CertyIQ

CertyIQ

Premium exam material

Get certification quickly with the CertyIQ Premium exam material.
Everything you need to prepare, learn & pass your certification exam easily. Lifetime free updates
First attempt guaranteed success.

https://www.CertyIQ.com

About CertyIQ

We here at CertyIQ eventually got enough of the industry's greedy exam paid for. Our team of IT professionals comes with years of experience in the IT industry Prior to training CertIQ we worked in test areas where we observed the horrors of the paywall exam preparation system.

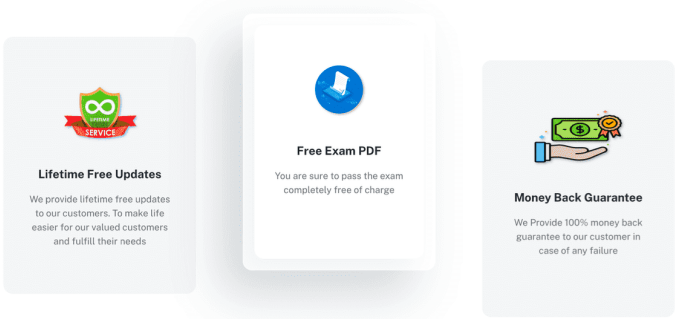
The misuse of the preparation system has left our team disillusioned. And for that reason, we decided it was time to make a difference. We had to make In this way, CertyIQ was created to provide quality materials without stealing from everyday people who are trying to make a living.

Doubt Support

We have developed a very scalable solution using which we are able to solve 400+ doubts every single day with an average rating of 4.8 out of 5.

https://www.certyiq.com

Mail us on - certyiqofficial@gmail.com



John

October 19, 2022

★★★★★

Thanks you so much for your help. I scored 972 in my exam today. More than 90% were from your PDFs!

Dana

September 04, 2022

★★★★★

Thanks a lot for this updated AZ-900 Q&A. I just passed my exam and got 974, I followed both of your Az-900 videos and the 6 PDF, the PDFs are very much valid, all answers are correct. Could you please create a similar video/PDF for DP900, your content/PDF's is really awesome. The team did a really good job. Thank You 😊.

Ahamed Shibly

2 months ago

★★★★★

Customer support is realy fast and helpful, I just finished my exam and this video along with the 6 PDF helped me pass! Definitely recommend getting the PDFs. Thank you!

October 22, 2022

★★★★★

Passed my exam today with 891 marks. Out of 52 questions, 51 were from certyiq PDFs including Contoso case study.
Thank You certyiq team!

Henry Rome

2 months ago

★★★★★

These questions are real and 100 % valid. Thank you so much for your efforts, also your 4 PDFs are awesome, I passed the DP900 exam on 1 Sept. With 968 marks. Thanks a lot, buddy!

Esmaria

2 months ago

★★★★★

Simple easy to understand explanations. To anyone out there wanting to write AZ900, I highly recommend 6 PDF's.Thank you so much, appreciate all your hard work in having such great content. Passed my exam Today - 3 September with 942 score.

Microsoft

(SC-200)

Microsoft Security Operations Analyst

Total: **297 Questions**

Link: https://certyiq.com/papers/microsoft/sc-200

Question: 1 CertyIQ

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
```

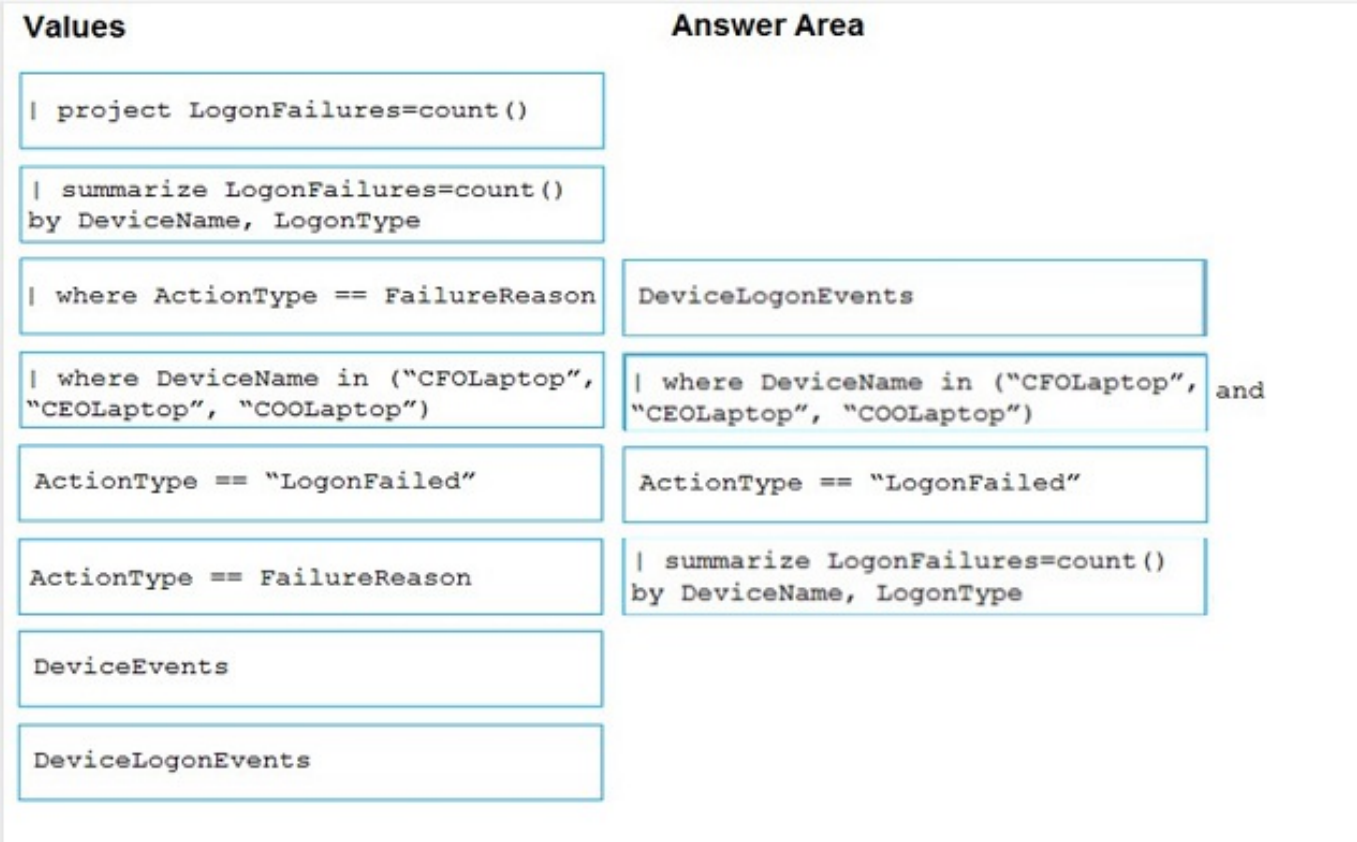
Answer Area

[ ] and [ ]

[ ]

[ ]

Answer:



Explanation:

DeviceLogonEvents

where DeviceName in ("CFOLaptop", "CEOLaptop", "COOLaptop")

ActionType == "LogonFailed"

| summarize LogonFailures=count() by DeviceName, LogonType

Reference

https://github.com/microsoft/Microsoft-365-Defender-Hunting-Queries/blob/master/General%20queries/Failed%20Logon%20Attempt.txt

Question: 2 CertyIQ

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

Explanation:

Activity from infrequent country

This detection considers past activity locations to determine new and infrequent locations. The anomaly

detection engine stores information about previous locations used by users in the organization. An alert is triggered when an activity occurs from a location that wasn't recently or never visited by any user in the organization.

Reference:

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

Question: 3 CertyIQ

You have a Microsoft 365 subscription that uses Microsoft Defender for Office 365.
You have Microsoft SharePoint Online sites that contain sensitive documents. The documents contain customer account numbers that each consists of 32 alphanumeric characters.
You need to create a data loss prevention (DLP) policy to protect the sensitive documents.
What should you use to detect which documents are sensitive?

A. SharePoint search
B. a hunting query in Microsoft 365 Defender
C. Azure Information Protection
D. RegEx pattern matching

Answer: C

Explanation:

Reference:
https://docs.microsoft.com/en-us/azure/information-protection/what-is-information-protection

Question: 4 CertyIQ

Your company uses line-of-business apps that contain Microsoft Office VBA macros.
You need to prevent users from downloading and running additional payloads from the Office VBA macros as additional child processes.
Which two commands can you run to achieve the goal? Each correct answer presents a complete solution.
NOTE: Each correct selection is worth one point.

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

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

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

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

Answer: AD

Explanation:

These are 2 complete solutions on their own. Not a step by step by step.

1) Add the rule and enable it.

2) Add the rule, set the rule to overwrite existing rules, and enable it.

"Set-MpPreference will always overwrite the existing set of rules. If you want to add to the existing set, use Add-MpPreference instead."

https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/enable-attack-surface-reduction?view=o365-worldwide#powershell

The command does not need to mention anything about block because the GUID references a Rule with already set actions.

Configuration Manager name: Block Office application from creating child processes

GUID: d4f940ab-401b-4efc-aadc-ad5f3c50688a

https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/attack-surface-reduction-rules-reference?source=recommendations&view=o365-worldwide#block-all-office-applications-from-creating-child-processes

Question: 5 CertyIQ

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: BDE

Explanation:

Here's a brief explanation of each option:

E. Generate the alert: You need to generate the alert first so that you can see it in the Alerts queue.

B. Hide the alert: After generating the alert, you can hide it if you want to remove it from view.

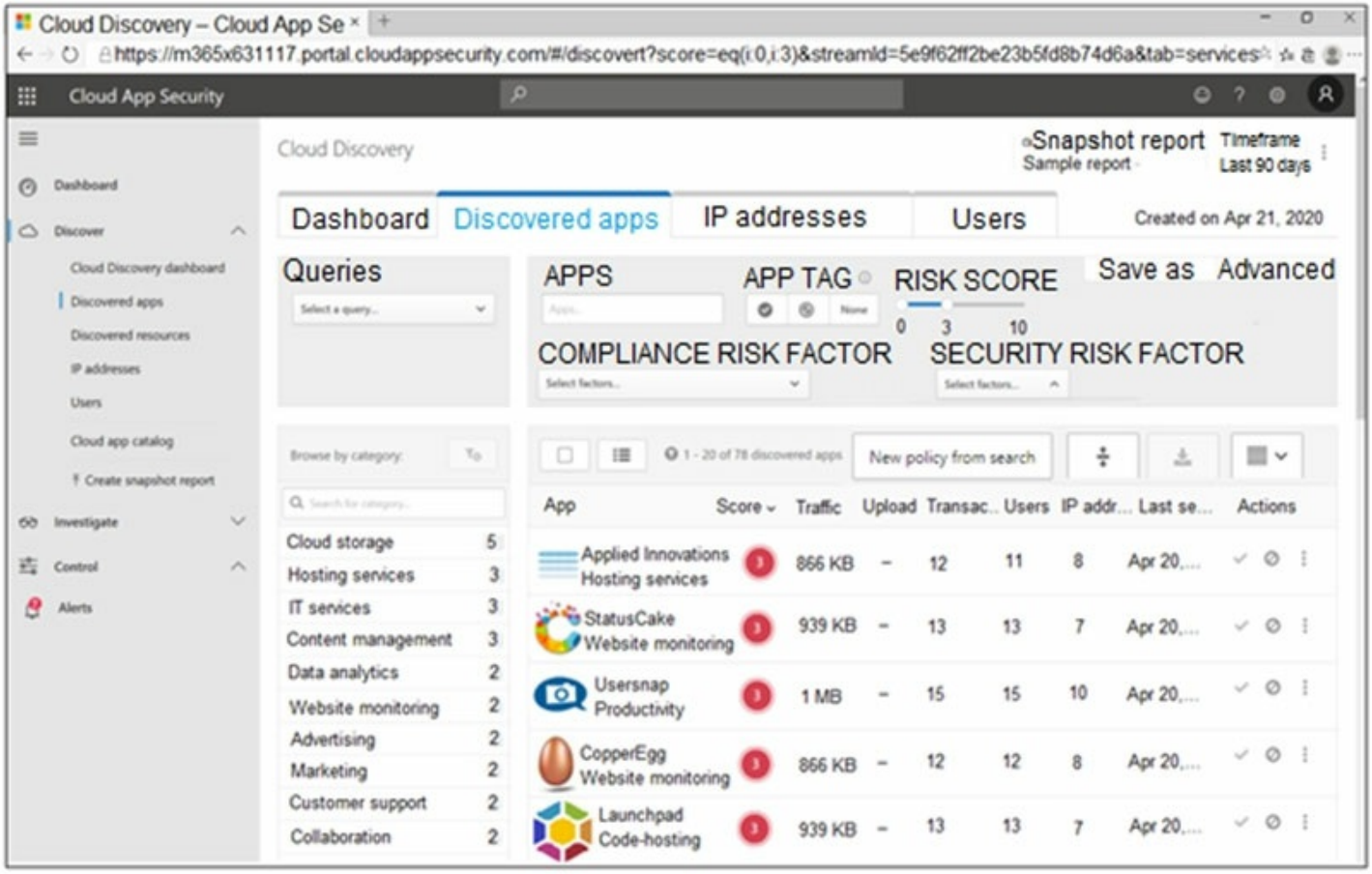
D. Create a suppression rule scoped to a device group: You can also create a suppression rule scoped to a specific device group if you want to only apply it to a specific group of devices. This helps you maintain the existing security posture.

According to the question, I will stick with these

Question: 6 CertyIQ

DRAG DROP -

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



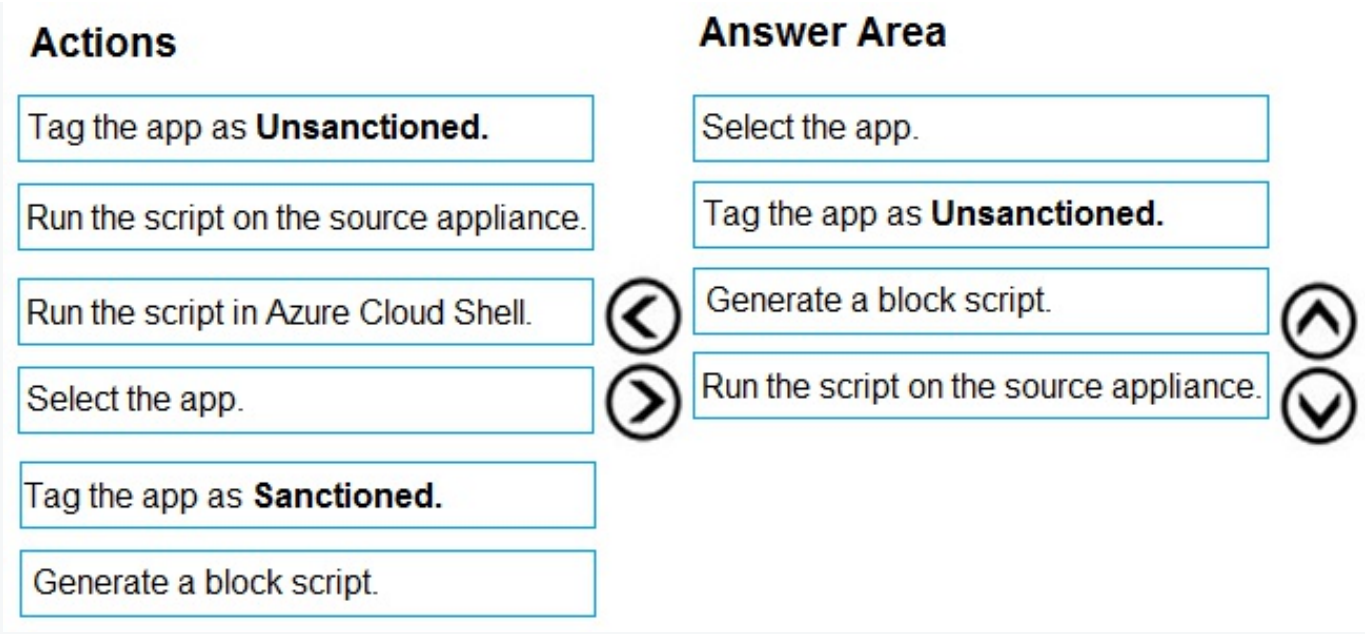
Your environment does NOT have Microsoft Defender for Endpoint enabled.
You need to remediate the risk for the Launchpad app.
Which four actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.
Select and Place:

Actions

- Tag the app as **Unsanctioned.**
- Run the script on the source appliance.
- Run the script in Azure Cloud Shell.
- Select the app.
- Tag the app as **Sanctioned.**
- Generate a block script.

Answer Area

Answer:



Explanation:

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

Question: 7 CertyIQ

HOTSPOT -
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.
Hot Area:

Answer Area

