogicApp2	When a Defender for Cloud alert is created or triggered	Send an email

You need to configure an automatic action that will run if a Suspicious process executed alert is triggered. The solution must minimize administrative effort.

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.



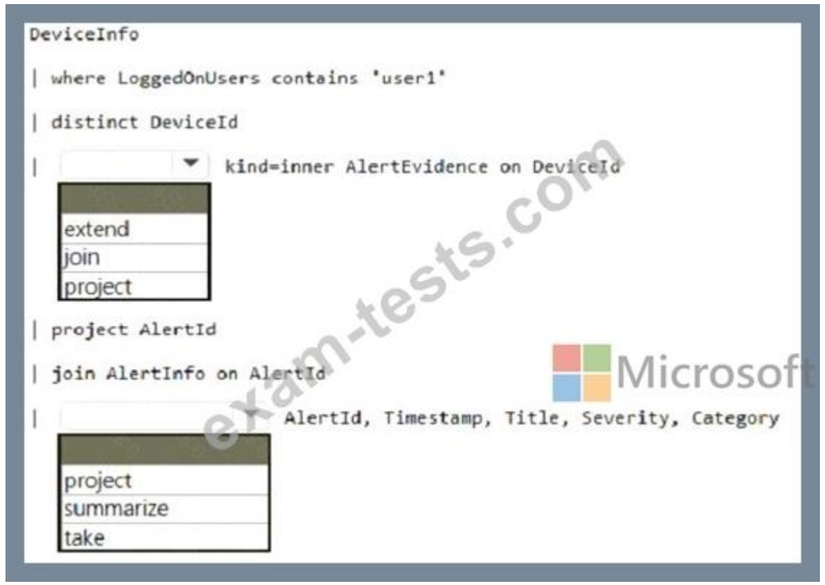
Answer:

1 - Configure teh Trigger automated respnse settings.
2 - Filter by alert title.
3 - Select Take Action

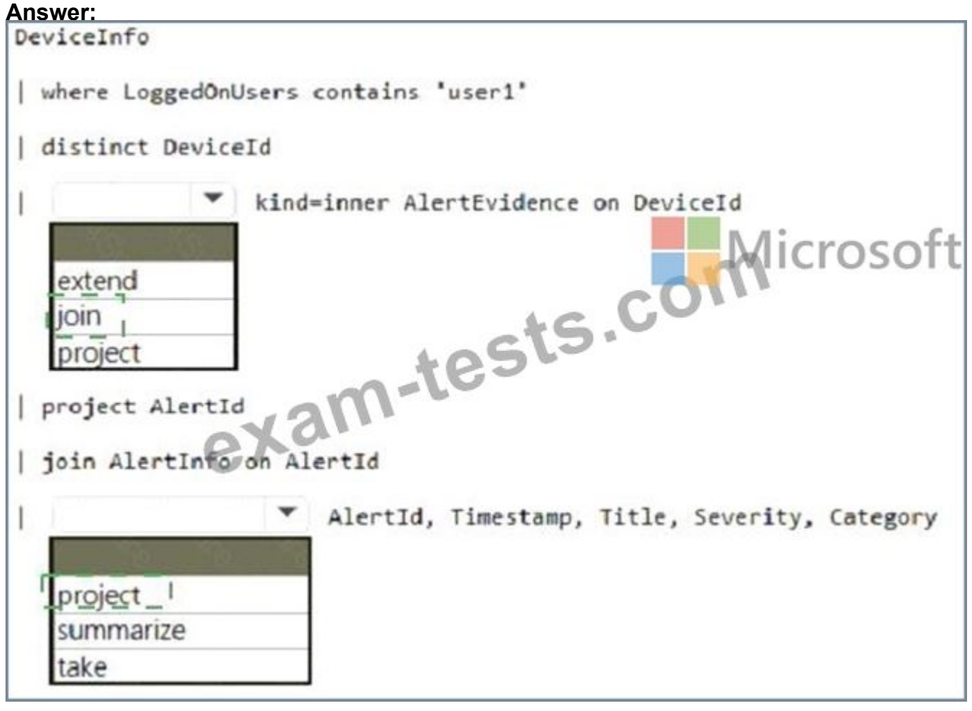
NEW QUESTION: 234
You have an Azure subscription that uses resource type for Cloud. You need to filter the security alerts view to show the following alerts:
* Unusual user accessed a key vault
* Log on from an unusual location
* Impossible travel activity
Which severity should you use?
A. Informational
B. Low
C. Medium
D. High
Answer: C (LEAVE A REPLY)
In Microsoft Defender for Cloud (and by extension Microsoft Defender XDR), each security alert is assigned a severity level based on the assessed risk, confidence, and potential impact. The severity levels are:
* High - Indicates a confirmed or severe threat (e.g., active malware, data exfiltration, privilege escalation).
* Medium - Indicates suspicious or anomalous activity that may require investigation but is not confirmed malicious.
* Low - Indicates be nign or informational activity with minimal risk.
* Informational - Alerts that provide context or enrichment but are not threats.
The alerts listed in the question -
* Unusual user accessed a key vault
* Log on from an unusual location
* Impossible travel activity -
are all behavioral anomaly detections generated by Defender for Cloud and Defender for Cloud Apps using machine learning and user behavior analytics (UEBA) . Microsoft classifies such anomaly-based detections as Medium severity by default, becaus e they represent potentially risky activity that might indicate compromise but are not confirmed attacks.
According to Microsoft's official documentation for Defender for Cloud alert severity classification:
"Medium severity alerts indicate suspicious acti vities that might represent legitimate anomalies or early stages of a potential attack, such as impossible travel, unusual sign-in location, or abnormal resource access." Thus, when filtering the Security Alerts view to include those specific anomaly-based alerts, the correct severity filter to use is:
Medium

NEW QUESTION: 235
You have a Microsoft 365 subscription that uses Microsoft 365 Defender and contains a user named User1.

You are notified that the account of User1 is compromised.
You need to review the alerts triggered on the devices to which User1 signed in.
How should you complete the query? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



Answer:



Explanation
Box 1: join
An inner join.
This query uses kind=inner to specify an inner-join, which prevents deduplication of left side values for DeviceId.
This query uses the DeviceInfo table to check if a potentially compromised user (<account-name>) has logged on to any devices and then lists the alerts that have been triggered on those devices.
DeviceInfo
//Query for devices that the potentially compromised account has logged onto
| where LoggedOnUsers contains '<account-name>'
| distinct DeviceId
//Crosscheck devices against alert records in AlertEvidence and AlertInfo tables
| join kind=inner AlertEvidence on DeviceId
| project AlertId
//List all alerts on devices that user has logged on to
| join AlertInfo on AlertId
| project AlertId, Timestamp, Title, Severity, Category
DeviceInfo LoggedOnUsers AlertEvidence "project AlertID"
Box 2: project
Reference:
https://docs.microsoft.com/en-us/microsoft-365/security/defender/advanced-hunting-query-emails-devices?view=

NEW QUESTION: 236
Hotspot Question
You have an Azure subscription that uses Microsoft Defender for Cloud.
You need to use an Azure Resource Manager (ARM) template to create a workflow automation that will trigger a logic app when specific alerts are received by Microsoft Defender for Cloud.
How should you complete the template? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Answer Area

```
{
  ...
  "resources": [
    {
      "type": [                                  ] /automations",
      "apiVersion": "2019-01-01-preview",
      "name": "[parameters('automationName')]",
      "location": "[parameters('location')]",
      "properties": {
        "description": "[format(variables('automationDescription'),'{0}', parameters('subscriptionId'))]",
        "isEnabled": true,
        "actions": [
          {
            "actionType": "LogicApp",
            "logicAppResourceId": "[resourceId('                                  ] /workflows', parameters('logicAppName'))]",
            "uri": "[listCallbackURL(resourceId(parameters('subscriptionId'), parameters('logicAppResourceGroupName'),
  ...
}
```

- Microsoft.AlertsManagement
- Microsoft.Automation
- Microsoft.Logic
- Microsoft.Security

Answer:

```
{
  ...
  "resources": [
    {
      "type":                                                    /automations",
      "apiVersion": "2019-01-01-preview",
      "name": "[parameters('automationName')]",
      "location": "[parameters('location')]",
      "properties": {
        "description": "[format(variables('automationDescription'),'{0}', parameters('subscriptionId'))]",
        "isEnabled": true,
        "actions": [
          {
            "actionType": "LogicApp",
            "logicAppResourceId": "[resourceId('                                    /workflows', parameters('logicAppName'))]",
            "uri": "[listCallbackURL(resourceId(parameters('subscriptionId'), parameters('logicAppResourceGroupName'),
  ...
}
```

- Microsoft.AlertsManagement
- Microsoft.Automation
- Microsoft.Logic
- Microsoft.Security

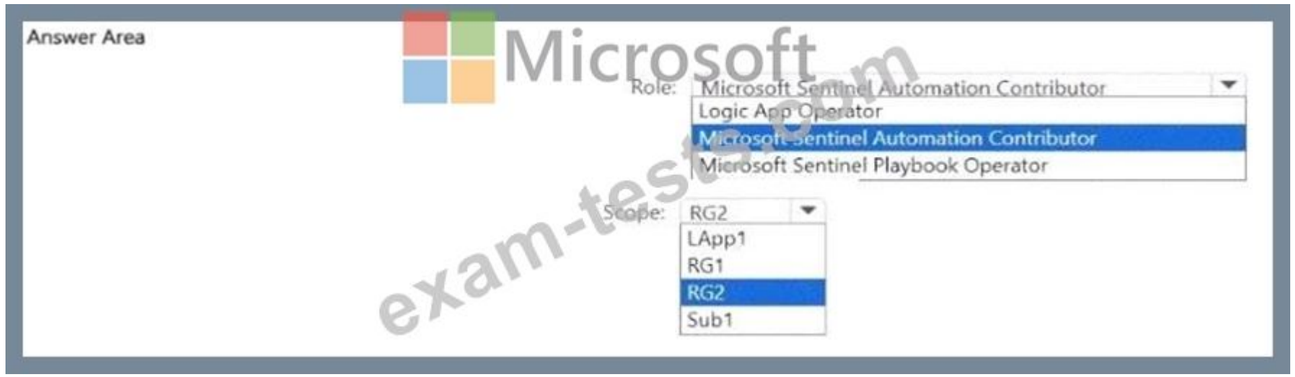
- Microsoft.AlertsManagement
- Microsoft.Automation
- Microsoft.Logic
- Microsoft.Security

NEW QUESTION: 237

You have an Azure subscription named Sub1 that contains the resources shown in the following table.

Name	Type	Resource group	Description
WS1	Microsoft Sentinel workspace	RG1	Contains a scheduled query rule named Rule1
LApp1	Azure logic app	RG2	Contains a Microsoft Sentinel incident trigger

You plan to configure Rule1 to trigger Lapp1 when an incident is generated.
You need to recommend the role-based access control (RBAC) role that you should assign to WS1, and the scope at which should you assign the role. The solution must follow the principle of least privilege.
What should you recommend? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



Answer:

Explanation:

NEW QUESTION: 238
You have a Microsoft Sentinel workspace that contains the following Advanced Security Information Model (ASIM) parsers:
* _Im_ProcessCreate
* InProceessCreate
You create a new source-specific parser named vimProcessCreate.
You need to modify the parsers to meet the following requirements:
* Call all the ProcessCreate parsers.
* Standardize fields to the Process schema.

Which parser should you modify to meet each requirement? To answer, drag the appropriate parsers to the correct requirements. tach parser 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.

Answer:

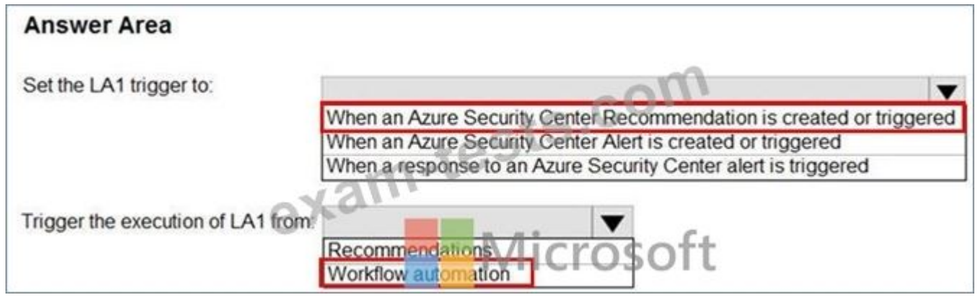
Explanation:

Microsoft Sentinel uses the Advanced Security Information Model (ASIM) to normalize logs into a consistent schema, enabling unified queries, analytics rules, and hunting queries across multiple data sources.
Each ASIM function has a structured parser hierarchy, typically consisting of:
* A master (or orchestrator) parser, which aggregates and calls all source-specific parsers.
* Source-specific parsers, which map raw data from each data source (like Windows SecurityEvents, Sysmon, or custom logs) to the ASIM schema fields.
In the case of ProcessCreate events:
* _Im_ProcessCreate is the master parser. Its role is to call all ProcessCreate parsers, including both built- in and custom ones (for example, imProcessCreate, vimProcessCreate, or other vendor-specific parsers).
* Parsers like imProcessCreate (for native sources) and vimProcessCreate (for custom or vendor-specific sources) are source-specific parsers. They are responsible for standardizing and mapping raw fields into the ASIM Process schema, ensuring consistent naming such as ActorProcessName, TargetProcessName, and TargetProcessCommandLine.
"The _Im_ functions are orchestrators that call all source-specific parsers. Each im or vim parser converts native data into the ASIM schema for its respective source." Therefore:
* To call all ProcessCreate parsers, modify _Im_ProcessCreate.
* To standardize fields to the Process schema, modify vimProcessCreate (the new source-specific parser you created).
# Final Answers:
* Call all the ProcessCreate parsers: _Im_ProcessCreate
* Standardize fields to the Process schema: vimProcessCreate

NEW QUESTION: 239
You have an Azure subscription that has Azure Defender enabled for all supported resource types.

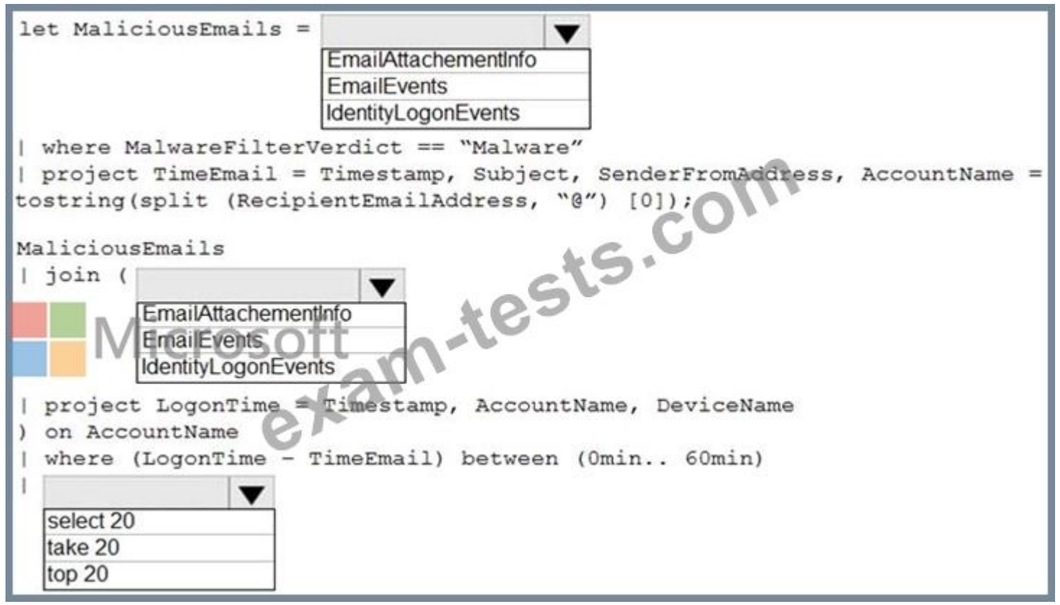
You create an Azure logic app named LA1.
You plan to use LA1 to automatically remediate security risks detected in Azure Security Center.
You need to test LA1 in Security Center.
What should you do? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Answer:

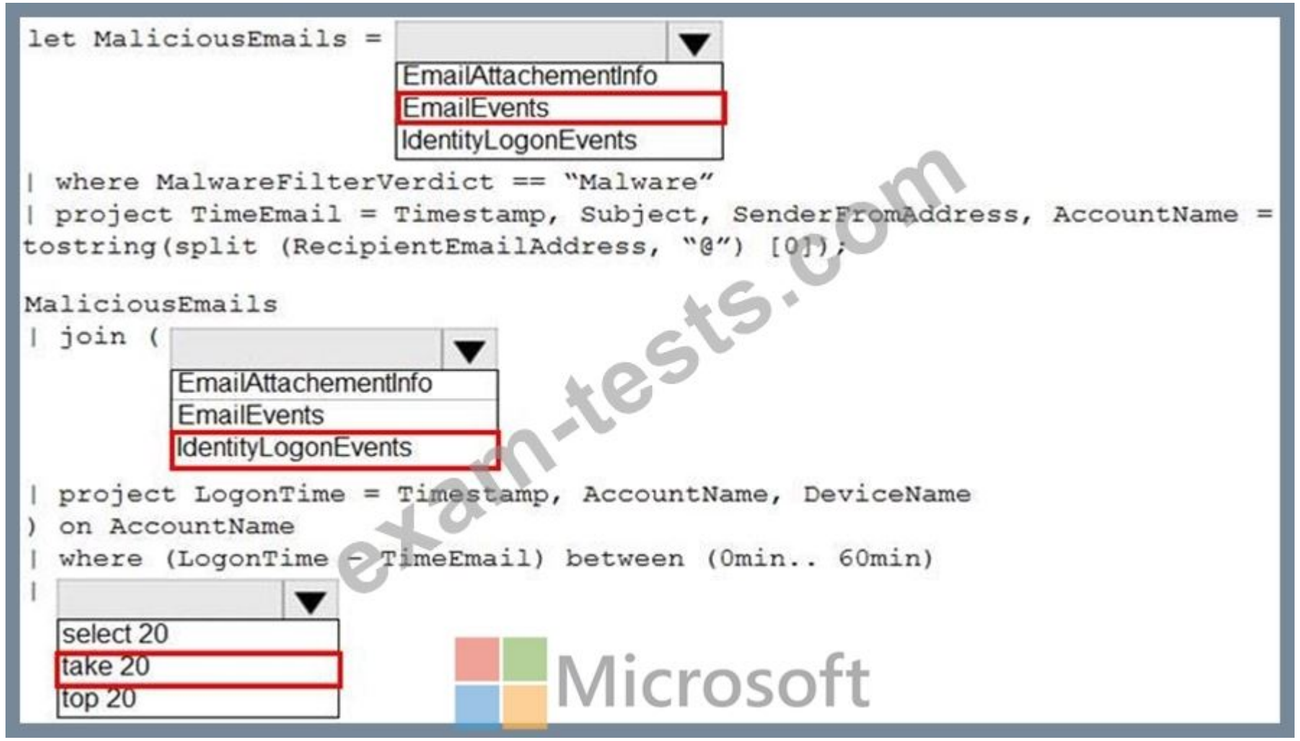


Reference:
https://docs.microsoft.com/en-us/azure/security-center/workflow-automation#create-a-logic-app-and-define-when-it-should-automatically-run

NEW QUESTION: 240
You are informed of an increase in malicious email being received by users.
You need to create an advanced hunting query in Microsoft 365 Defender to identify whether the accounts of the email recipients were compromised. The query must return the most recent 20 sign-ins performed by the recipients within an hour of receiving the known malicious email.
How should you complete the query? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

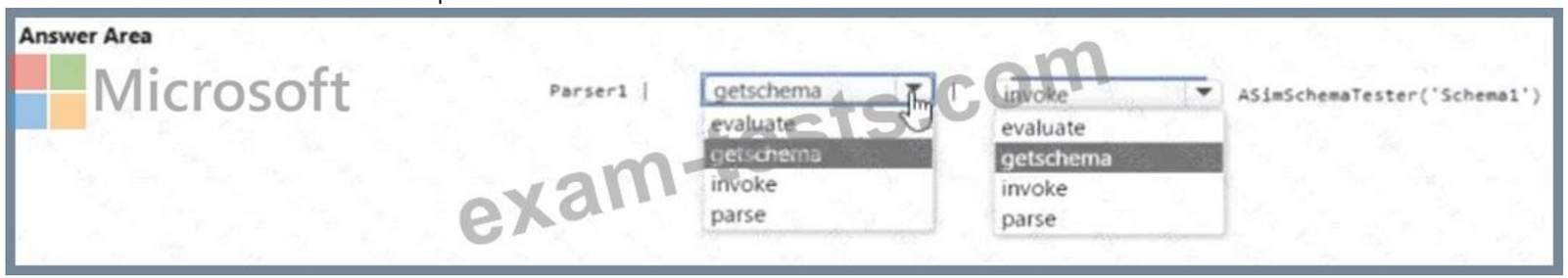


Answer:

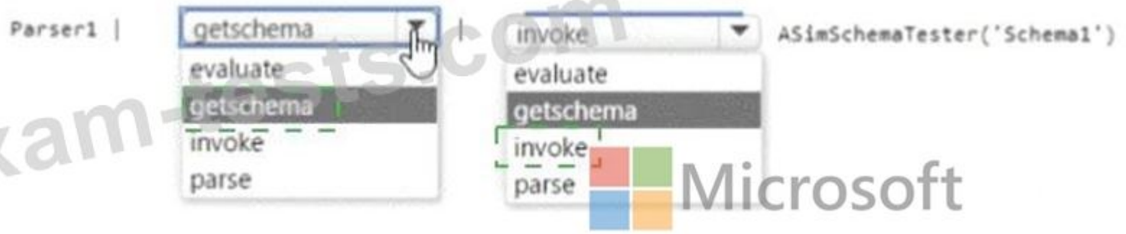


Reference:
https://docs.microsoft.com/en-us/microsoft-365/security/defender/advanced-hunting-query-emails-devices?view=o365-worldwide

NEW QUESTION: 241
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:
Answer Area



Explanation:

To validate a custom ASIM parser output, you test that the parser's resulting table structure complies with the intended ASIM schema . In KQL, the getschema operator produces a tabular representation of the current pipeline's schema (column names, types, order). The invoke operator is then used to call a function on that tabular input. ASIM provides the helper function ASimSchemaTester() , which accepts the schema table and the target schema name and validates that the input conforms (columns exist, types match, required fields are present).
Therefore, the correct construction is to run the parser (here, Parser1), pipe its output to getschema to obtain the schema of the produced table, and then invoke ASimSchemaTester(' Schema1 ') to perform the validation. Other options are not appropriate: evaluate is for plugins; parse extracts fields from strings rather than validate schema; and calling the tester without getschema would not pass the required schema table.
Hence, the correct command is:
Parser1 | getschema | invoke ASimSchemaTester(' Schema1 ') .

NEW QUESTION: 242

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.

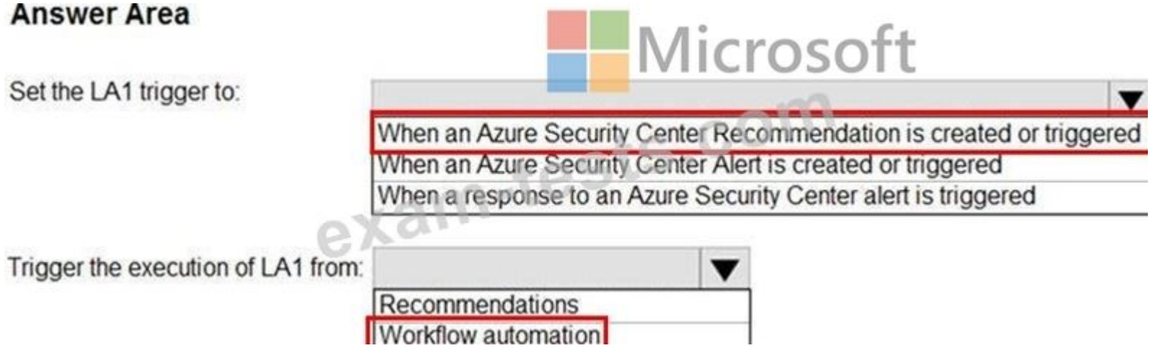
View the window

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:

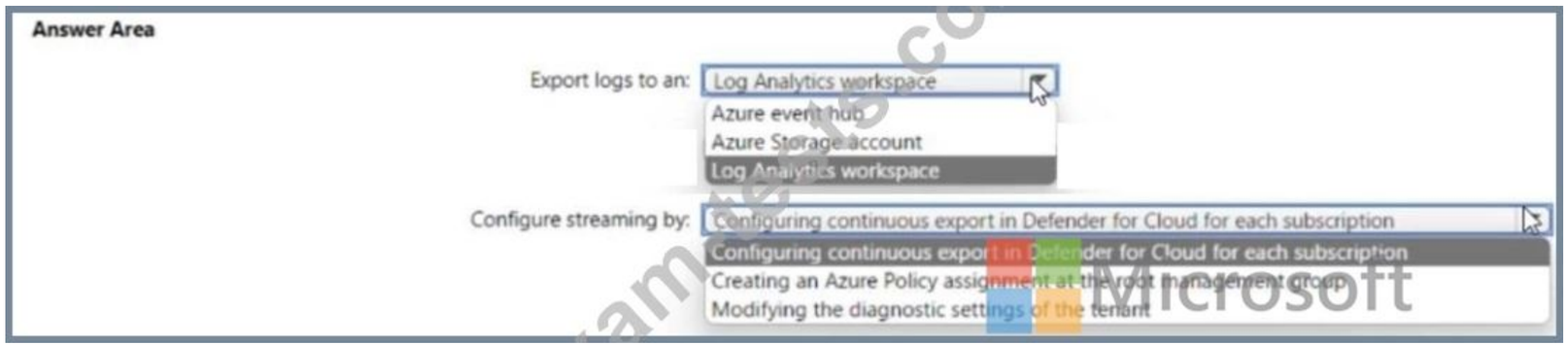


Reference:

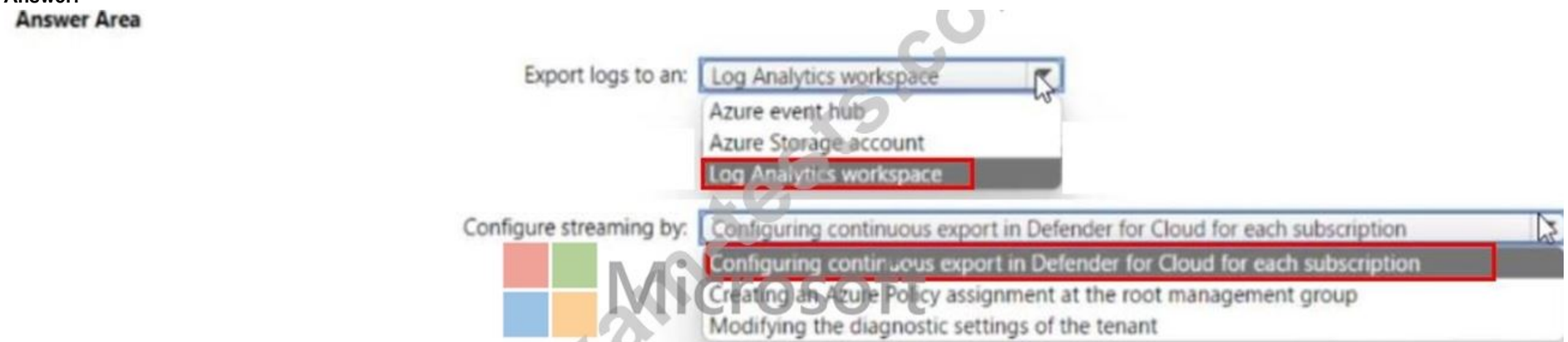
https://docs.microsoft.com/en-us/azure/security-center/workflow-automation#create-a-logic-app-and-define-when-it-should-automatically-run

NEW QUESTION: 243

You have 100 Azure subscriptions that have enhanced security features m Microsoft Defender for Cloud enabled. All the subscriptions are linked to a single Azure AD tenant. You need to stream the Defender for Cloud togs 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:



NEW QUESTION: 244

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 All Events

B. From the Microsoft Endpoint Manager admin center, enable automatic enrollment.

C. From the workspace created by Defender for Cloud, set the data collection level to Common

D. From the Azure portal, create an Azure Event Grid subscription.

E. From Defender for Cloud in the Azure portal, enable automatic provisioning for the virtual machines.

Answer: A,E (LEAVE A REPLY)

NEW QUESTION: 245

You have a Microsoft 365 E5 subscription.