```
EmailAttachmentInfo

| where SenderFromAddress =~ "MaliciousSender@example.com"

| where isnotempty (SHA256)

| [ ▼ ] (
```

- extend
- join
- project
- union

```
DeviceFileEvents

| [ ▼ ] FileName, SHA256
```

- extend
- join
- project
- union

```
) on SHA256

| [ ▼ ] Timestamp, FileName, SHA256, DeviceName, DeviceId,
```

- extend
- join
- project
- union

```
NetworkMessageId, SenderFromAddress, RecipientEmailAddress
```

Answer:

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
```

Explanation:

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

Question: 8 CertyIQ

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.Replace DeviceProcessEvents with DeviceNetworkEvents.

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

Answer: AE

Explanation:

A = Requirement is to create an alert.

Not B = This will hide the the alert.

Not C = Avoid filtering custom detections using the Timestamp column. The data used for custom detections is pre-filtered based on the detection frequency.

Not D = Random filler answer

E = To create a custom detection rule, the query must return the following columns:->Timestamp — used to set the timestamp for generated alerts->ReportId — enables lookups for the original recordsOne of the following columns that identify specific devices, users, or mailboxes: -> DeviceId

Reference:

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

Question: 9 CertyIQ

You are investigating a potential attack that deploys a new ransomware strain.
You have three custom device groups. The groups contain devices that store highly sensitive information.
You plan to perform automated actions on all devices.
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.Assign a tag to the device group.

B.Add the device users to the admin role.

C.Add a tag to the machines.

D.Create a new device group that has a rank of 1.

E.Create a new admin role.

F.Create a new device group that has a rank of 4.

Answer: ACD

Explanation:

There are 3 device groups.You want to take action on all devices. Meaning you want 1(One) Device group with all devices.--> A: So you create this custom group(AllDeviceTempGroup) and add a Tag filter(RansomIRTag) to group devices into this device group.You see that there are no devices in this group. Why? You have not tagged your devices yet.--> B: You add the tag, RansomIRTag, to all devices.You notice that your devices have not populated your new device group, AllDeviceTempGroup. Why?In the details of the question, you are informed that these devices already have a group. Which means if your group is not promoted to highest rank, then the devices will choose their original group instead.-->C: Promote AllDeviceTempGroup to highest rank.

Reference:

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

Question: 10 CertyIQ

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

Explanation:

Reference:
https://docs.microsoft.com/en-us/defender-for-identity/manage-sensitive-honeytoken-accounts

Question: 11 CertyIQ

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 Azure AD Identity Protection, you configure the sign-in risk policy.
Does this meet the goal?

A.Yes
B.No

Answer: B

Explanation:

Honeytoken entities are used as traps for malicious actors. Any authentication associated with these honeytoken entities triggers an alert.Settings>Identities>Entity tags>Honey Token> Add Users or Devices

Reference:

https://docs.microsoft.com/en-us/defender-for-identity/manage-sensitive-honeytoken-accounts

Question: 12 CertyIQ

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: You add the accounts to an Active Directory group and add the group as a Sensitive group.
Does this meet the goal?

A.Yes
B.No

Answer: B

Explanation:

This is what honeytoken accounts are meant for (i.e. dormant accounts that generate alerts if accessed). Sensitivity tags are meant for active users and groups.

Reference:

https://docs.microsoft.com/en-us/defender-for-identity/manage-sensitive-honeytoken-accounts

Question: 13 CertyIQ

You implement Safe Attachments policies in Microsoft Defender for Office 365.
Users report that email messages containing attachments take longer than expected to be received.
You need to reduce the amount of time it takes to deliver messages that contain attachments without compromising security. The attachments must be scanned for malware, and any messages that contain malware must be blocked.
What should you configure in the Safe Attachments policies?

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

Answer: A

Explanation:

CorrectDynamic DeliveryDelivers messages immediately, but replaces attachments with placeholders until Safe Attachments scanning is complete.For details, see the Dynamic Delivery in Safe Attachments policies section later in this article.Avoid message delays while protecting recipients from malicious files.Enable recipients to preview attachments in safe mode while scanning is taking place.

Reference:

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

Question: 14 CertyIQ

HOTSPOT -
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.
Hot Area:

Answer Area

```
let MaliciousEmails = [ ▼ ]
                      EmailAttachementInfo
                      EmailEvents
                      IdentityLogonEvents
| where MalwareFilterVerdict == "Malware"
| project TimeEmail = Timestamp, Subject, SenderFromAddress, AccountName =
tostring(split (RecipientEmailAddress, "@") [0]);

MaliciousEmails
| join ( [ ▼ ]
         EmailAttachementInfo
         EmailEvents
         IdentityLogonEvents
| project LogonTime = Timestamp, AccountName, DeviceName
) on AccountName
| where (LogonTime - TimeEmail) between (0min.. 60min)
| [ ▼ ]
  select 20
  take 20
  top 20
```

Answer:

Answer Area

```
let MaliciousEmails = [EmailAttachementInfo | EmailEvents | IdentityLogonEvents]
| where MalwareFilterVerdict == "Malware"
| project TimeEmail = Timestamp, Subject, SenderFromAddress, AccountName =
tostring(split (RecipientEmailAddress, "@") [0]);

MaliciousEmails
| join ( [EmailAttachementInfo | EmailEvents | IdentityLogonEvents]
| project LogonTime = Timestamp, AccountName, DeviceName
) on AccountName
| where (LogonTime - TimeEmail) between (0min.. 60min)
| [select 20 | take 20 | top 20]
```

Explanation:

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

Question: 15 CertyIQ

You receive a security bulletin about a potential attack that uses an image file.
You need to create an indicator of compromise (IoC) in Microsoft Defender for Endpoint to prevent the attack.
Which indicator type should you use?

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

Answer: C

Explanation:

The correct answer it seems like, as steps for to Create an indicator for files from the settings page1. In the navigation pane, selectSettings > Endpoints > Indicators (under Rules).2. Select theFile hashestab.3. SelectAdd indicator.4. Specify the following details:5. Indicator - Specify the entity details and define the expiration of the indicator.* Action - Specify the action to be taken and provide a description.* Scope - Define the scope of the device group.* Review the details in the Summary tab, then select Save.

Reference:

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

Question: 16 CertyIQ

Your company deploys the following services:
- Microsoft Defender for Identity
- Microsoft Defender for Endpoint
- Microsoft Defender for Office 365

You need to provide a security analyst with the ability to use the Microsoft 365 security center. The analyst must be able to approve and reject pending actions generated by Microsoft Defender for Endpoint. The solution must use the principle of least privilege.
Which two roles should assign to the analyst? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

A.the Compliance Data Administrator in Azure Active Directory (Azure AD)

B.the Active remediation actions role in Microsoft Defender for Endpoint

C.the Security Administrator role in Azure Active Directory (Azure AD)

D.the Security Reader role in Azure Active Directory (Azure AD)

Answer: BD

Explanation:

B and D is correct.Security Reader - can access M365 Security Center.Active Remediation Actions role in Defender for Endpoint meets need to 'approve and reject' pending actions with respect to Defender For Endpoint.Requirement does not need more.

Reference:

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

Question: 17 CertyIQ

HOTSPOT -
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.
Hot Area:

Answer Area

```
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:

Answer Area

```
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:

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

view=o365-worldwide

Question: 18 CertyIQ

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

A.From Settings, select Information Protection, select Azure Information Protection, and then select Only scan files for Azure Information Protection classification labels and content inspection warnings from this tenant.

B.Select Investigate files, and then filter App to Office 365.

C.Select Investigate files, and then select New policy from search.

D.From Settings, select Information Protection, select Azure Information Protection, and then select Automatically scan new files for Azure Information Protection classification labels and content inspection warnings.

E.From Settings, select Information Protection, select Files, and then enable file monitoring.

F.Select Investigate files, and then filter File Type to Document.

Answer: DE

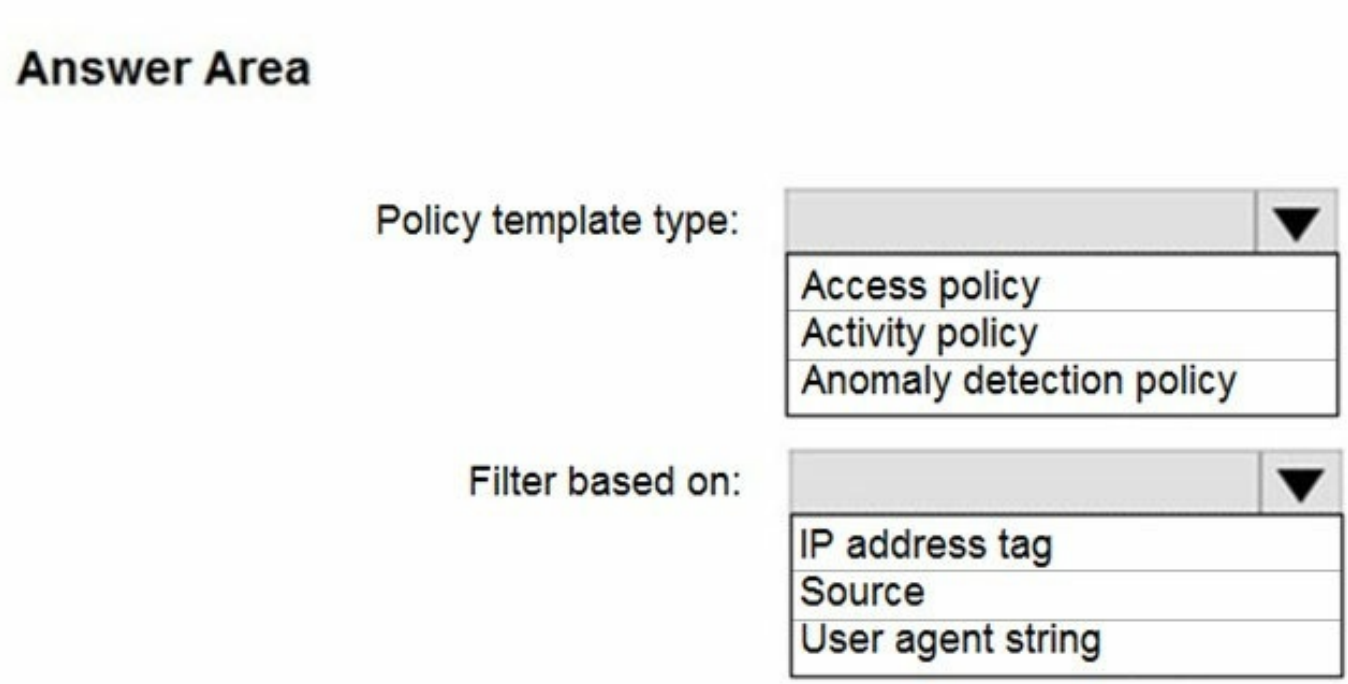
Explanation:

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. This will enable Cloud App Security to automatically scan new files for Azure Information Protection classification labels and content inspection warnings, which can be used to detect and protect confidential files.

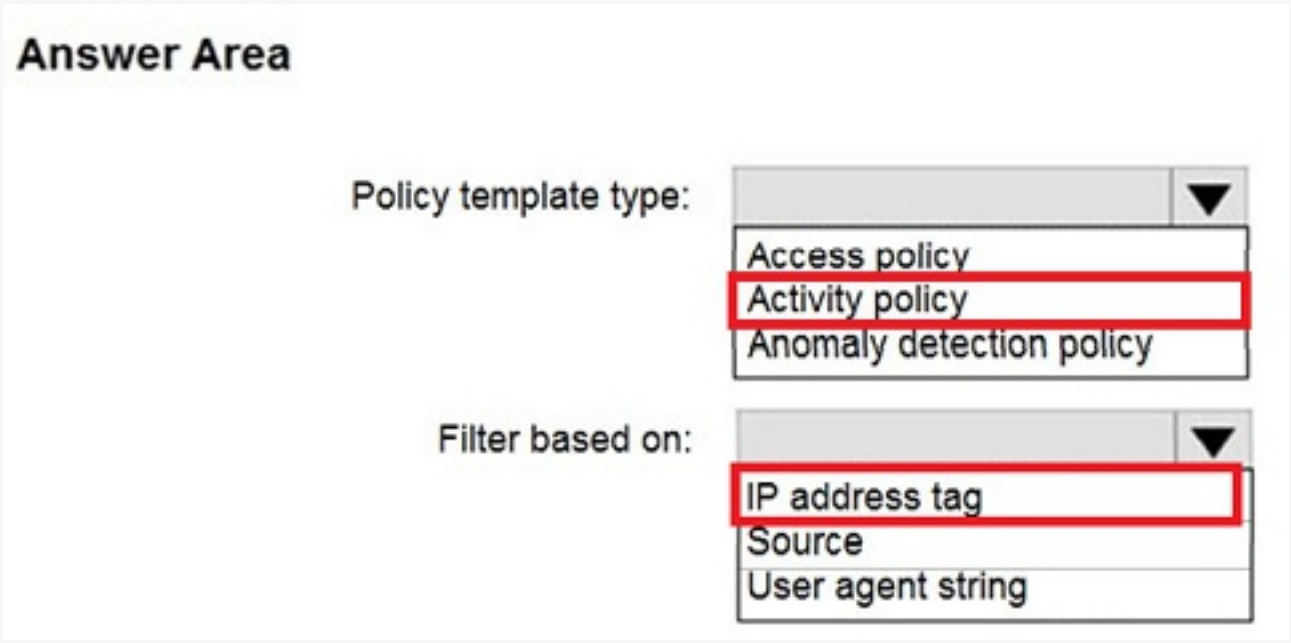
E. From Settings, select Information Protection, select Files, and then enable file monitoring. This will enable Cloud App Security to monitor files for external sharing and other activities, and to generate alerts and trigger remediation actions in response to potential threats or policy violations.

Question: 19 CertyIQ

HOTSPOT -
You purchase a Microsoft 365 subscription.
You plan to configure Microsoft Cloud App Security.
You need to create a custom template-based policy that detects connections to Microsoft 365 apps that originate from a botnet network.
What should you use? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.
Hot Area:



Answer:



Explanation:

Policy template type: Activity PolicyFilter based on: IP address tagTested on the MCAS portal. When you select Activity policy only you get to filter from IP address.

Question: 20

CertyIQ

Your company has a single office in Istanbul and a Microsoft 365 subscription.
The company plans to use conditional access policies to enforce multi-factor authentication (MFA).
You need to enforce MFA for all users who work remotely.
What should you include in the solution?

A.a fraud alert

B.a user risk policy

C.a named location

D.a sign-in user policy

Answer: C

Explanation:

Named locations can be defined by IPv4/IPv6 address ranges or by countries.https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/location-condition#named-locations

Reference:

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

Question: 21 CertyIQ

You are configuring Microsoft Cloud App Security.
You have a custom threat detection policy based on the IP address ranges of your company's United States-based offices.
You receive many alerts related to impossible travel and sign-ins from risky IP addresses.
You determine that 99% of the alerts are legitimate sign-ins from your corporate offices.
You need to prevent alerts for legitimate sign-ins from known locations.
Which two actions should you perform? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

A.Configure automatic data enrichment.

B.Add the IP addresses to the corporate address range category.

C.Increase the sensitivity level of the impossible travel anomaly detection policy.

D.Add the IP addresses to the other address range category and add a tag.

E.Create an activity policy that has an exclusion for the IP addresses.

Answer: AB

Explanation:

A - this seems correct, as if you override the automatic detection of location for company IP address ranges, you can prevent the impossible travel alerts.B - This makes sense as you need to define your corporate address ranges so that they are not seen as risky.C - Increasing the sensitivity of the impossible travel detection would create more alerts.D - Why would you set the IP addresses to the "Other" category when there is a "Corporate" category that fits the description?E - Creating a new policy when there is already an existing one that you need to reduce the alerts from, would not reduce the number of alerts.

You can add IP range through API enrichment or "add IP range" and give it "Corporate" category.

Question: 22 CertyIQ

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: You add each account as a Sensitive account.
Does this meet the goal?

A.Yes

B.No

Answer: B

Explanation:

Reference:
https://docs.microsoft.com/en-us/defender-for-identity/manage-sensitive-honeytoken-accounts

Question: 23 CertyIQ

You have a Microsoft 365 tenant that uses Microsoft Exchange Online and Microsoft Defender for Office 365.
What should you use to identify whether zero-hour auto purge (ZAP) moved an email message from the mailbox of a user?

A.the Threat Protection Status report in Microsoft Defender for Office 365

B.the mailbox audit log in Exchange

C.the Safe Attachments file types report in Microsoft Defender for Office 365

D.the mail flow report in Exchange

Answer: A

Explanation:
To determine if ZAP moved your message, you can use either the Threat Protection Status report or Threat Explorer (and real-time detections).

Reference:
https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/zero-hour-auto-purge?view=o365-worldwide

Question: 24 CertyIQ

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

What should you use?