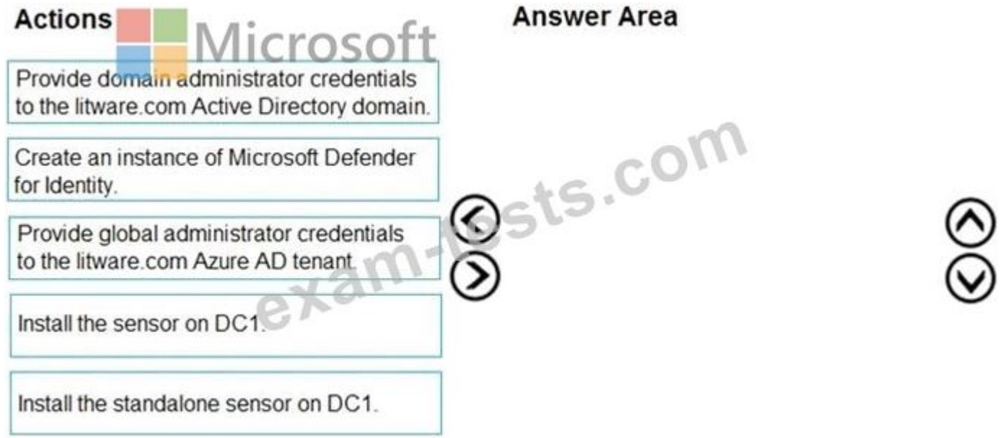
You have 1,000 Windows devices that have a third-party antivirus product installed and Microsoft Defender Antivirus in passive mode.

All Windows devices are on boarded to Microsoft Defender for Endpoint.

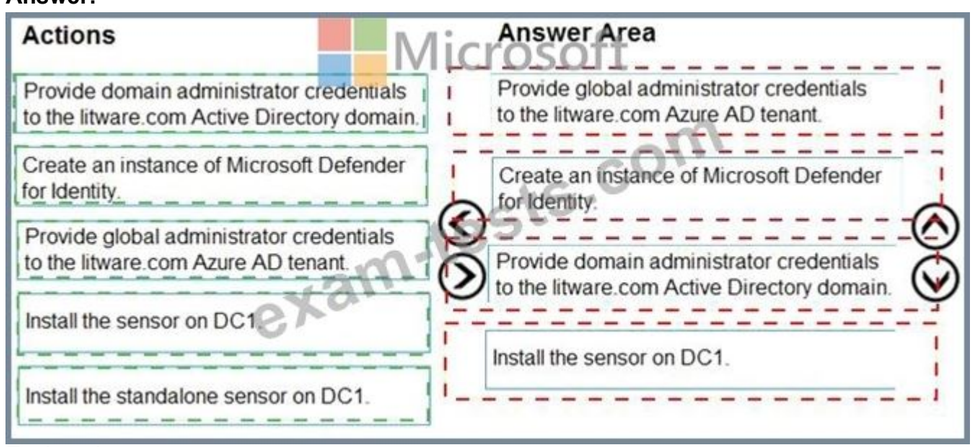
You need to ensure that the devices are protected from malicious artifacts that were undetected by the third- party antivirus product.

Solution: You enable Live Response.
Does this meet the goal?
A. Yes
B. No
Answer: (SHOW ANSWER)
Live Response in Microsoft Defender for Endpoint is a powerful investigative and remediation capability that lets responders interactively run commands on an endpoint, collect files, and perform remediation steps (collect investigation packages, pull files, run scripts, or take forensic artifacts). However, Live Response is an on-demand tool invoked during or after an investigation; it does not by itself provide continuous detection coverage or automatic blocking of artifacts that a third-party AV missed. The requirement is to ensure devices are protected from malicious artifacts that were undetected by the third-party antivirus. To meet that objective you need capabilities that detect and block artifacts automatically (for example, EDR in block mode which actively blocks/remediates post-breach artifacts even when Defender AV is passive). Live Response helps respond to an identified artifact but does not create the detection and automatic blocking coverage that prevents or remediate undetected malicious artifacts at scale. Therefore enabling Live Response alone does not meet the stated protection goal.

NEW QUESTION: 246
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.



Answer:

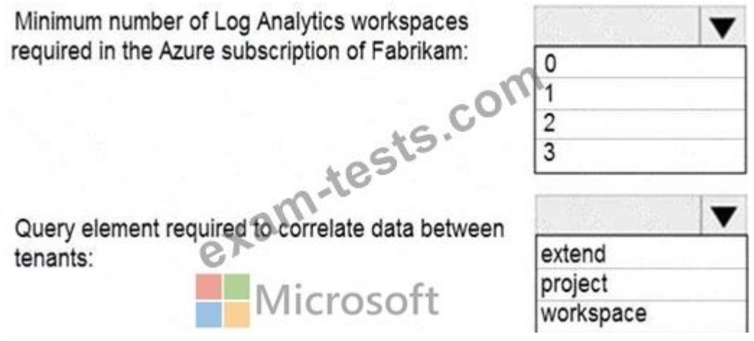


Explanation

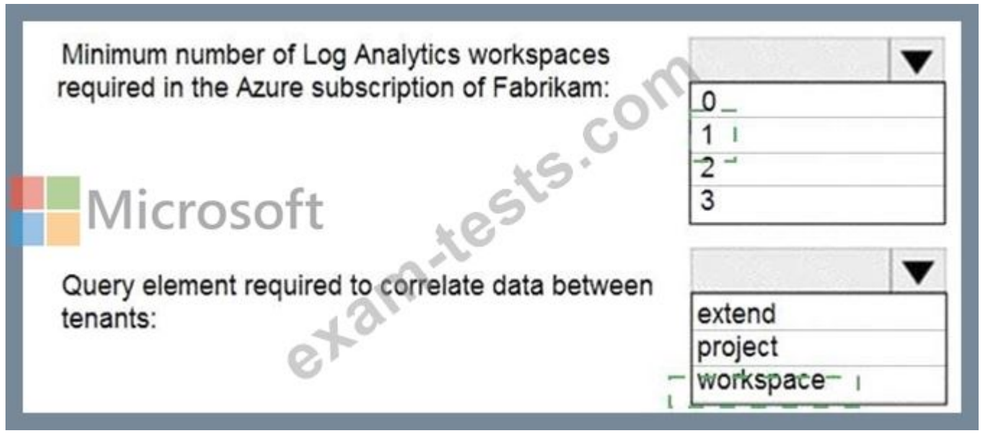
Text Description automatically generated with medium confidence

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.
Reference:
https://docs.microsoft.com/en-us/defender-for-identity/install-step1
https://docs.microsoft.com/en-us/defender-for-identity/install-step4

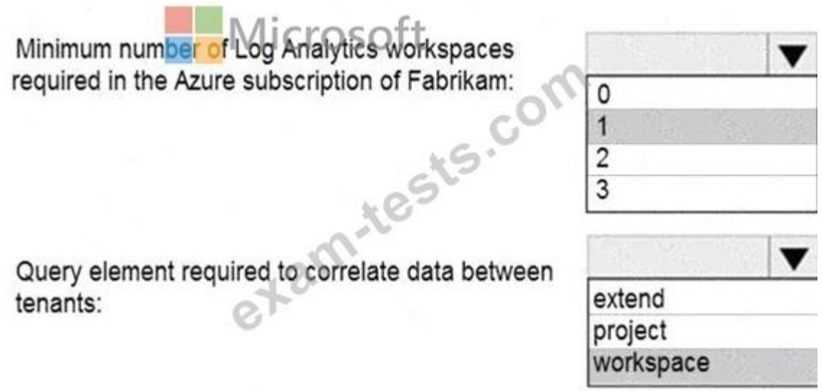
NEW QUESTION: 247
You need to implement Azure Sentinel queries for Contoso and Fabrikam to meet the technical requirements.
What should you include in the solution? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



Answer:



Explanation:

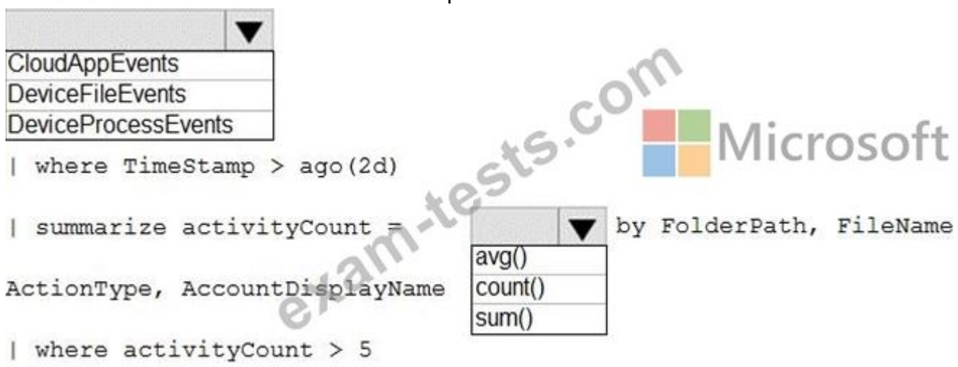


In Microsoft Sentinel (built on Azure Monitor Logs), analytics and hunting queries are executed within a Log Analytics workspace. To run Sentinel queries for Fabrikam, the tenant must have at least one workspace (with Sentinel enabled) in its subscription to host rules, incidents, hunting queries, and workbooks. Sentinel's cross-workspace/tenant capability is provided by cross-resource queries in Kusto Query Language (KQL).
The key construct for reaching outside the current workspace is the workspace() function, which lets you reference another Log Analytics workspace by name or resource ID-even across subscriptions or tenants when proper permissions (often via Azure Lighthouse or guest access) are in place.
Typical correlation looks like:
union workspace('Fabrikam-WS').SecurityEvent, workspace('Contoso-WS').SecurityEvent | ...
Here, workspace() is the required element to bring together data sets from multiple tenants; operators like extend and project only shape columns and do not establish cross-tenant scope. Therefore, to meet the requirements with minimal overhead: Fabrikam needs one workspace to host its Sentinel content, and you use workspace() in your KQL to correlate Contoso and Fabrikam data.

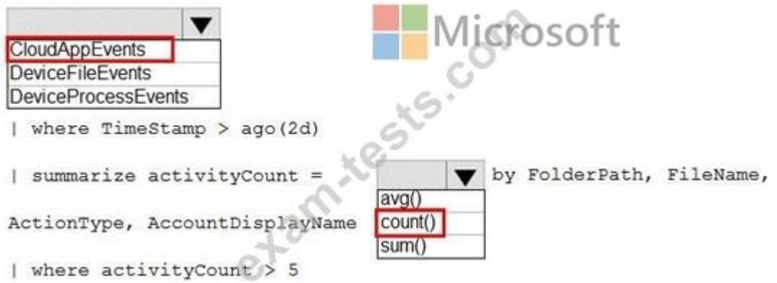
NEW QUESTION: 248
You have a Microsoft 365 E5 subscription that contains a device named Device1.
From the Microsoft Defender portal, you discover that an alert was triggered for Device1.
From the Device inventory page, you isolate Device1.
You need to collect a list of installed programs on Device1.
What should you do?
A. Collect an investigation package and download the results from the Action center.

B. Initiate a live response session and run the analyze command.
C. Run an advanced hunting query against the DeviceTvmInfoGathering table.
D. Run an advanced hunting query against the DeviceProcessEvents table.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 249
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.



Answer:

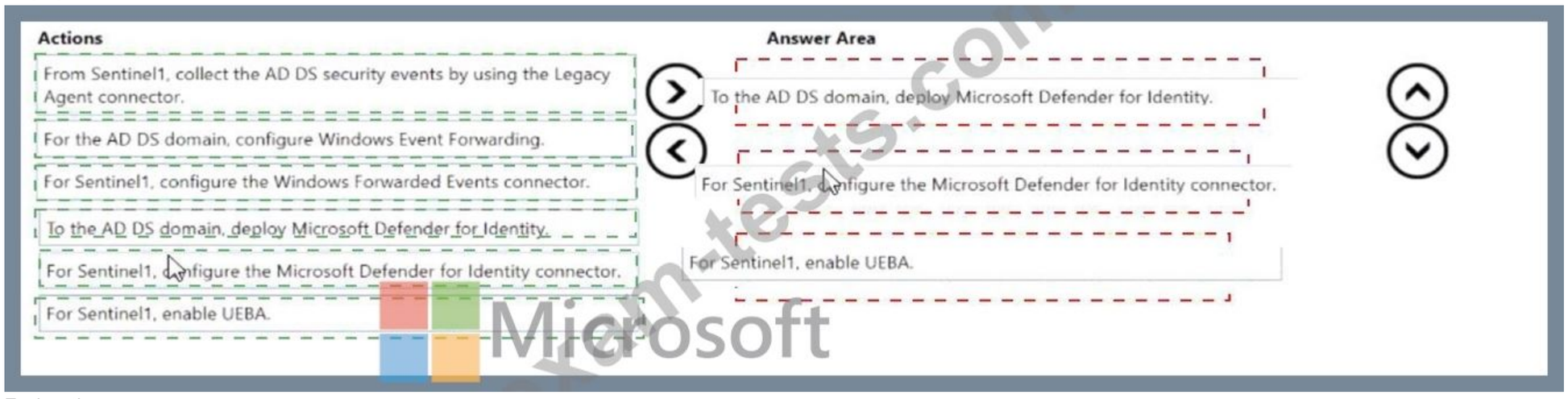


NEW QUESTION: 250
You have an Azure subscription named Sub1 and a Microsoft 365 subscription. Sub1 is linked to an Azure Active Directory (Azure AD) tenant named contoso.com.
You create an Azure Sentinel workspace named workspace1. In workspace1, you activate an Azure AD connector for contoso.com and 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: A,B (LEAVE A REPLY)
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.