A.Microsoft Defender Antivirus

B.attack surface reduction rules in Microsoft Defender for Endpoint

C.Windows Defender Firewall

D.adaptive application control in Azure Defender

Answer: B

Explanation:

B: Attack Surface Reduction rules.https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/attack-surface-reduction-rules-reference?view=o365-worldwideBlock all Office applications from creating child processesBlock executable content from email client and webmail

Reference:

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

Question: 25 CertyIQ

You have a third-party security information and event management (SIEM) solution.
You need to ensure that the SIEM solution can generate alerts for Azure Active Directory (Azure AD) sign-events in near real time.
What should you do to route events to the SIEM solution?

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

Answer: B

Explanation:

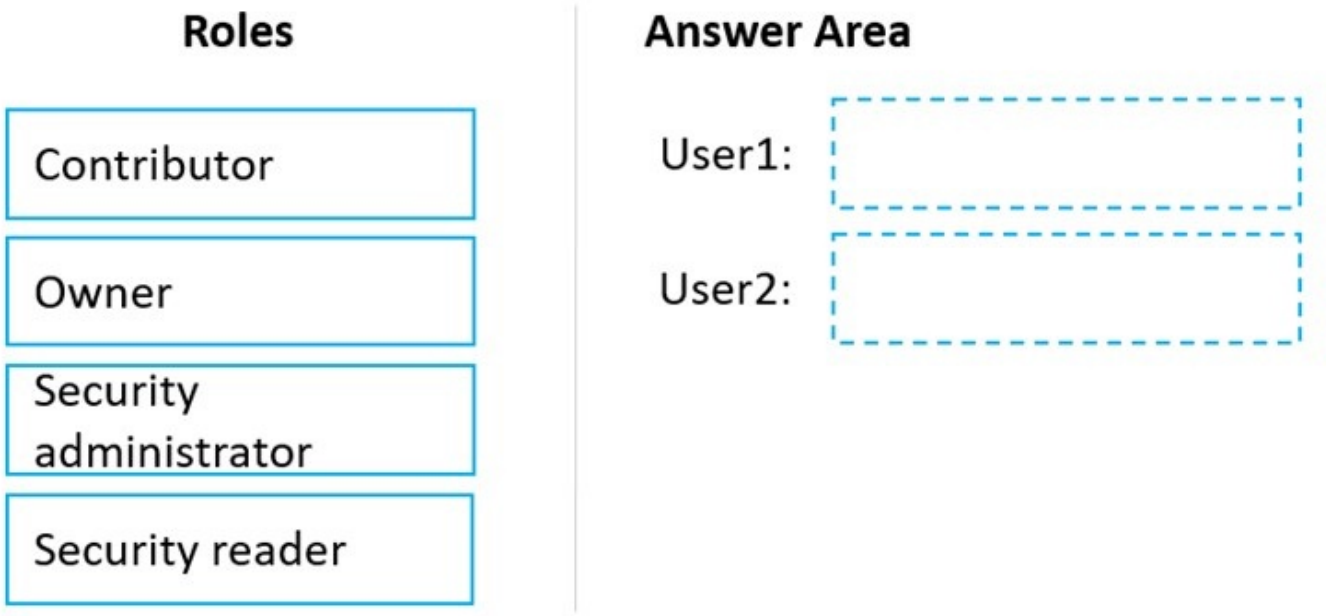
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/overview-monitoring

Question: 26 CertyIQ

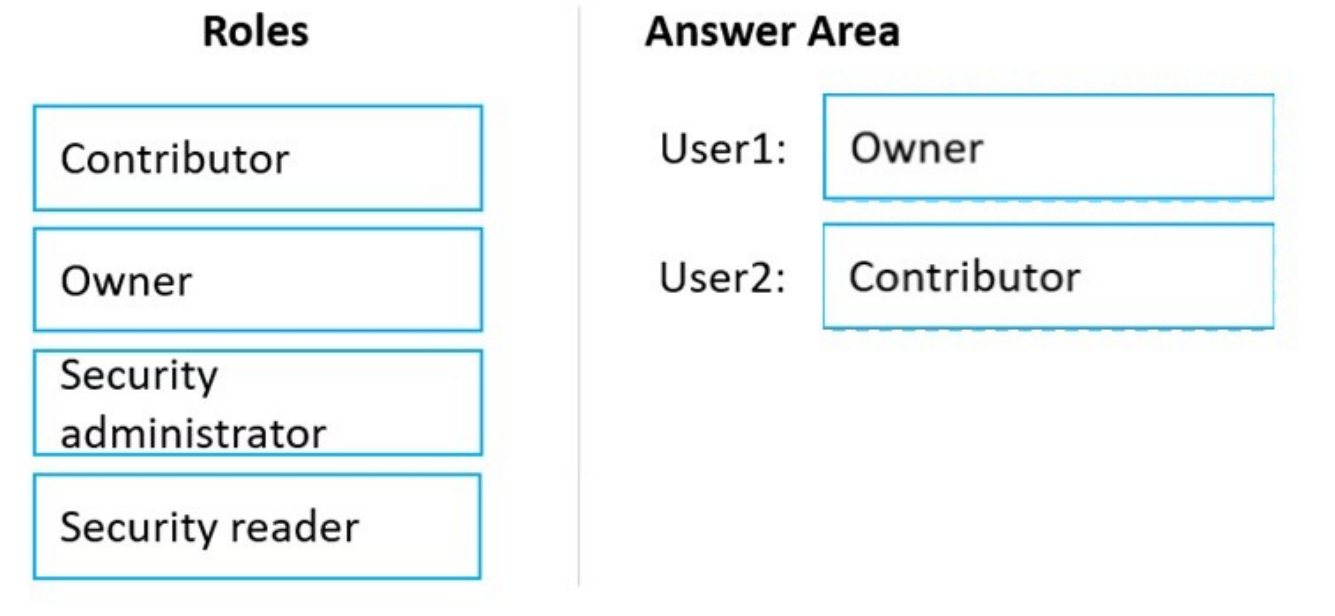
DRAG DROP -
You have an Azure subscription linked to an Azure Active Directory (Azure AD) tenant. The tenant contains two users named User1 and User2.
You plan to deploy Azure Defender.
You need to enable User1 and User2 to perform tasks at the subscription level as shown in the following table.

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.
Select and Place:



Answer:



Explanation:
Box 1: Owner -
Only the Owner can assign initiatives.

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

Question: 27 CertyIQ

HOTSPOT -
You have a Microsoft 365 E5 subscription that contains 200 Windows 10 devices enrolled in Microsoft Defender for Endpoint.
You need to ensure that users can access the devices by using a remote shell connection directly from the Microsoft 365 Defender portal. The solution must use the principle of least privilege.

What should you do in the Microsoft 365 Defender portal? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.
Hot Area:

Answer Area

To configure Microsoft Defender for Endpoint:
- Turn on endpoint detection and response (EDR) in block mode
- Turn on Live Response
- Turn off Tamper Protection

To configure the devices:
- Add a network assessment job
- Create a device group that contains the devices and set Automation level to Full
- Create a device group that contains the devices and set Automation level to No automated response

Answer:

Answer Area

To configure Microsoft Defender for Endpoint:
- Turn on endpoint detection and response (EDR) in block mode
- **Turn on Live Response**
- Turn off Tamper Protection

To configure the devices:
- Add a network assessment job
- **Create a device group that contains the devices and set Automation level to Full**
- Create a device group that contains the devices and set Automation level to No automated response

Explanation:

Box 1: Turn on Live Response -

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

Box: 2 - create a device group that contains the devices and set Automation level to Full

Question: 28

CertyIQ

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

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

extend
join
project

project
summarize
take

Answer:

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

extend
join
project

project
summarize
take

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=o365-worldwide

Question: 29 CertyIQ

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 access review policy
C.an alert policy in Microsoft Defender for Office 365
D.an insider risk policy

Answer: D

Explanation:

D: Insider risk policy.Data theft by departing users:https://learn.microsoft.com/en-us/microsoft-365/compliance/insider-risk-management-policies?view=o365-worldwide#data-theft-by-departing-usersWhen users leave your organization, there are specific risk indicators typically associated with data theft by departing users. This policy template uses exfiltration indicators for risk scoring and focuses on detection and alerts in this risk area.

To be notified if the deleted users downloaded numerous documents from SharePoint Online sites during the month before their accounts were deleted, you should use an insider risk policy.Insider risk policies in Microsoft 365 can monitor user activity across different services, including SharePoint Online, to detect potential insider risks such as data leaks or theft. You can configure an insider risk policy to trigger an alert when certain user activity matches a defined risk level or condition, such as downloading a large number of

documents.

Question: 30 CertyIQ

You have a Microsoft 365 subscription that has Microsoft 365 Defender enabled.
You need to identify all the changes made to sensitivity labels during the past seven days.
What should you use?

A.the Incidents blade of the Microsoft 365 Defender portal
B.the Alerts settings on the Data Loss Prevention blade of the Microsoft 365 compliance center
C.Activity explorer in the Microsoft 365 compliance center
D.the Explorer settings on the Email & collaboration blade of the Microsoft 365 Defender portal

Answer: C

Explanation:
Labeling activities are available in Activity explorer.
For example:

Sensitivity label applied -
This event is generated each time an unlabeled document is labeled or an email is sent with a sensitivity label.
It is captured at the time of save in Office native applications and web applications.
It is captured at the time of occurrence in Azure Information protection add-ins.
Upgrade and downgrade labels actions can also be monitored via the Label event type field and filter.

Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/data-classification-activity-explorer-available-events?view=o365-worldwide

Question: 31 CertyIQ

You have a Microsoft 365 subscription that uses Microsoft 365 Defender.
You need to identify all the entities affected by an incident.
Which tab should you use in the Microsoft 365 Defender portal?

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

Answer: C

Explanation:
The Evidence and Response tab shows all the supported events and suspicious entities in the alerts in the incident.
Incorrect:
* The Investigations tab lists all the automated investigations triggered by alerts in this incident. Automated investigations will perform remediation actions or wait for analyst approval of actions, depending on how you configured your automated investigations to run in Defender for Endpoint and Defender for Office 365.
* Devices
The Devices tab lists all the devices related to the incident.

Reference:
https://docs.microsoft.com/en-us/microsoft-365/security/defender/investigate-incidents

Question: 32 CertyIQ

You have a Microsoft 365 E5 subscription that is linked to a hybrid Azure AD tenant.

You need to identify all the changes made to Domain Admins group during the past 30 days.

What should you use?

A.the Modifications of sensitive groups report in Microsoft Defender for Identity
B.the identity security posture assessment in Microsoft Defender for Cloud Apps
C.the Azure Active Directory Provisioning Analysis workbook
D.the Overview settings of Insider risk management

Answer: A

Explanation:

A. The Modifications of sensitive groups report in Microsoft Defender for Identity would be the best option to use to identify all the changes made to the Domain Admins group during the past 30 days. This report provides information about changes made to sensitive groups, including the Domain Admins group, in the Azure AD environment and helps to identify potential security threats.

Question: 33 CertyIQ

You have a Microsoft 365 subscription. The subscription uses Microsoft 365 Defender and has data loss prevention (DLP) policies that have aggregated alerts configured.

You need to identify the impacted entities in an aggregated alert.

What should you review in the DLP alert management dashboard of the Microsoft 365 compliance center?

A.the Events tab of the alert
B.the Sensitive Info Types tab of the alert
C.Management log
D.the Details tab of the alert

Answer: A

Explanation:

In order to identify the impacted entities in an aggregated alert, you should review the "Events" tab of the DLP alert management dashboard in the Microsoft 365 compliance center. This tab will display a list of all the events that triggered the alert, including the specific entities (e.g. files, emails, etc.) that were affected. You can further investigate each event to identify the specific user, device and action that caused the alert to be triggered.

The correct answer is A.More on: https://learn.microsoft.com/en-us/microsoft-365/compliance/dlp-configure-view-alerts-policies?view=o365-worldwide

Question: 34 CertyIQ

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

You plan to create a hunting query from Microsoft Defender.

You need to create a custom tracked query that will be used to assess the threat status of the subscription.

From the Microsoft 365 Defender portal, which page should you use to create the query?

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

Answer: B

Explanation:

https://learn.microsoft.com/en-us/microsoft-365/security/defender/advanced-hunting-overview?view=o365-worldwide"Use Advance mode if you're comfortable creating custom queries." Answer is B

Question: 35 CertyIQ

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

You need to add threat indicators for all the IP addresses in a range of 171.23.34.32-171.23.34.63. The solution must minimize administrative effort.

What should you do in the Microsoft 365 Defender portal?

A.Create an import file that contains the individual IP addresses in the range. Select Import and import the file.
B.Create an import file that contains the IP address of 171.23.34.32/27. Select Import and import the file.
C.Select Add indicator and set the IP address to 171.23.34.32-171.23.34.63.
D.Select Add indicator and set the IP address to 171.23.34.32/27.

Answer: A

Explanation:

You can choose to upload a CSV file that defines the attributes of indicators, the action to be taken, and other details.Type of the indicator. Possible values are: "FileSha1", "FileSha256", "IpAddress", "DomainName" and "Url".Classless Inter-Domain Routing (CIDR) notation for IP addresses is not supported.
https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/indicator-manage

Question: 36 CertyIQ

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

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

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

A.custom network indicators

B.live response for servers

C.endpoint detection and response (EDR) in block mode

D.web content filtering

Answer: A

Explanation:

Answer A is correct. Checked it thru MS defender for Endpoint portal.Custom network indicatorsConfigures devices to allow or block connections to IP addresses, domains, or URLs in your custom indicator lists. To use this feature, devices must be running Windows 10 version 1709 or later. They should also have network protection in block mode and version 4.18.1906.3 or later of the antimalware platform (see KB 4052623). Note that network protection leverages reputation services that process requests in locations that might be outside of the location you have selected for your Microsoft Defender for Endpoint data.

Question: 37 CertyIQ

DRAG DROP
-

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:

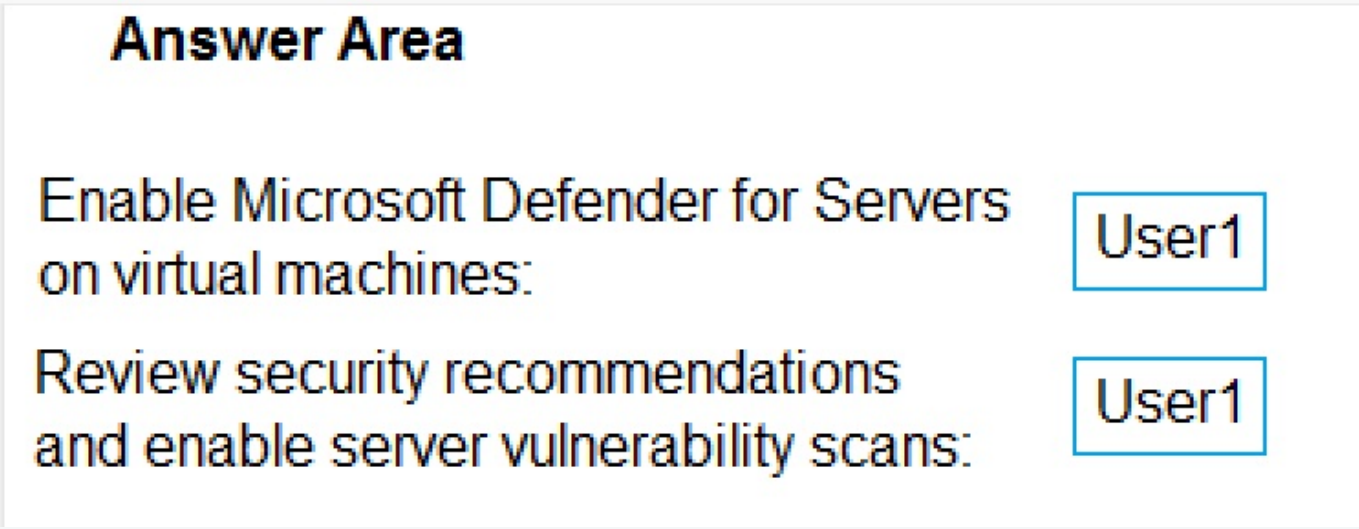
•Enable Microsoft Defender for Servers on virtual machines.
•Review security recommendations and enable server vulnerability scans.

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.

Answer:



Explanation:

It be User1 for both!How security reader can enable server vulnerability scans?User1User1

Question: 38 CertyIQ

HOTSPOT
-

You have a Microsoft 365 E5 subscription.

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

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

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

NOTE: Each correct selection is worth one point.

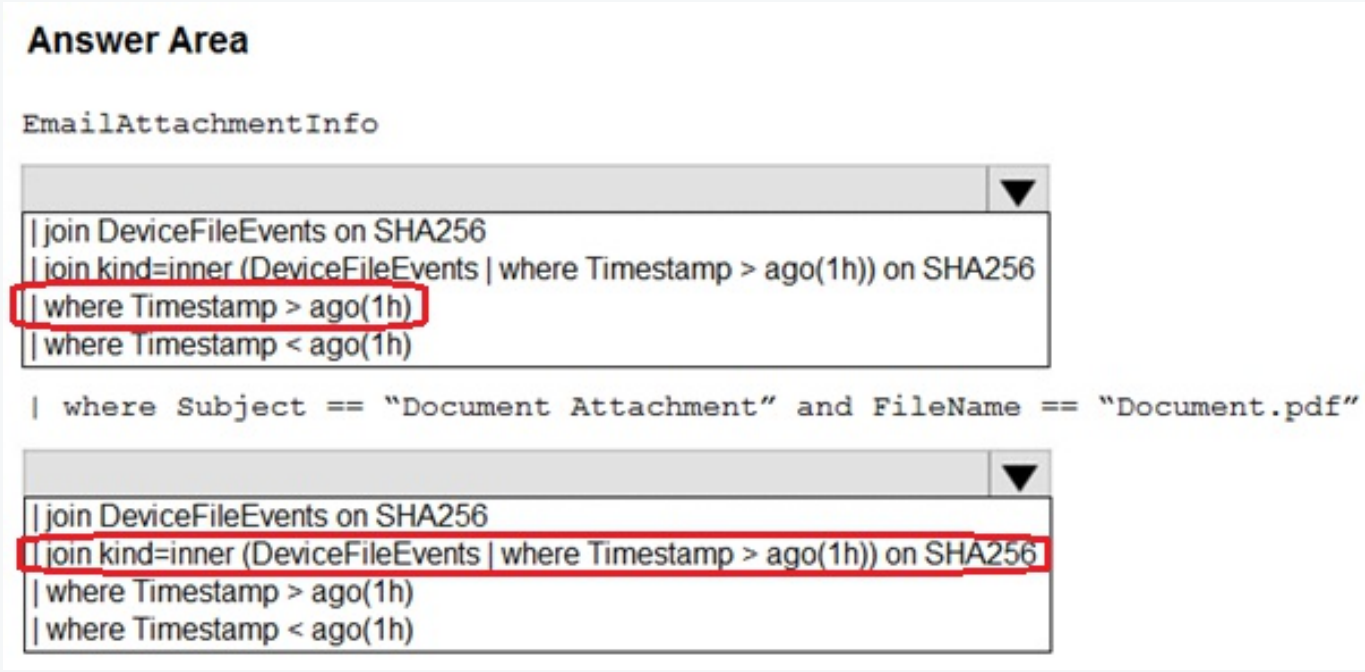
Answer Area

```
EmailAttachmentInfo
[ ▼ ]
| where Subject == "Document Attachment" and FileName == "Document.pdf"
[ ▼ ]
```

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

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

Answer:



Question: 39 CertyIQ

Your company has an on-premises network that uses Microsoft Defender for Identity.

The Microsoft Secure Score for the company includes a security assessment associated with unsecure Kerberos delegation.

You need remediate the security risk.

What should you do?

A.Disable legacy protocols on the computers listed as exposed entities.

B.Enforce LDAP signing on the computers listed as exposed entities.

C.Modify the properties of the computer objects listed as exposed entities.

D.Install the Local Administrator Password Solution (LAPS) extension on the computers listed as exposed entities.

Answer: C

Explanation:

Option A, disabling legacy protocols, is not relevant to the question since it's a security measure that restricts the use of legacy protocols that may be less secure than modern protocols.Option B, enforcing LDAP signing, is also not relevant to the question since it's a security measure that ensures that LDAP traffic is signed and encrypted.Option D, installing the Local Administrator Password Solution (LAPS) extension, is not relevant to the question since it's a solution that automatically manages local administrator account passwords to help prevent credential theft.Therefore, the correct answer is C. Modify the properties of the computer objects listed as exposed entities.

Question: 40 CertyIQ

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

A remediation action for an automated investigation quarantines a file across multiple devices.

You need to mark the file as safe and remove the file from quarantine on the devices.

What should you use in the Microsoft 365 Defender portal?

A.From the History tab in the Action center, revert the actions.
B.From the investigation page, review the AIR processes.
C.From Quarantine from the Review page, modify the rules.
D.From Threat tracker, review the queries.

Answer: A

Explanation:

https://learn.microsoft.com/en-us/microsoft-365/security/defender/m365d-autoir-actions?view=o365-worldwide#undo-completed-actions

Question: 41 CertyIQ

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

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

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

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

Answer: B

Explanation:

it is Bhttps://learn.microsoft.com/en-us/microsoft-365/security/defender/threat-analytics?view=o365-worldwide

Question: 42 CertyIQ

Case study -

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 -

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 minimize the effort required to investigate the Microsoft Defender for Identity false positive alerts.

What should you review?