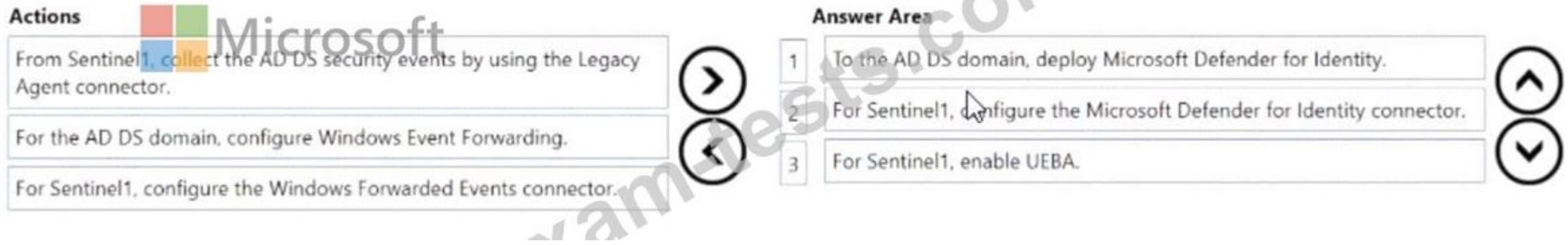
Create a custom rule based on the Office 365 connector templates. This will allow you to monitor and detect anomalous activities in the Microsoft 365 subscription. Reference: https://docs.microsoft.com/en-us/azure/sentinel/fusion-rules

NEW QUESTION: 251
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.

Answer:



Explanation:



NEW QUESTION: 252
Your company uses Microsoft Defender for Endpoint.
The company has Microsoft Word documents that contain macros. The documents are used frequently on the devices of the company's accounting team.
You need to hide false positive in the Alerts queue, while maintaining the existing security posture. Which three actions should you perform? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.
A. Resolve the alert automatically.
B. Hide the alert.
C. Create a suppression rule scoped to any device.
D. Create a suppression rule scoped to a device group.
E. Generate the alert.
Answer: B,C,E (LEAVE A REPLY)
Reference:
https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/manage-alerts

NEW QUESTION: 253
You have multiple Azure subscriptions that contain multiple Microsoft Sentinel workspaces.
You are creating a Microsoft Sentinel workbook that will include references to the AzureActivity table.
You need to create a KQL query that will perform the following actions:
. Check whether the AzureActivity table exists in each workspace.
. If the table exists, return a single row that has the isMissing column set to 0.
. If the table does NOT exist, return a single row that has the isMissing column set to 1.
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:

Explanation:

let mTable = makelist(isMissing:int) [1];

The union kind=outer statement combines results from both branches.

NEW QUESTION: 254

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.	○	○

Answer:

Explanation:

NEW QUESTION: 255

Hotspot Question

You have a Microsoft 365 E5 subscription that contains the hosts shown in the following table.

Name	Platform	Device group
Host1	Windows 11	DG1
Host2	Windows 11	DG2
Host3	macOS	DG1

You have indicators in Microsoft Defender for Endpoint as shown in the following table.

Name	Value	Type	Expiration date (UTC)	Action	Organization scope
ID1	b94d27b9934d3e08a52e52d7da7dabfac484efe37a5380ee9088f7ace2efcde9	SHA-256	Sep 15, 2026	Block and remediate	DG2
ID2	b94d27b9934d3e08a52e52d7da7dabfac484efe37a5380ee9088f7ace2efcde9	SHA-256	*None*	Allow	DG1
ID3	2aae6c35c94fcfb415dbe95f408b9ce91ee846ed	SHA-1	Jan 1, 2026	Block execution	DG1, DG2
ID4	88d4266fd4e6338d13b845fcf289579d209c897823b9217da3e161936f031589	SHA-256	*None*	Block execution	DG1

ID1 and ID2 reference the same file as ID3.

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
Host1 will block the execution of a file that has the SHA-1 hash value of 2aae6c35c94fcfb415dbe95f408b9ce91ee846ed.	○	○
Host2 will block and remediate a file that has the SHA-256 hash value of 88d4266fd4e6338d13b845fcf289579d209c897823b9217da3e161936f031589.	○	○
Host3 will block the execution of a file that has the SHA-256 hash value of 88d4266fd4e6338d13b845fcf289579d209c897823b9217da3e161936f031589.	○	○

Answer:

Answer Area

Statements	Yes	No
Host1 will block the execution of a file that has the SHA-1 hash value of 2aae6c35c94fcfb415dbe95f408b9ce91ee846ed.	○	○
Host2 will block and remediate a file that has the SHA-256 hash value of 88d4266fd4e6338d13b845fcf289579d209c897823b9217da3e161936f031589.	○	○
Host3 will block the execution of a file that has the SHA-256 hash value of 88d4266fd4e6338d13b845fcf289579d209c897823b9217da3e161936f031589.	○	○

NEW QUESTION: 256
You have a Microsoft 365 E5 subscription that uses Microsoft SharePoint Online.
You delete users from the subscription.
You need to be notified if the deleted users downloaded numerous documents from SharePoint Online sites during the month before their accounts were deleted.
What should you use?
A. an alert policy in Microsoft Defender for Office 365
B. a file policy in Microsoft Defender for Cloud Apps
C. an insider risk policy
D. an access review policy
Answer: (SHOW ANSWER)
Alert policies let you categorize the alerts that are triggered by a policy, apply the policy to all users in your organization, set a threshold level for when an alert is triggered, and decide whether to receive email notifications when alerts are triggered.
Default alert policies include:
Unusual external user file activity - Generates an alert when an unusually large number of activities are performed on files in SharePoint or OneDrive by users outside of your organization. This includes activities such as accessing files, downloading files, and deleting files. This policy has a High severity setting.

NEW QUESTION: 257
You have the following advanced hunting query in Microsoft 365 Defender.

```
DeviceProcessEvents
| where Timestamp > ago (24h)
and InitiatingProcessFileName =~ 'runsll32.exe'
and InitiatingProcessCommandLine !contains "" and InitiatingProcessCommandLine != ""
and FileName in~ ('schtasks.exe')
and ProcessCommandLine has 'Change' and ProcessCommandLine has 'SystemRestore'
and ProcessCommandLine has 'disable'
| project Timestamp, AccountName, ProcessCommandLine
```

You need to receive an alert when any process disables System Restore on a device managed by Microsoft Defender during the last 24 hours.

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 detection rule.

B. Create a suppression rule.

C. Add | order by Timestamp to the query.

D. Block DeviceProcessEvents with DeviceNetworkEvents.

E. Add DeviceId and ReportId to the output of the query.

Answer: A,E (LEAVE A REPLY)

Reference:

https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/custom-detection- rules

NEW QUESTION: 258

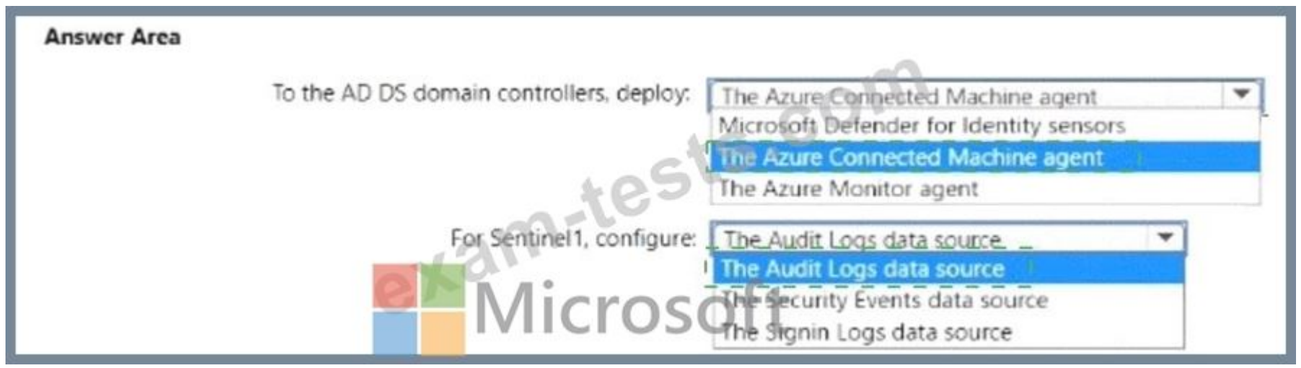
You have an Azure subscription that is linked to a hybrid Azure AD tenant and contains a Microsoft Sentinel workspace named Sentinel1.

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:



Explanation:

NEW QUESTION: 259

You have an Azure subscription that contains a user named User1 and a Microsoft Sentinel workspace named WS1.

You need to ensure that User1 can enable User and Entity Behavior Analytics (UEBA) for WS1. The solution must follow 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:

Explanation:

NEW QUESTION: 260

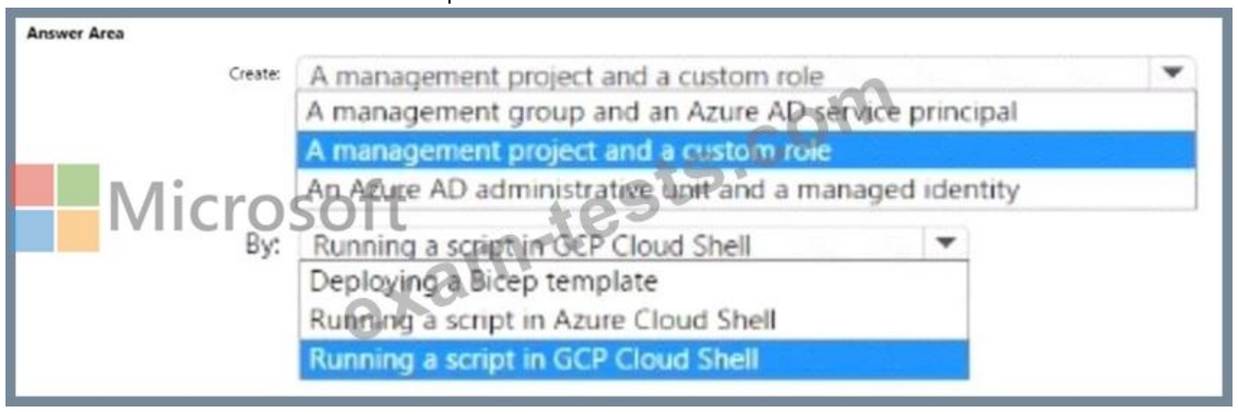
You have an Azure subscription that uses Microsoft Defender for Cloud.

You create a Google Cloud Platform (GCP) organization named GCP1.

You need to onboard GCP1 to Defender for Cloud by using the native cloud connector. The solution must ensure that all future GCP projects are onboarded automatically.

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

NOTE: Each correct selection is worth one point.



Answer:

Explanation

NEW QUESTION: 261

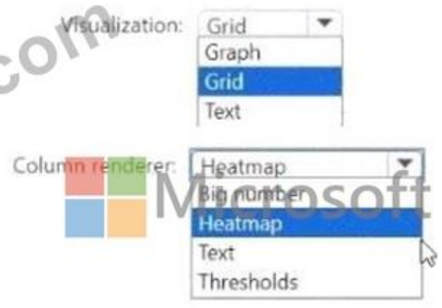
You have a Microsoft Sentinel workbook that contains the following KQL query.

```
let nonInteractive = AADNonInteractiveUserSignInLogs
| extend Status = parse_json(Status)
union SigninLogs,nonInteractive
| extend ErrorCode = tostring(Status.errorCode)
| extend FailureReason = tostring(Status.failureReason)
| summarize errCount = count() by ErrorCode, FailureReason, Category
```

You need to create a visual that will change the color of the errCount column based on the value returned.

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

Answer Area



Answer:

Explanation:

In Microsoft Sentinel workbooks, when you want to display query results in a tabular format and visually emphasize numeric values through color intensity (such as counts or frequencies), you use the Grid visualization type combined with the Heatmap column renderer.

In this scenario, the query aggregates failed sign-in events from SigninLogs and AADNonInteractiveUserSignInLogs, summarizing them by ErrorCode, FailureReason, and Category with a calculated count (errCount). The errCount column holds numeric data that indicates how many times each unique failure pattern occurred.

To visually represent the severity or frequency of these counts, you configure:

* Visualization = Grid - Displays tabular data in a workbook. It's the standard view type for showing multiple columns of query output (such as error codes and counts).

* Column renderer = Heatmap - Applies a gradient color scheme to the selected numeric column (errCount) so that higher values are highlighted with darker or more intense colors, making patterns or anomalies easier to spot.

Microsoft Sentinel workbook documentation explains:

"Heatmap rendering can be applied to numerical columns in Grid visualizations to provide color-coded representation of value ranges." Alternative renderers like Text or Big number do not provide dynamic color intensity, and Thresholds are used for conditional formatting rather than continuous color gradients.