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

Answer: D

Explanation:

https://learn.microsoft.com/en-us/defender-for-identity/understanding-security-alerts#defender-for-identity-and-nnr-network-name-resolution

Question: 43 CertyIQ

HOTSPOT
-

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

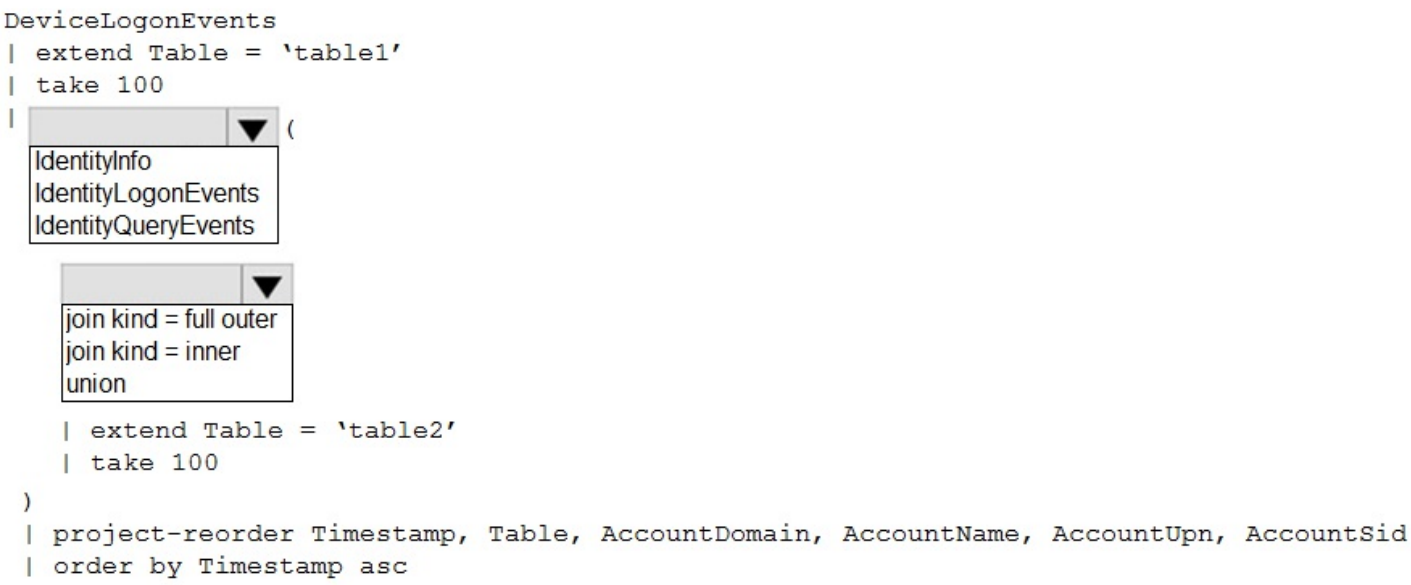
Your network contains an on-premises Active Directory Domain Services (AD DS) domain that syncs with Azure AD.

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 Area



Answer:

Answer Area

```
DeviceLogonEvents
| extend Table = 'table1'
| take 100
| [IdentityInfo / IdentityLogonEvents / IdentityQueryEvents] (
    [join kind = full outer / join kind = inner / union]
    | extend Table = 'table2'
    | take 100
)
| project-reorder Timestamp, Table, AccountDomain, AccountName, AccountUpn, AccountSid
| order by Timestamp asc
```

Question: 44 CertyIQ

HOTSPOT
-

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 LDAP requests by AD DS users to enumerate AD DS objects.

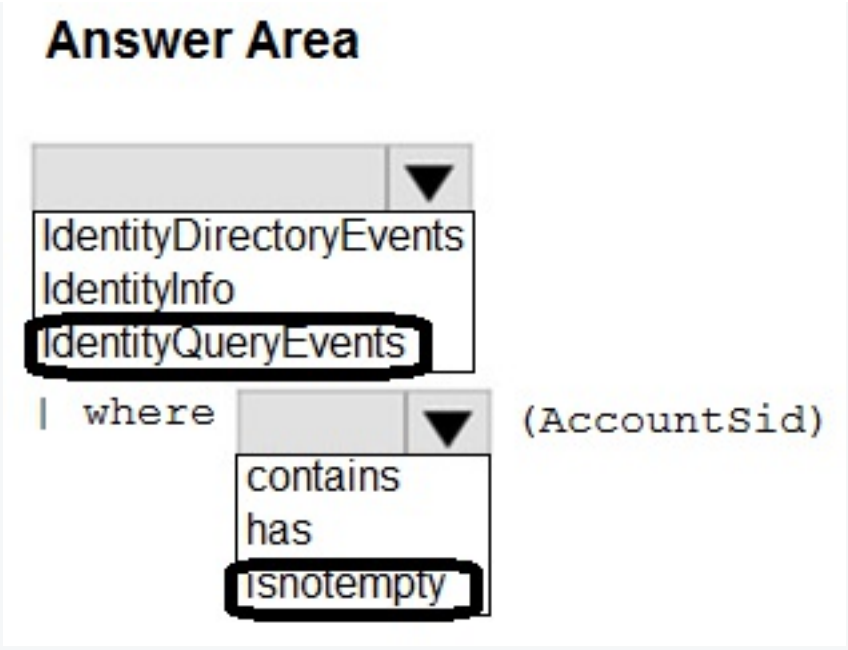
How should you complete the KQL query? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

```
[IdentityDirectoryEvents / IdentityInfo / IdentityQueryEvents]
| where [contains / has / isnotempty] (AccountSid)
```

Answer:



Question: 45 CertyIQ

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: C

Explanation:

C - Office 365 connector

https://learn.microsoft.com/en-us/defender-cloud-apps/connect-office-365

Question: 46 CertyIQ

51 HOTSPOT

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 Area

Statements	Yes	No
The custom detection rule can be used to automate the deletion of email messages from a user's mailbox based on the `RecipientEmailAddress` column.	○	○
The custom detection rule can be used to restrict app execution automatically based on the `DeviceId` column.	○	○
The custom detection rule can be used to automate the deletion of a file based on the `SHA256` column.	○	○

Answer:

Answer Area

Statements	Yes	No
The custom detection rule can be used to automate the deletion of email messages from a user's mailbox based on the `RecipientEmailAddress` column.	◉	○
The custom detection rule can be used to restrict app execution automatically based on the `DeviceId` column.	○	◉
The custom detection rule can be used to automate the deletion of a file based on the `SHA256` column.	○	◉

Question: 47 CertyIQ

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

You enable agentless scanning.

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

What should you do?

A.Create an exclusion tag.

B.Upgrade the subscription to Defender for Servers Plan 2.

C.Create a governance rule.

D.Create an exclusion group.

Answer: A

Explanation:

A. Create an exclusion tag.

https://learn.microsoft.com/en-us/azure/defender-for-cloud/enable-agentless-scanning-vms

Question: 48 CertyIQ

You need to configure Microsoft Defender for Cloud Apps to generate alerts and trigger remediation actions in response to external sharing of confidential files.

Which two actions should you perform in the Microsoft 365 Defender 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.From Cloud apps, select Files, and then filter File Type to Document.
B. From Settings, select Information Protection, select Files, and then enable file monitoring.

D.From Cloud apps, select Files, and then filter App to Office 365.

E.From Cloud apps, select Files, and then select New policy from search.

F.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.

Answer: CF

Explanation:

Correction in question.

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.From Cloud apps, select Files, and then filter File Type to Document.

C. From Settings, select Information Protection, select Files, and then enable file monitoring.

D.From Cloud apps, select Files, and then filter App to Office 365.

E.From Cloud apps, select Files, and then select New policy from search.

F.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.

Correct answer=CF

C. From Settings, select Information Protection, select Files, and then enable file monitoring.

F.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.

Question: 49 CertyIQ

HOTSPOT
-

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

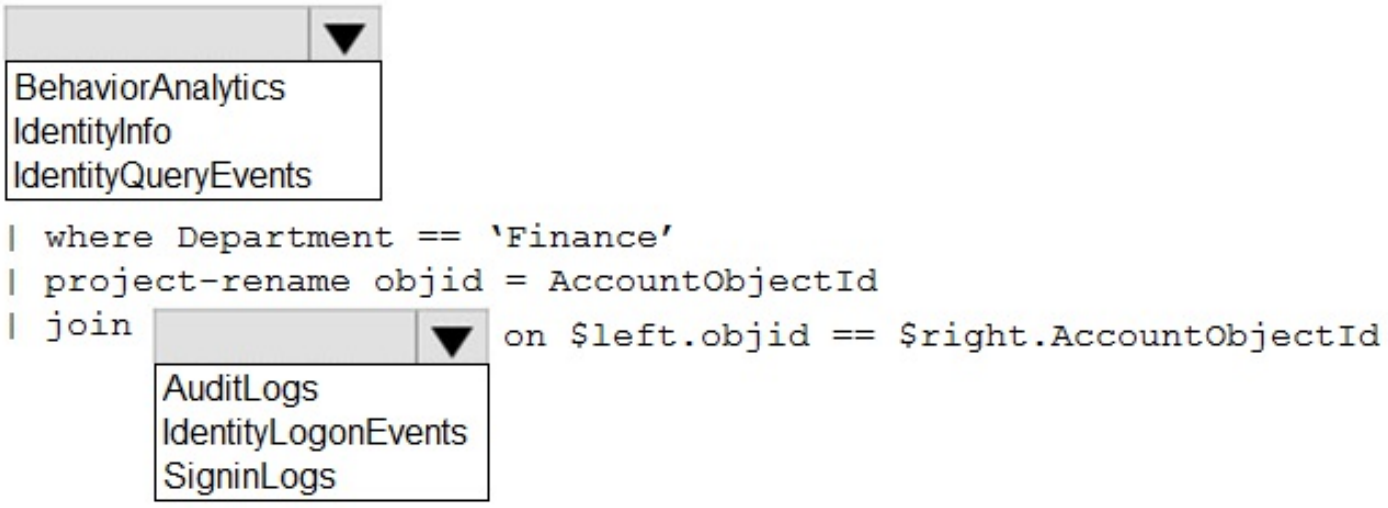
You have a Microsoft 365 E5 subscription that uses Microsoft Defender 365.

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.

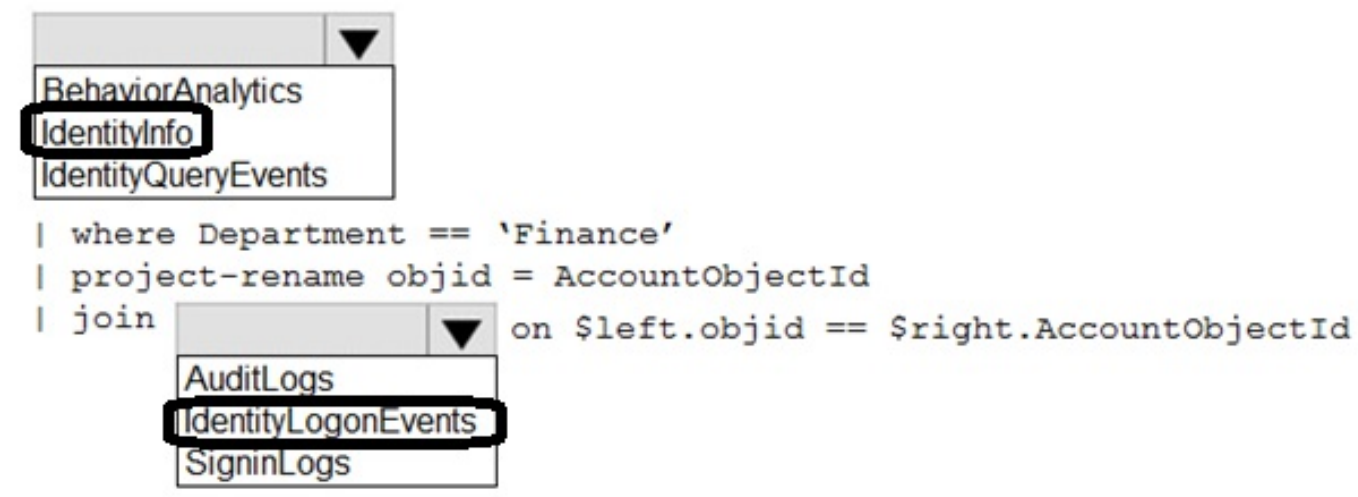
NOTE: Each correct selection is worth one point.

Answer Area



Answer:

Answer Area



Question: 50 CertyIQ

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

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

What should you use in the Microsoft 365 Defender portal?

A.incidents
B.Remediation
C.Investigations
D.Advanced hunting

Answer: C

Explanation:

C. Investigations

Question: 51 CertyIQ

HOTSPOT
-

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

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

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

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

NOTE: Each correct selection is worth one point.

Answer Area

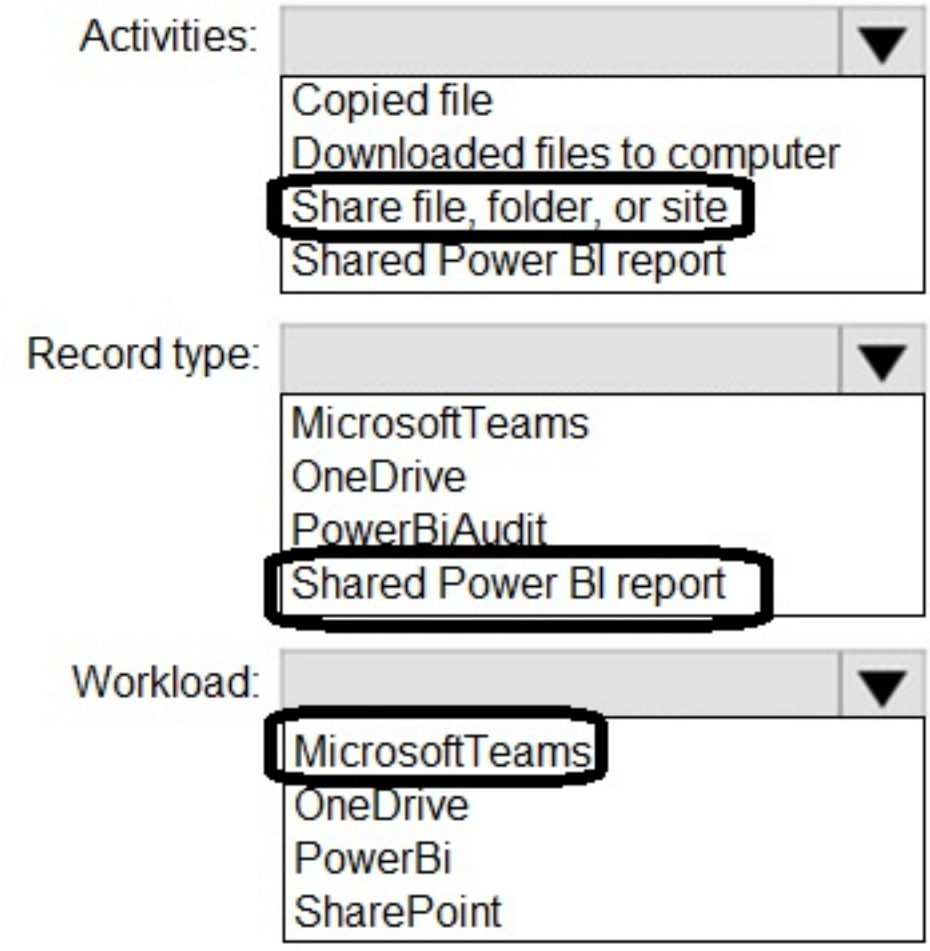
Activities:
- Copied file
- Downloaded files to computer
- Share file, folder, or site
- Shared Power BI report

Record type:
- MicrosoftTeams
- OneDrive
- PowerBiAudit
- Shared Power BI report

Workload:
- MicrosoftTeams
- OneDrive
- PowerBi
- SharePoint

Answer:

Answer Area



Question: 52 CertyIQ

DRAG DROP
-

Case study
-

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 energy 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 Defender for Cloud Apps 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
-

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

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
-

Microsoft Defender for Cloud Apps frequently generates false positive alerts when users connect to both offices simultaneously.

Planned Changes and Requirements

Planned Changes
-

Litware plans to implement the following changes:

•Create and configure Microsoft Sentinel in the Azure subscription.
•Validate Microsoft Sentinel functionality by using Azure AD test user accounts.

Business Requirements
-

Litware identifies the following business requirements:

•The principle of least privilege must be used whenever possible.
•Costs must be minimized, as long as all other requirements are met.
•Logs collected by Log Analytics must provide a full audit trail of user activities.
•All domain controllers must be protected by using Microsoft Defender for Identity.

Azure Information Protection Requirements

All files that have sensitivity 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 Microsoft Defender for Cloud Apps unsanctioned apps must be blocked on the Windows 10 computers by using Microsoft Defender for Endpoint.

Microsoft Defender for Cloud Apps Security Requirements

Microsoft Defender for Cloud Apps must identify whether a user connection is anomalous based on tenant-level data.

Microsoft Defender for Cloud Requirements

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

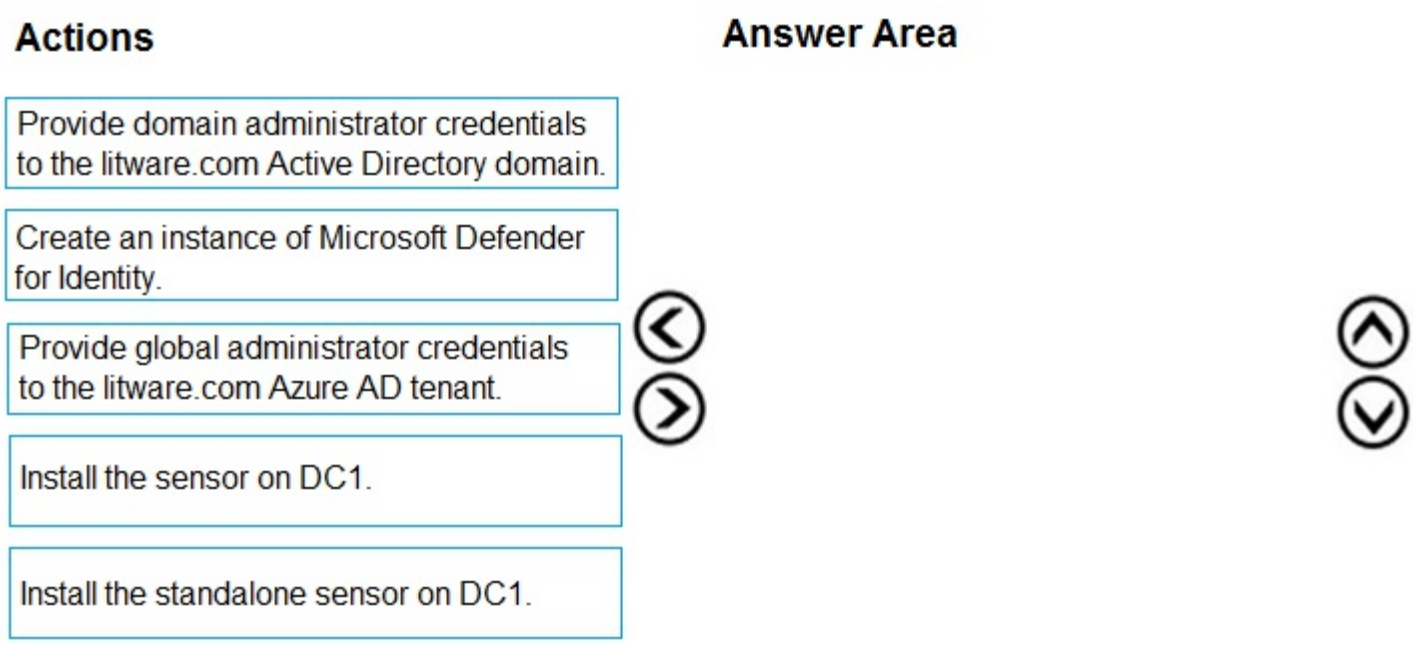
Microsoft Sentinel Requirements

Litware must meet the following Microsoft Sentinel requirements:

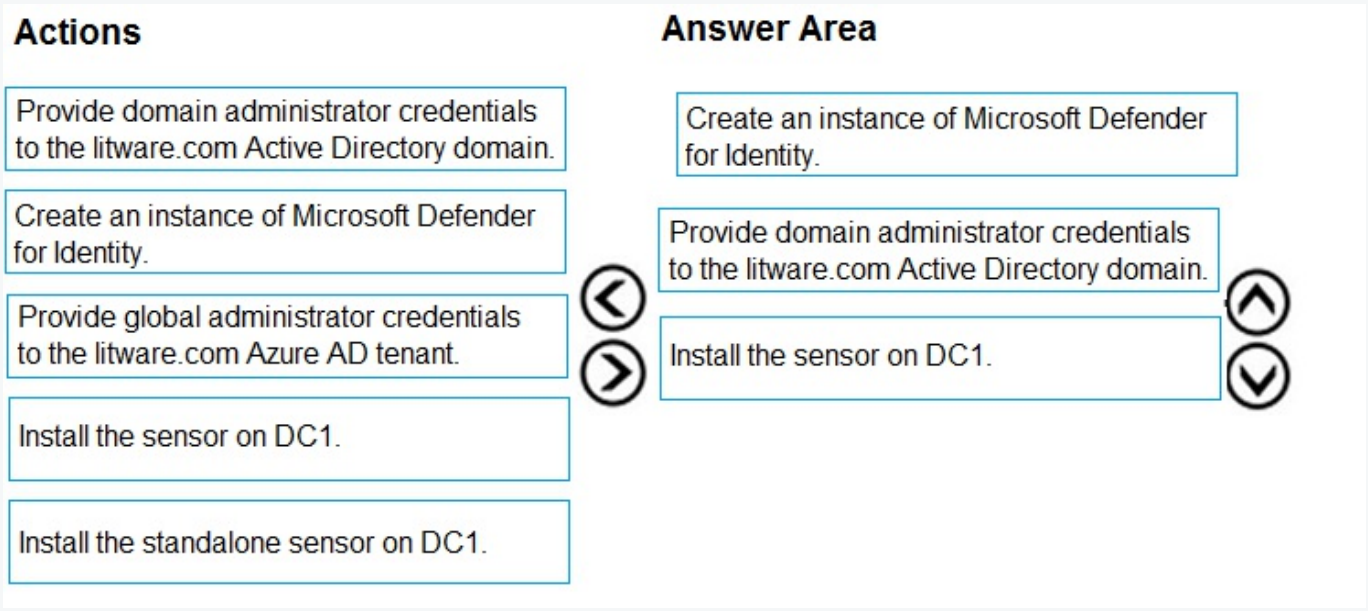
•Integrate Microsoft Sentinel and Microsoft Defender for Cloud Apps.
•Ensure that a user named admin1 can configure Microsoft Sentinel playbooks.
•Create a Microsoft Sentinel analytics rule based on a custom query. The rule must automatically initiate the execution of a playbook.
•Add notes to events 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.

You need to configure DC1 to meet the business requirements.

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:

1). Create an instance of MS Defender for Identity.

2). Provide domain admin credentials.

3). install the sensor on DC1.

Question: 53 CertyIQ

You have a Microsoft 365 subscription that uses Microsoft Purview and Microsoft Teams.