Final configuration:

* Visualization: Grid

* Column renderer: Heatmap

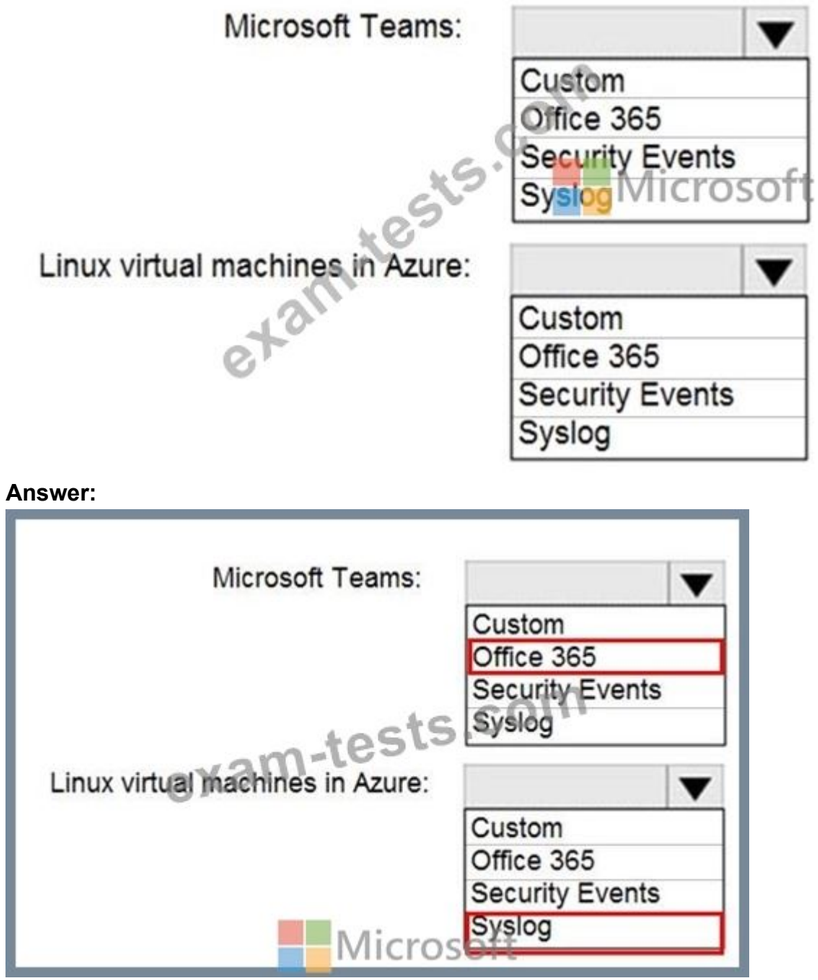
NEW QUESTION: 262

You deploy Azure Sentinel.

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

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

NOTE: Each correct selection is worth one point.



Answer:

Reference:
https://docs.microsoft.com/en-us/azure/sentinel/connect-office-365
https://docs.microsoft.com/en-us/azure/sentinel/connect-syslog

NEW QUESTION: 263
Drag and Drop Question
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

Answer:

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

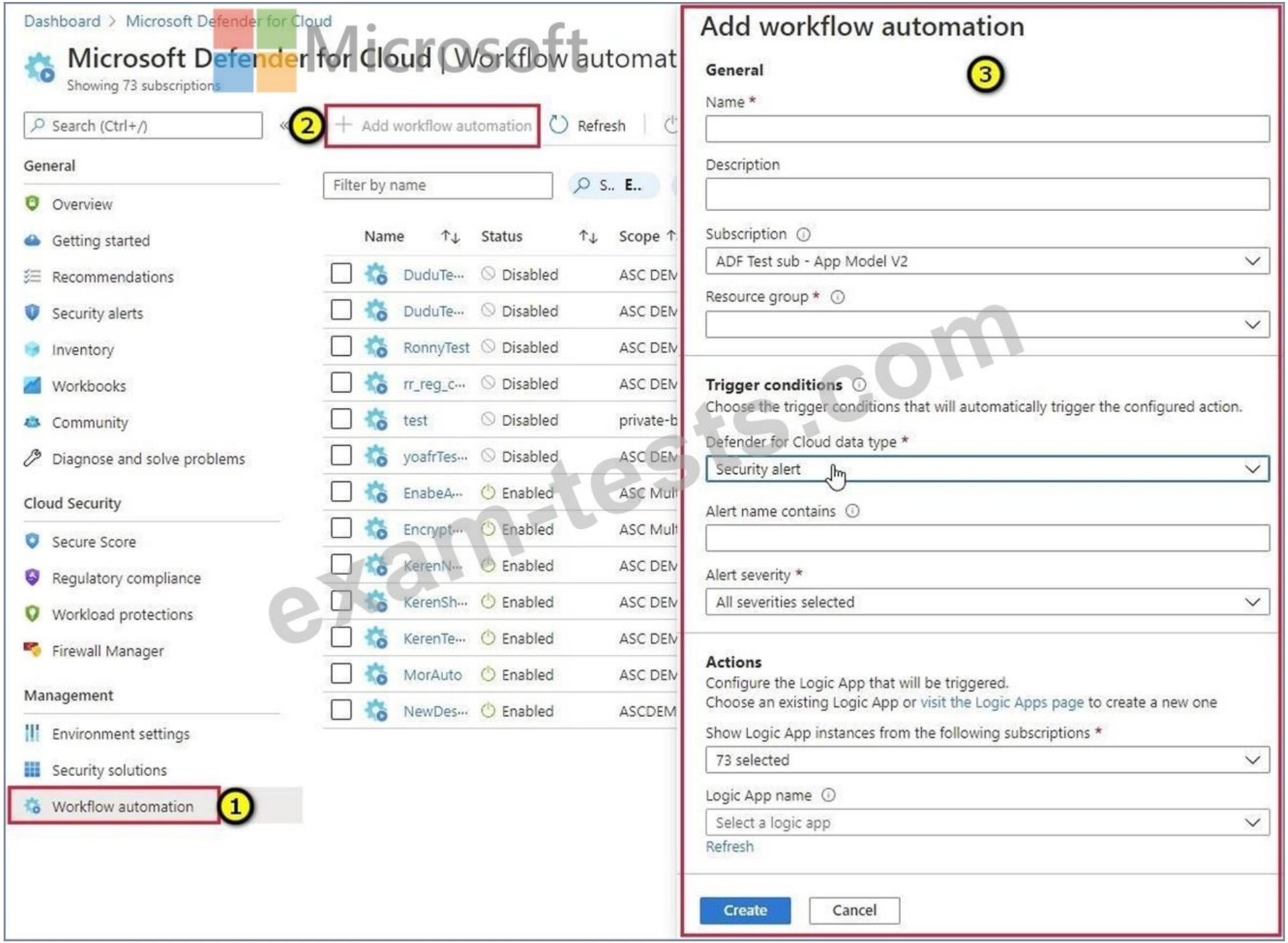
- From Logic App Designer, create a logic app.
- From Logic App Designer, run a trigger.
- From Workflow automation in Defender for Cloud, add a workflow automation.

Explanation:

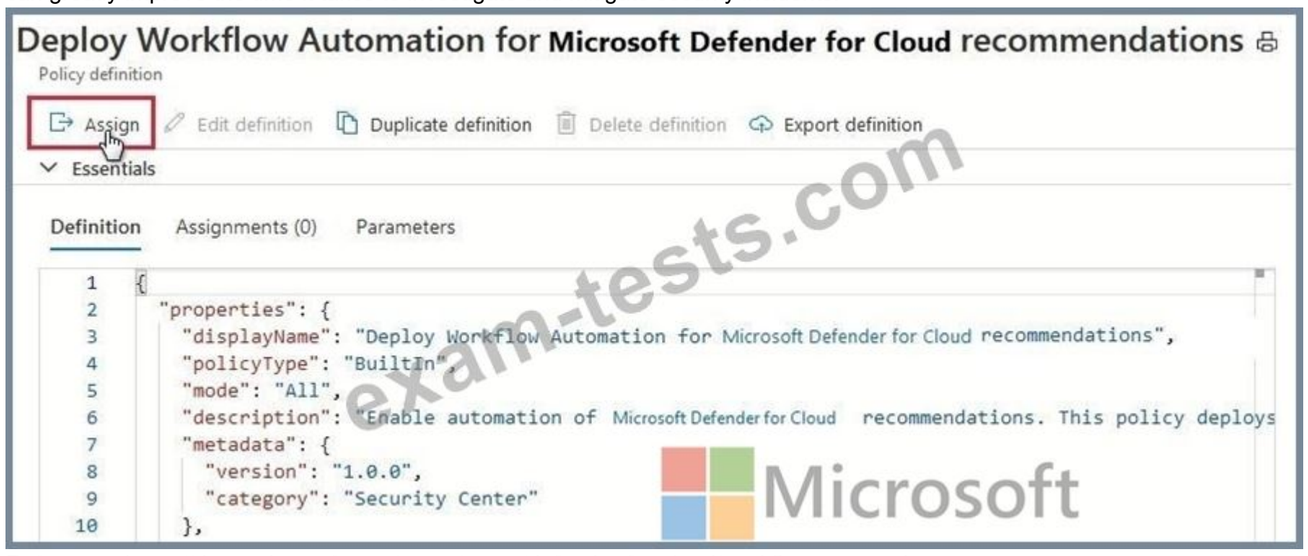
Step 1: From Logic App Designer, create a logic app.

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.

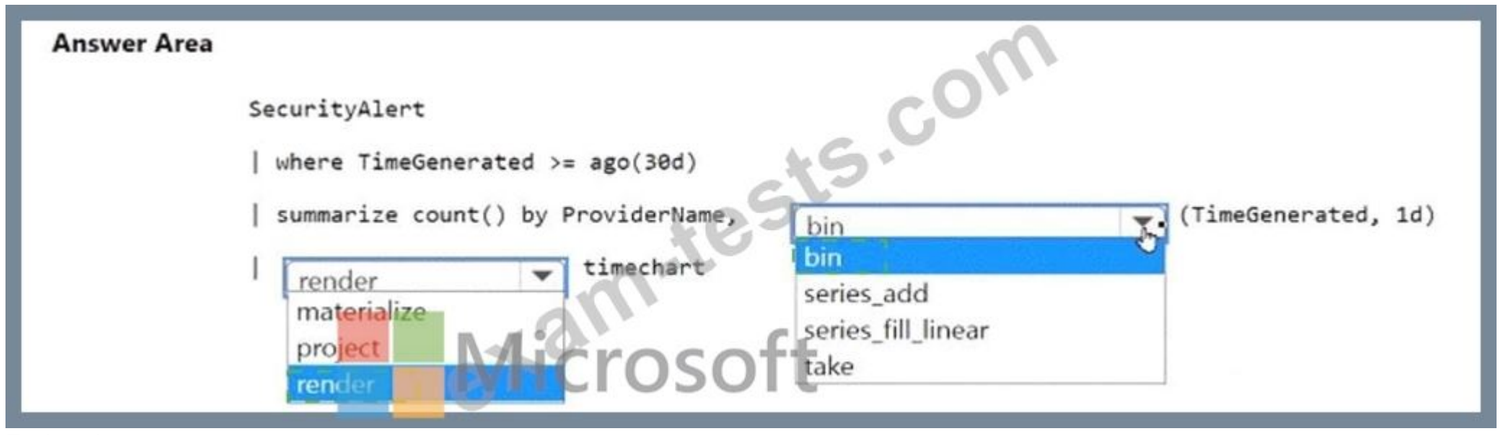


Reference: https://docs.microsoft.com/en-us/azure/defender-for-cloud/workflow-automation

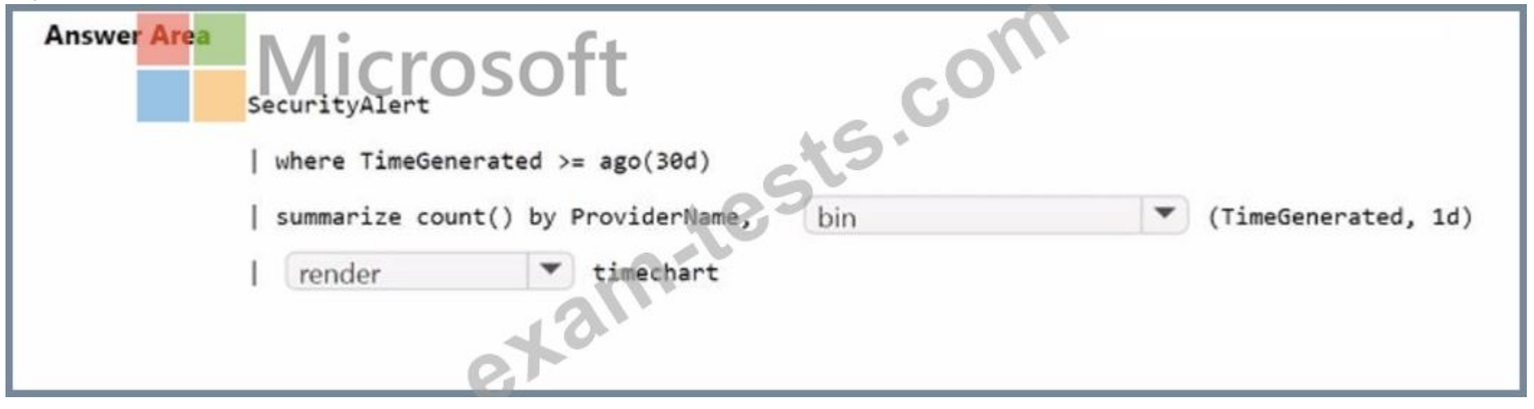
NEW QUESTION: 264
You have an Microsoft Sentinel workspace named SW1.
You plan to create a custom workbook that will include a time chart.
You need to create a query that will identify the number of security alerts per day for each provider.
How should you complete the query? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Answer Area

Answer:



Explanation:



NEW QUESTION: 265

Hotspot Question

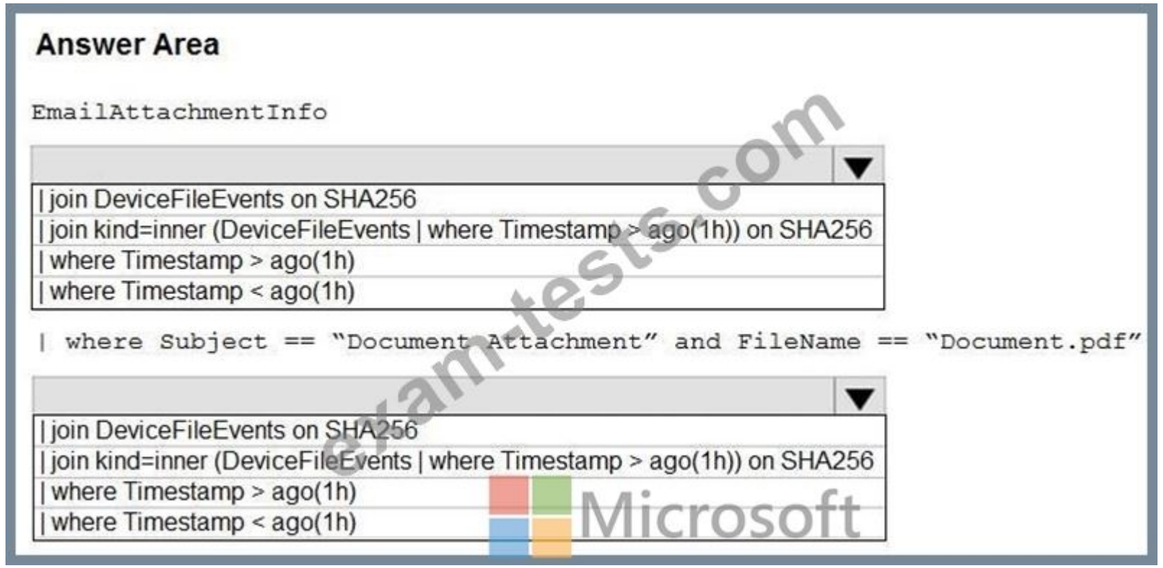
You have a Microsoft 365 E5 subscription.

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:

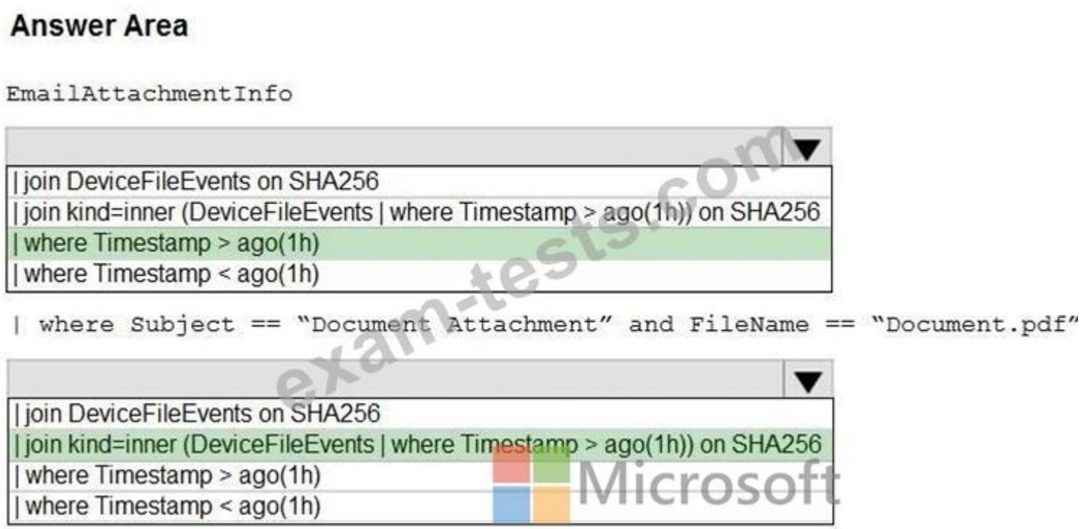
- Only show emails sent during the last hour.
- Optimize query performance.

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:



Explanation:

https://learn.microsoft.com/en-us/microsoft-365/security/defender/advanced-hunting-best- practices?view=o365-worldwide Apply filters early - so start with the timestamp > ago(1h) then the join with an inner-join

NEW QUESTION: 266
Case Study 3 - Litware Inc
Overview
Fabrikam, Inc. is a financial services company.
The company has branch offices in New York, London, and Singapore. Fabrikam has remote users located across the globe. The remote users access company resources, including cloud resources, by using a VPN connection to a branch office.
Existing Environment
Identity Environment
The network contains an Active Directory Domain Services (AD DS) forest named fabrikam.com that syncs with an Azure AD tenant named fabrikam.com. To sync the forest, Fabrikam uses Azure AD Connect with pass-through authentication enabled and password hash synchronization disabled.
The fabrikam.com forest contains two global groups named Group1 and Group2.
Microsoft 365 Environment
All the users at Fabrikam are assigned a Microsoft 365 E5 license and an Azure Active Directory Premium Plan 2 license.
Fabrikam implements Microsoft Defender for Identity and Microsoft Defender for Cloud Apps and enables log collectors.
Azure Environment
Fabrikam has an Azure subscription that contains the resources shown in the following table.

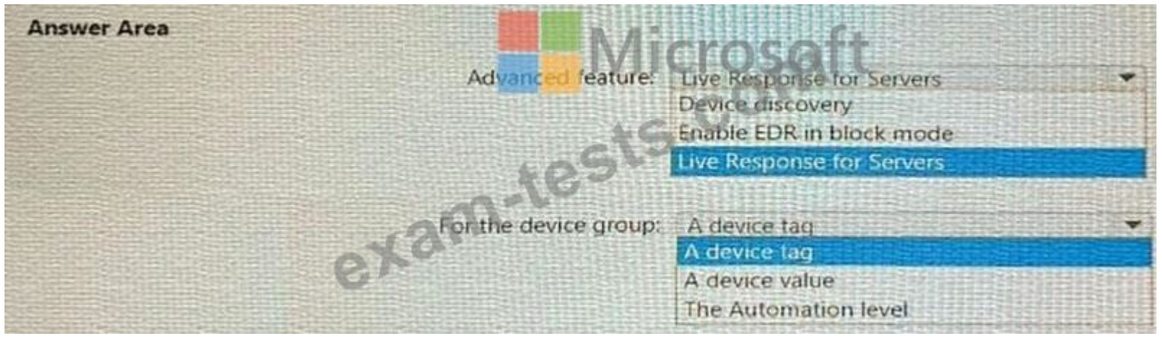
Name	Type	Description
App1	Azure logic app	To automate incident generation in an internal ticketing system, the security operations (SecOps) team invokes App1 by using an HTTP endpoint.
SAWkspc1	Azure Synapse Analytics workspace	SAWkspc1 hosts an Apache Spark pool named Pool1.
LAWkspc1	Log Analytics workspace	LAWkspc1 will be used in a planned Microsoft Sentinel implementation.

Amazon Web Services (AWS) Environment
Fabrikam has an Amazon Web Services (AWS) account named Account1. Account1 contains
100 Amazon Elastic Compute Cloud (EC2) instances that run a custom Windows Server 2022.
The image includes Microsoft SQL Server 2019 and does NOT have any agents installed.
Current Issues
When the users use the VPN connections, Microsoft 365 Defender raises a high volume of impossible travel alerts that are false positives.
Defender for Identity raises a high volume of Suspected DCSync attack alerts that are false positives.
Requirements
Planned changes
Fabrikam plans to implement the following services:
- Microsoft Defender for Cloud
- Microsoft Sentinel
Business Requirements
Fabrikam identifies the following business requirements:
- Use the principle of least privilege, whenever possible.
- Minimize administrative effort.

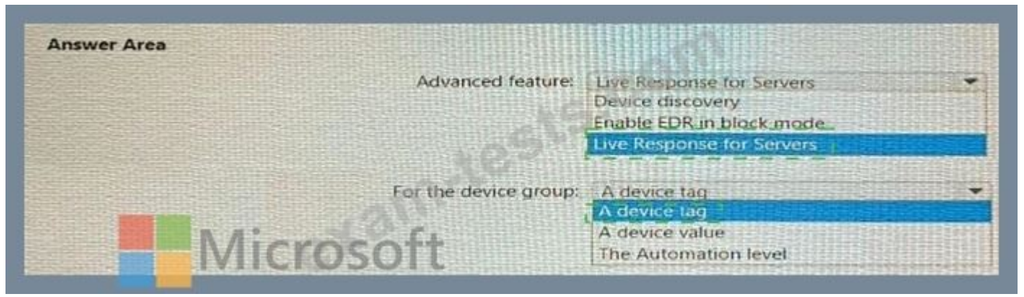
Microsoft Defender for Cloud Apps Requirements
Fabrikam identifies the following Microsoft Defender for Cloud Apps requirements:
- Ensure that impossible travel alert policies are based on the previous activities of each user.
- Reduce the amount of impossible travel alerts that are false positives.
Microsoft Defender for Identity Requirements
Minimize the administrative effort required to investigate the false positive alerts.
Microsoft Defender for Cloud Requirements
Fabrikam identifies the following Microsoft Defender for Cloud requirements:
- Ensure that the members of Group2 can modify security policies.
- Ensure that the members of Group1 can assign regulatory compliance policy initiatives at the Azure subscription level.
- Automate the deployment of the Azure Connected Machine agent for Azure Arc-enabled servers to the existing and future resources of Account1.
- Minimize the administrative effort required to investigate the false positive alerts.
Microsoft Sentinel Requirements
Fabrikam identifies the following Microsoft Sentinel requirements:
- Query for NXDOMAIN DNS requests from the last seven days by using built-in Advanced Security Information Model (ASIM) unifying parsers.
- From AWS EC2 instances, collect Windows Security event log entries that include local group membership changes.
- Identify anomalous activities of Azure AD users by using User and Entity Behavior Analytics (UEBA).
- Evaluate the potential impact of compromised Azure AD user credentials by using UEBA.
- Ensure that App1 is available for use in Microsoft Sentinel automation rules.
- Identify the mean time to triage for incidents generated during the last 30 days.
- Identify the mean time to close incidents generated during the last 30 days.
- Ensure that the members of Group1 can create and run playbooks.
- Ensure that the members of Group1 can manage analytics rules.
- Run hunting queries on Pool1 by using Jupyter notebooks.
- Ensure that the members of Group2 can manage incidents.
- Maximize the performance of data queries.
- Minimize the amount of collected data.
You need to identify which mean time metrics to use to meet the Microsoft Sentinel requirements.
Which workbook should you use?
A. Event Analyzer
B. Investigation Insights
C. Security Operations Efficiency
D. Analytics Efficiency
Answer: (SHOW ANSWER)
https://learn.microsoft.com/en-us/azure/sentinel/manage-soc-with-incident-metrics

NEW QUESTION: 267
You have a Microsoft 365 E5 subscription that uses Microsoft 365 Defender for Endpoint.
You need to ensure that you can initiate remote shell connections to Windows servers by using the Microsoft 365 Defender portal.
What should you configure? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.



Answer:



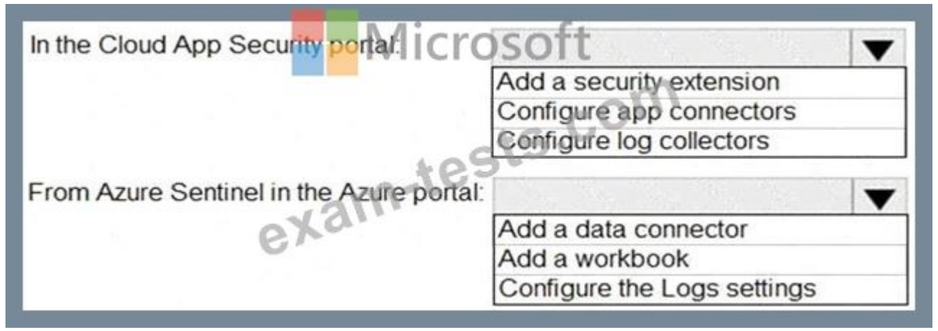
Explanation:

NEW QUESTION: 268

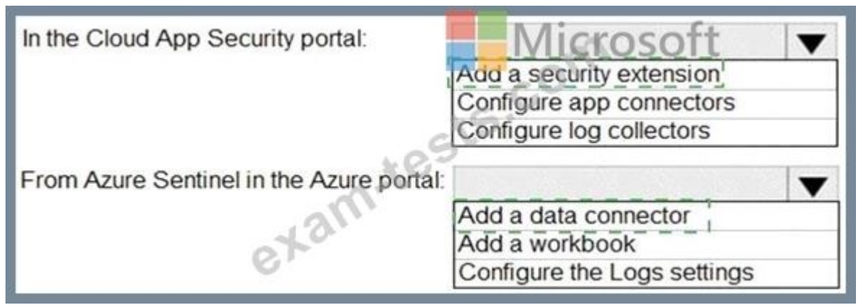
You need to configure the Azure Sentinel integration to meet the Azure Sentinel requirements.