You have a team named Team1 that has a project named Project1.

You need to identify any Project1 files that were stored on the team site of Team1 between February 1, 2023, and February 10, 2023.

Which KQL query should you run?

A.(c:c)(Project1)(date=(2023-02-01)..date=(2023-02-10))

B.AuditLogs -
| where Timestamp between (datetime(2023-02-01)..datetime(2023-02-10))
| where FileName contains “Project1”

C.Project1(c:c)(date=2023-02-01..2023-02-10)

D.AuditLogs -
| where Timestamp > ago(10d)
| where FileName contains “Project1”

Answer: C

Explanation:

Tested in content search in the purview portal. project1(c:c)(date=2023-02-01..2023-02-10)This is the correct syntax for KQL content search in Purview, and searches for keyword "project1" in selected team, and between said dates.

Question: 54 CertyIQ

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

You need to create a query that will link the AlertInfo, AlertEvidence, and DeviceLogonEvents tables. The solution must return all the rows in the tables.

Which operator should you use?

A.search *

B.union kind = inner

C.join kind = inner

D.evaluate hint.remote =

Answer: B

Explanation:

B. Correct Answer. Union takes two or more tables and returns the rows of all of them. C. Join Kind inner will not produce every row as inner means output has one row for every combination of left and right. So only if the columns appears in both tables will we get a hit. This doesn't meet the ask. D. Evaluate in KQL calls a plugin this is not relevant to the question

Question: 55 CertyIQ

You have a Microsoft 365 E5 subscription that contains 100 Windows 10 devices.

You onboard the devices to Microsoft Defender 365.

You need to ensure that you can initiate remote shell connections to the onboarded devices from the Microsoft 365 Defender portal.

What should you do first?

A.Modify the permissions for Microsoft 365 Defender.

B.Create a device group.

C.From Advanced features in the Endpoints settings of the Microsoft 365 Defender portal, enable automated investigation.

D.Configure role-based access control (RBAC).

Answer: D

Explanation:

Configure role-based access control (RBAC).

Reference:

https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/live-response?view=o365-worldwide

Question: 56

CertyIQ

HOTSPOT
-

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

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

```
DeviceTvmSoftwareVulnerabilities
| where VulnerabilitySeverityLevel == 'Critical'
```

[▼]

- | distinct CveId
- | distinct DeviceId
- | project-away CveId
- | project-keep DeviceId

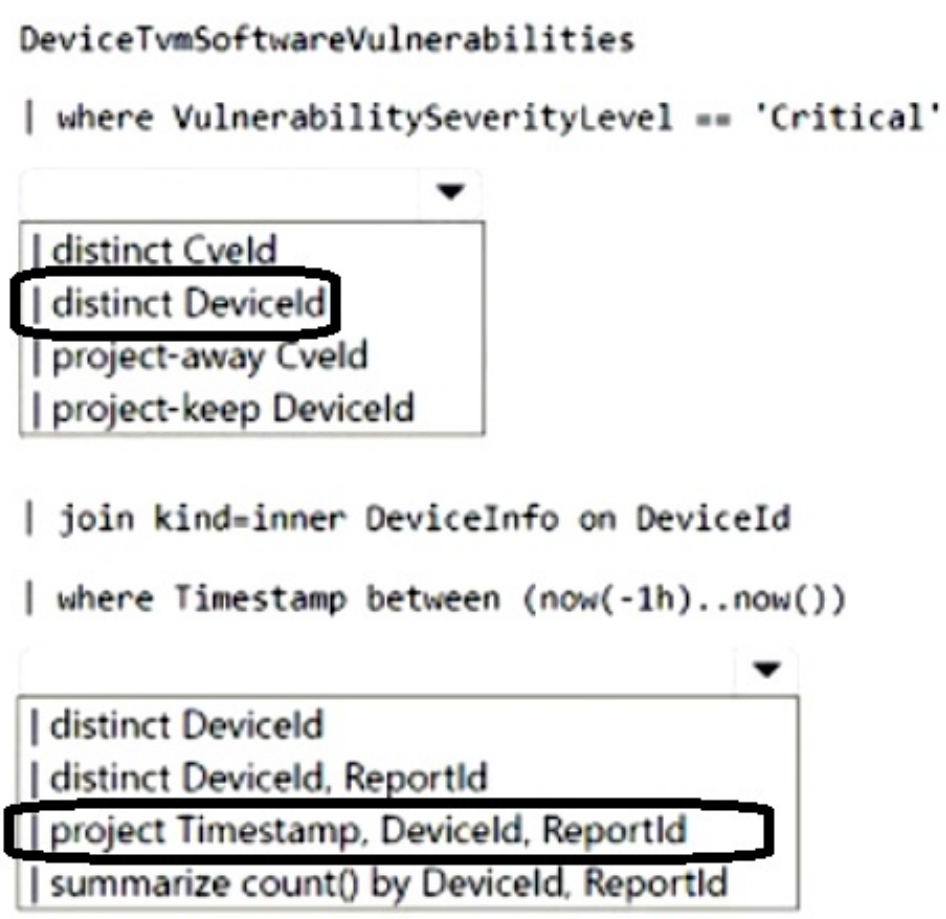
```
| join kind=inner DeviceInfo on DeviceId
| where Timestamp between (now(-1h)..now())
```

[▼]

- | distinct DeviceId
- | distinct DeviceId, ReportId
- | project Timestamp, DeviceId, ReportId
- | summarize count() by DeviceId, ReportId

Answer:

Answer Area



Question: 57 CertyIQ

HOTSPOT
-

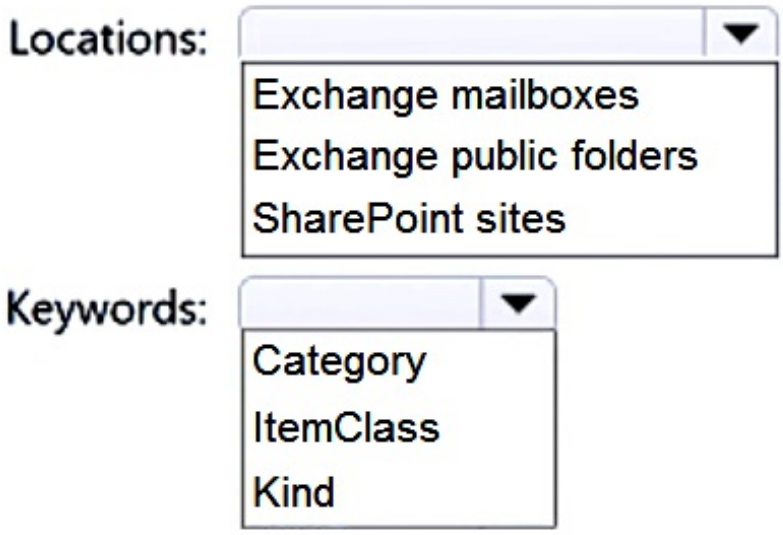
You have a Microsoft 365 E5 subscription that uses Microsoft Teams.

You need to perform a content search of Teams chats for a user by using the Microsoft Purview compliance portal. The solution must minimize the scope of the search.

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

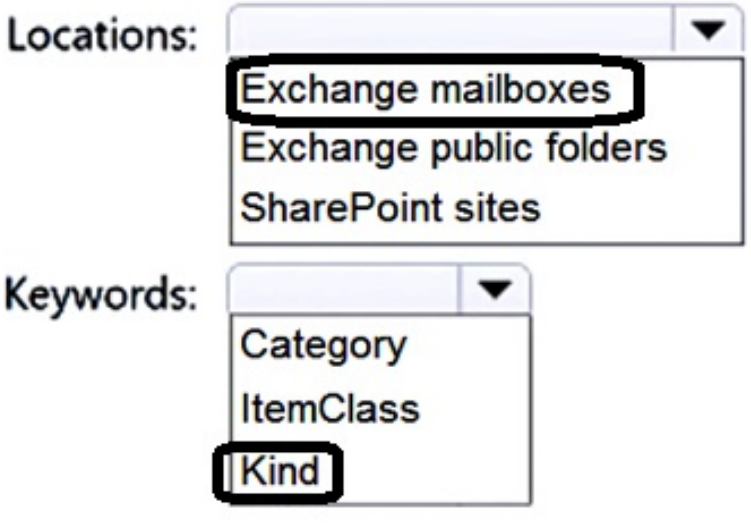
NOTE: Each correct selection is worth one point.

Answer Area



Answer:

Answer Area



Explanation:

Exchange mailboxes

Kind

Categories are "The categories to search. Categories can be defined by users by using Outlook or Outlook on the web... The possible values are red, blue, green, etc." Item Class: "Use this property to search specific third-party data types that your organization imported to Office 365." We are not importing any third-party data types. Kind: "The type of email message to search for. Possible values: contacts, microsoft teams, meetings, etc."

https://learn.microsoft.com/en-us/purview/ediscovery-keyword-queries-and-search-conditions

Question: 58 CertyIQ

You have a Microsoft 365 E5 subscription that contains 100 Linux devices. The devices are onboarded to Microsoft Defender 365.

You need to initiate the collection of investigation packages from the devices by using the Microsoft 365 Defender portal.

Which response action should you use?

A.Run antivirus scan

B.Initiate Automated Investigation

C.Collect investigation package

D.Initiate Live Response Session

Answer: D

Explanation:

Initiate Live Response Session.

Question: 59 CertyIQ

You need to configure Microsoft Defender for Cloud Apps to generate alerts and trigger remediation actions in response to external sharing of confidential files.

Which two actions should you perform in the Microsoft 365 Defender portal? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

A.From Settings, select Cloud App, select Microsoft Information Protection, and then select Only scan files for Microsoft Information Protection sensitivity labels and content inspection warnings from this tenant.

B.From Cloud apps, select Files, and then filter File Type to Document.

C.From Settings, select Cloud App, select Microsoft Information Protection, select Files, and then enable file monitoring.

D.From Cloud apps, select Files, and then filter App to Office 365.

E.From Cloud apps, select Files, and then select New policy from search.

F.From Settings, select Cloud App, select Microsoft Information Protection, and then select Automatically scan new files for Microsoft Information Protection sensitivity labels and content inspection warnings.

Answer: CF

Explanation:

C.From Settings, select Cloud App, select Microsoft Information Protection, select Files, and then enable file monitoring.

F. From Settings, select Cloud App, select Microsoft Information Protection, and then select Automatically scan new files for Microsoft Information Protection sensitivity labels and content inspection warnings.

Question: 60 CertyIQ

Note: This question is part of a series of questions that present the same scenario. Each question in the series

contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You use Azure Security Center.
You receive a security alert in Security Center.
You need to view recommendations to resolve the alert in Security Center.
Solution: From Security alerts, you select the alert, select Take Action, and then expand the Prevent future attacks section.
Does this meet the goal?

A.Yes

B.No

Answer: B

Explanation:
You need to resolve the existing alert, not prevent future alerts. Therefore, you need to select the 'Mitigate the threat' option.

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

Question: 61 CertyIQ

You receive an alert from Azure Defender for Key Vault.
You discover that the alert is generated from multiple suspicious IP addresses.
You need to reduce the potential of Key Vault secrets being leaked while you investigate the issue. The solution must be implemented as soon as possible and must minimize the impact on legitimate users.
What should you do first?

A.Modify the access control settings for the key vault.

B.