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

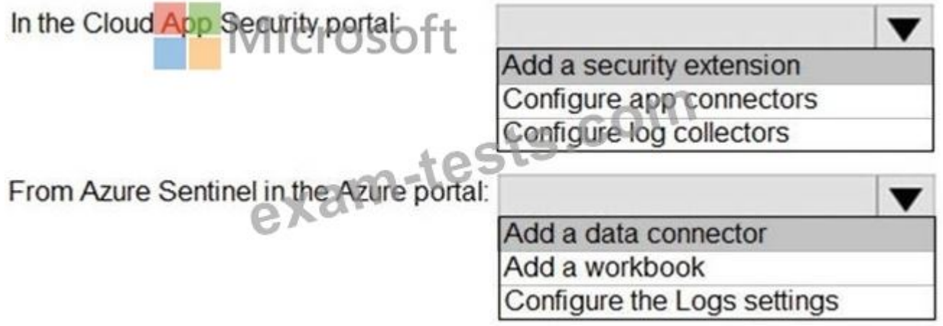
NOTE: Each correct selection is worth one point.



Answer:



Explanation:



Reference:
https://docs.microsoft.com/en-us/cloud-app-security/siem-sentinel

NEW QUESTION: 269
You need to configure the Microsoft Sentinel integration to meet the Microsoft Sentinel requirements. What should you do? To answer, select the appropriate options in the answer are a. NOTE: Each correct selection is worth one point.

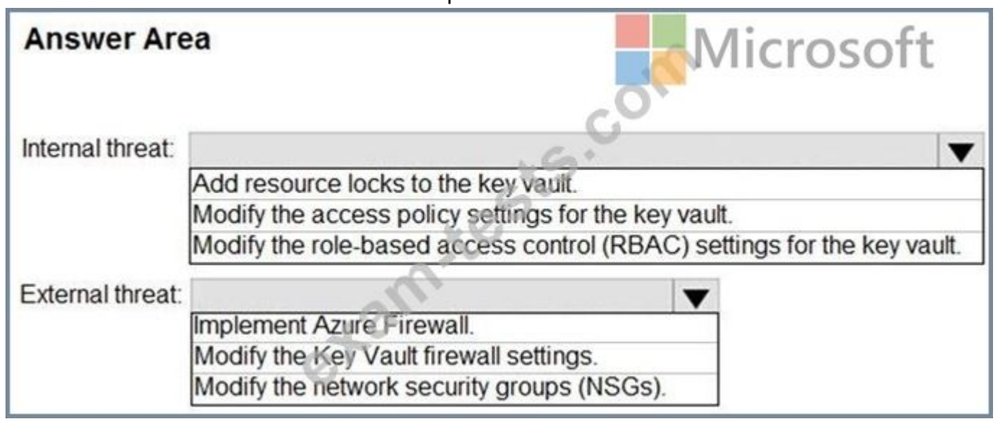
Answer:

NEW QUESTION: 270

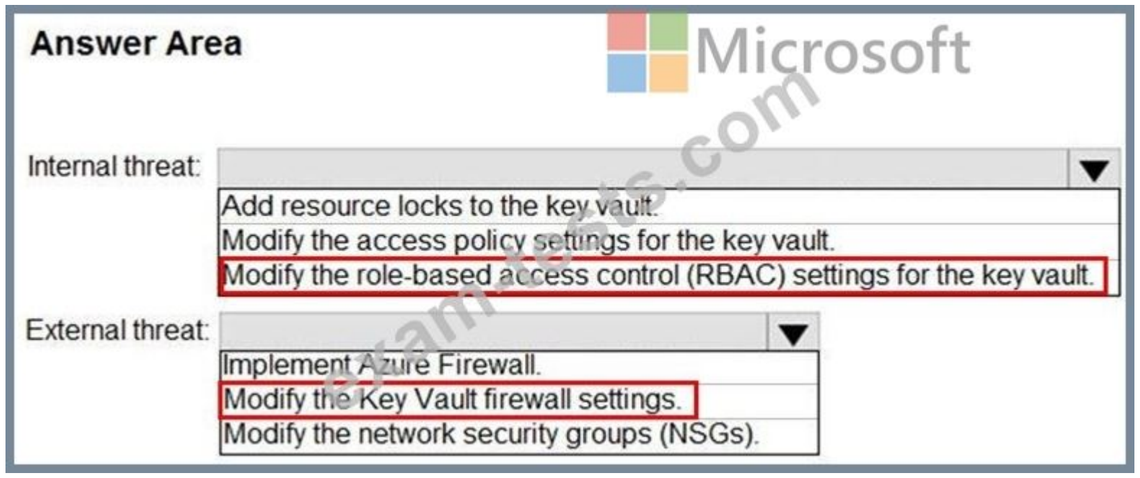
You need to recommend remediation actions for the Azure Defender alerts for Fabrikam.

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:

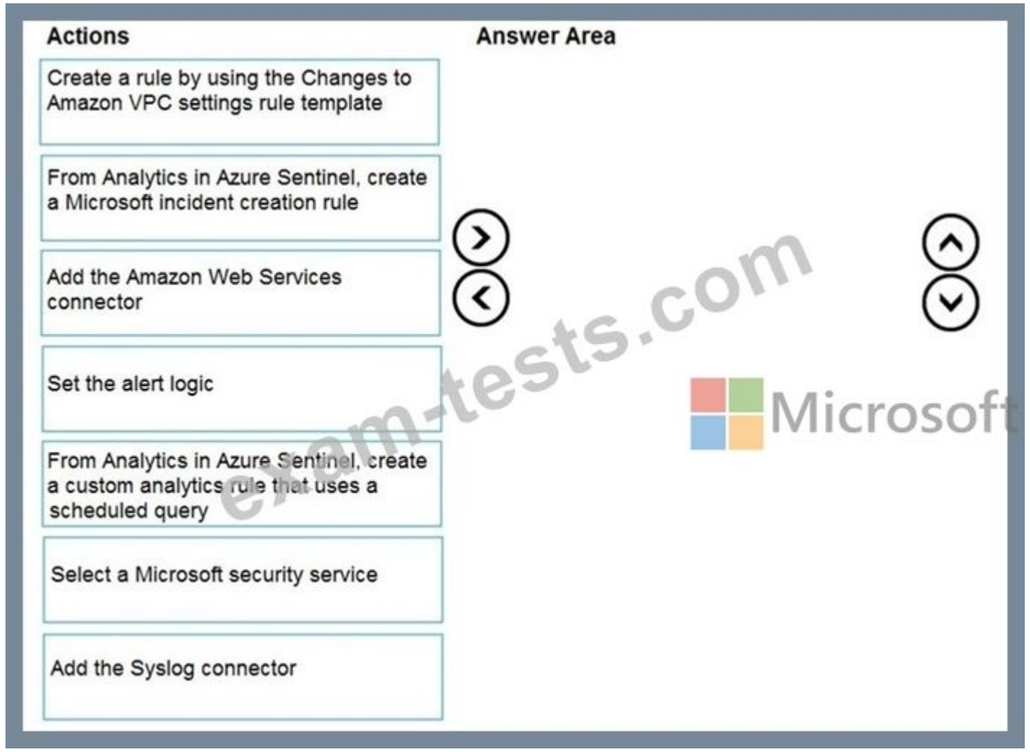


Reference:
https://docs.microsoft.com/en-us/azure/key-vault/general/secure-your-key-vault

NEW QUESTION: 271
You have a Microsoft Sentinel workspace named Workspace1 that is connected to the Microsoft Sentinel data lake. Workspace1 retains 12 years of historical data in the data lake tier.
You plan to run an advanced hunting query that uses join across multiple tables and directly accesses the data in the data lake.
You need to ensure that you can run the query on demand during investigations and on a schedule. The solution must ensure that the query can run asynchronously.
What should you use?
A. a summary rule
B. a scheduled analytics rule that queries the analytics tier only
C. a search job
D. a KQL job
Answer: D (LEAVE A REPLY)
To meet your exact investigative requirements, you should use KQL jobs in the Microsoft Sentinel data lake.
Direct Data Lake Access: KQL jobs run natively against the long-term data lake tier to process massive historical datasets spanning up to 12 years.
Advanced Multi-Table Joins: Unlike standard Search jobs (which typically prioritize single-table lookups or strict hydration scenarios), KQL jobs allow you to execute complex Kusto Query Language (KQL) scripts involving multi-table joins and data aggregations.
Asynchronous Execution: Jobs naturally decouple compute from your real-time session. They run entirely in the background, preventing timeout limits commonly found in interactive queries.
On-Demand & Scheduled Support: You can execute a KQL job explicitly on-demand when conducting a live investigation, or configure it on a recurring schedule to promote findings continuously into a target table.
Reference:
https://learn.microsoft.com/en-us/azure/sentinel/datalake/kql-jobs

NEW QUESTION: 272
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



Answer:

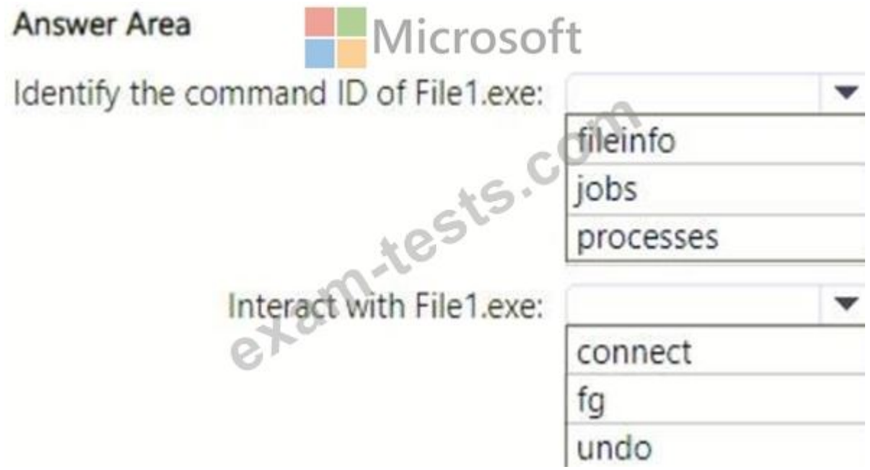
1 - Add the Amazon Web Services connector
2 - From Analytics in Azure Sentinel, create...
3 - Set the alert logic

Reference:
https://docs.microsoft.com/en-us/azure/sentinel/detect-threats-custom

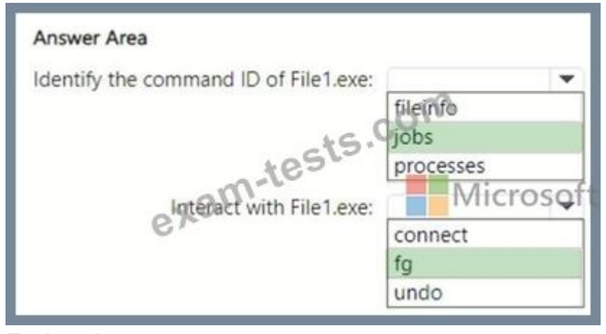
NEW QUESTION: 273
Hotspot Question
You have a Microsoft 365 subscription that uses Microsoft Defender for Endpoint Plan 2 and contains a Windows device named Device1.
You initiate a live response session on Device1 and launch an executable file named File1.exe in the background.

You need to perform the following actions:
- Identify the command ID of File1.exe.
- Interact with File1.exe.

Which live response command should you run for each action? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



Answer:

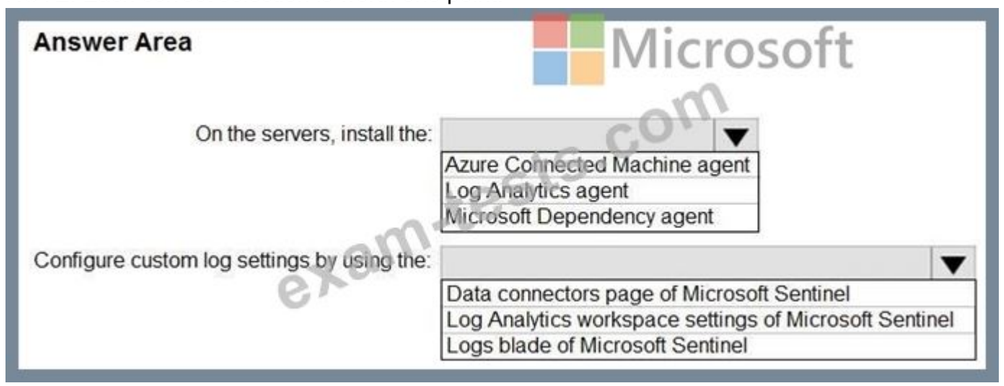


Explanation:
https://learn.microsoft.com/en-us/defender-endpoint/live-response

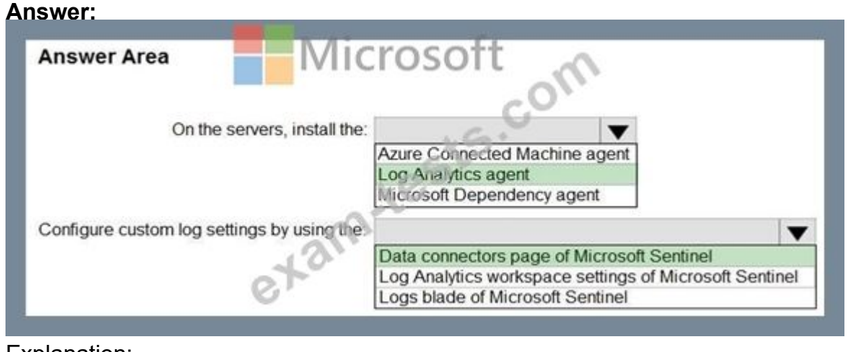
NEW QUESTION: 274
You have a Microsoft 365 subscription that contains 1,000 Windows 10 devices. The devices have Microsoft Office 365 installed.
You need to mitigate the following device threats:
Microsoft Excel macros that download scripts from untrusted websites
Users that open executable attachments 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: (SHOW ANSWER)
Reference:
https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/overview-attack-surface-reduction?v

NEW QUESTION: 275
Hotspot Question
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.
NOTE: Each correct selection is worth one point.



Answer:



Explanation:
https://learn.microsoft.com/en-us/azure/sentinel/connect-custom-logs?tabs=DCG

NEW QUESTION: 276
Hotspot Question
You have a Microsoft Sentinel workspace that has User and Entity Behavior Analytics (UEBA) enabled.
You need to identify all the log entries that relate to security-sensitive user actions performed on a server named Server1. The solution must meet the following requirements:
- Only include security-sensitive actions by users that are NOT members of the IT department.

- Minimize the number of false positives.

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

```
SecurityEvent
| where EventID in ("4624","4672")
| where Computer == "SERVER1"
[ ▼ ]
    | join kind=fullouter (
    | join kind=inner (
    | join kind=innerunique (
[ ▼ ]
    BehaviorAnalytics
    IdentityInfo
    SecurityEvent
    | summarize arg_max(TimeGenerated, *) by AccountObjectId) on $left.SubjectUserSid == $right.AccountSI
| where Department != "IT"
```


Answer:

Answer Area

```
SecurityEvent
| where EventID in ("4624","4672")
| where Computer == "SERVER1"
[ ▼ ]
    | join kind=fullouter (
    | join kind=inner (
    | join kind=innerunique (
[ ▼ ]
    BehaviorAnalytics
    IdentityInfo
    SecurityEvent
    | summarize arg_max(TimeGenerated, *) by AccountObjectId) on $left.SubjectUserSid == $right.AccountSID
| where Department != "IT"
```


Explanation:

https://learn.microsoft.com/en-us/azure/sentinel/investigate-with-ueba#embed-identityinfo-data-in- your-analytics-rules-public-preview

NEW QUESTION: 277

Hotspot Question

You have an Azure subscription named Sub1 that contains a resource group named RG1. RG1 contains two Azure key vaults named KV1 and KV2 that use Azure role-based access control (Azure RBAC).

The subscription contains the users shown in the following table.

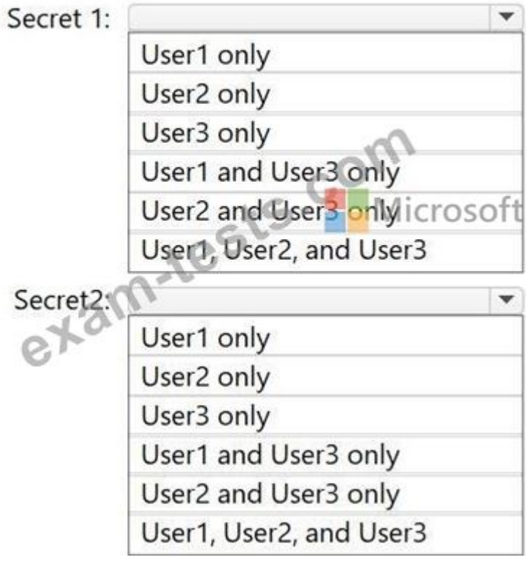
Name	Role	Scope
User1	Kev Vault Administrator	Sub1
User2	Key Vault Reader	RG1
User3	Key Vault Secrets User	KV1

KV1 contains a secret named Secret1. KV2 contains a secret named Secret2.

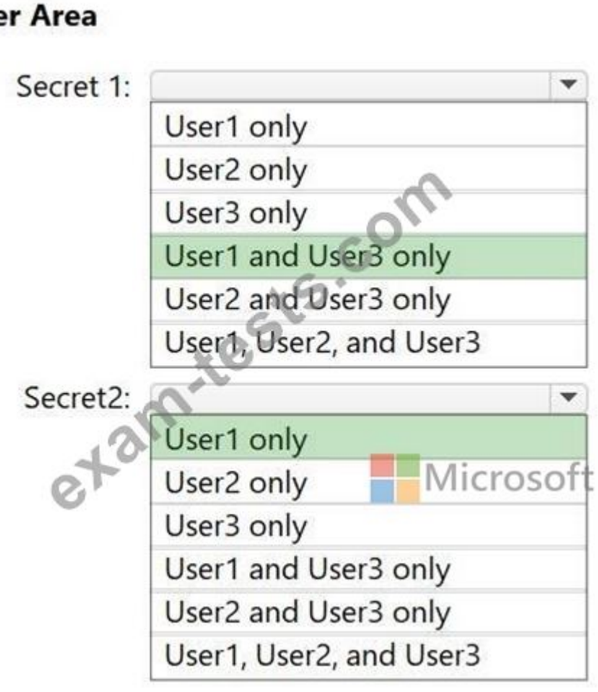
Which users can read the values of each secret? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

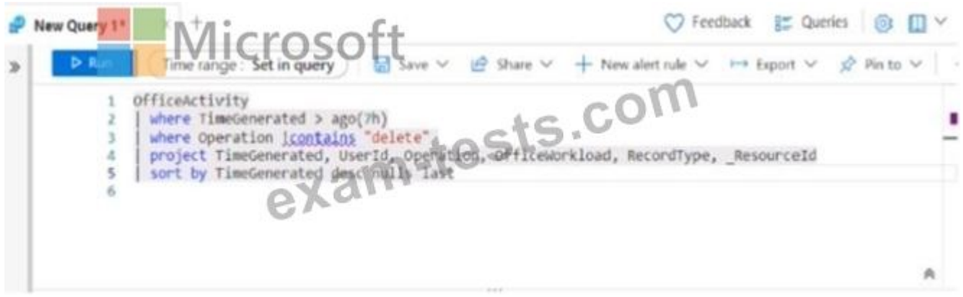


Answer:



NEW QUESTION: 278

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: (SHOW ANSWER)

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: 279

Hotspot Question

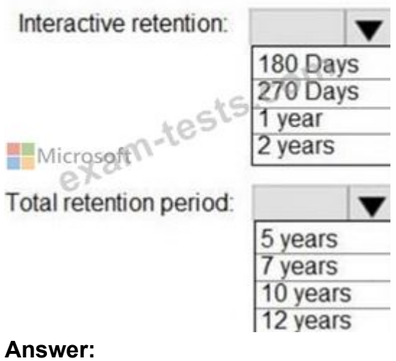
You have a Microsoft Sentinel workspace that contains a table named Table1. Table1 has the Analytics plan configured.

You need to configure the retention period for Table1. The solution must maximize the retention of data stored in Table1.

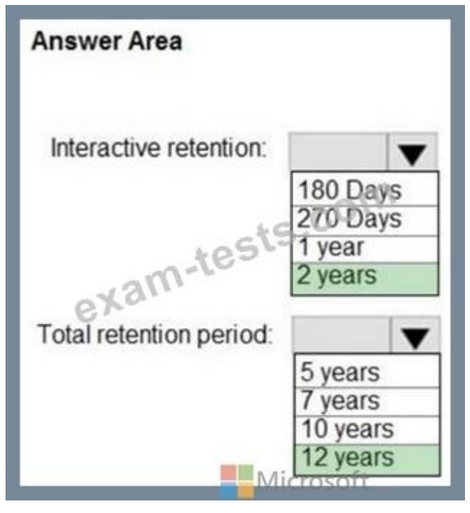
How should you configure the Data retention settings? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

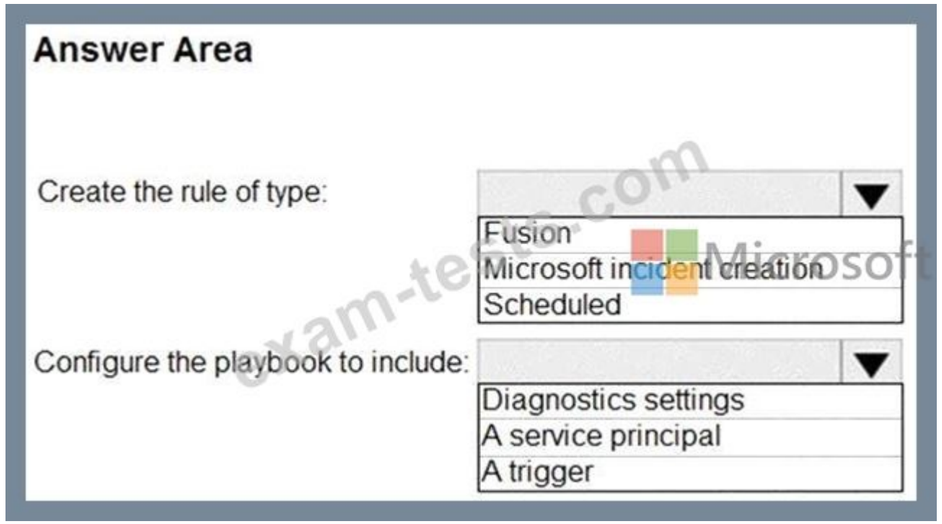


Answer:

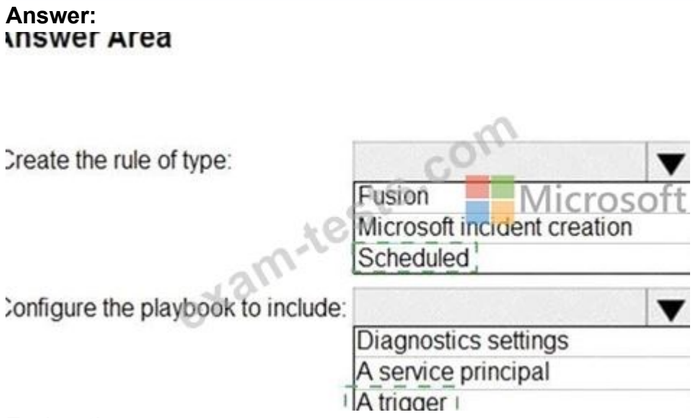


NEW QUESTION: 280
Your on-premises network contains an Active Directory Domain Services (AD DS) forest.
You have a Microsoft Entra tenant that uses Microsoft Defender for Identity. The AD DS forest syncs with the tenant You need to create a hunting query that will identify LDAP simple binds to the AD DS domain controllers.
Which table should you query?
A. AADServicePrincipalRiskEventi
B. IdentityLOgonEvents
C. AADDomainServicesAccountLogon
D. Signinlogs
Answer: B (LEAVE A REPLY)
In Microsoft Defender for Identity (MDI) , data collected from Active Directory Domain Serv ices (AD DS) is stored in Microsoft 365 Defender advanced hunting tables under the Identity schema.
When investigating LDAP or authentication activities related to domain controllers, the correct table is IdentityLogonEvents .
The IdentityLogonEvents table contains information about all logons detected by Defender for Identity sensors on domain controllers - including LDAP binds , Kerberos , NTLM , and other authentication types.
You can identify LDAP simple binds using a query such as:
IdentityLogonEvents
| wh ere Protocol == " LDAP "
| where AuthenticationPackage == " SimpleBind "
Other options explained:
* AADServicePrincipalRiskEvents - Contains Entra (Azure AD) service principal risk detections, not AD DS activity.
* AADDomainServicesAccountLogon - Used for Azure AD Domain Services (AAD DS), not traditional on-prem AD DS.
* SigninLogs - Contains Entra (Azure AD) sign-in data, not LDAP or on-prem authentication.
# Correct table: IdentityLogonEvents

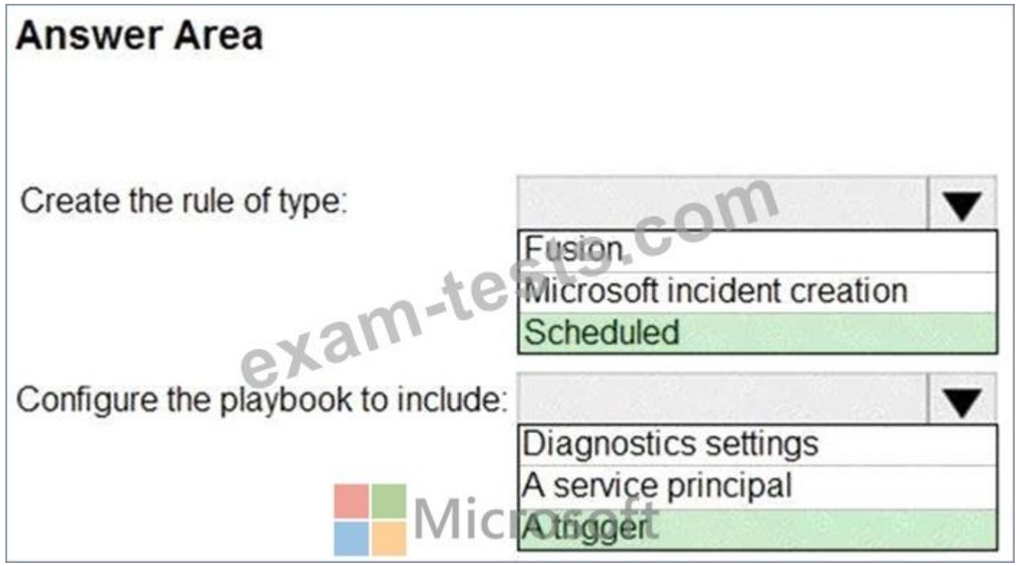
NEW QUESTION: 281
You need to create the analytics rule to meet the Azure Sentinel requirements.
What should you do? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



Answer:



Explanation:



NEW QUESTION: 282

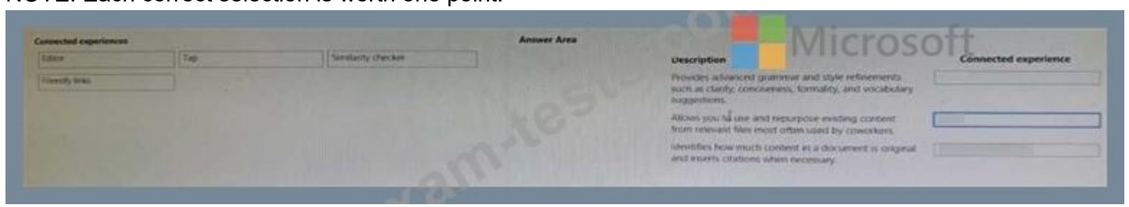
Drag and Drop Question

A company wants to analyze by using Microsoft 365 Apps.

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

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

NOTE: Each correct selection is worth one point.



Answer: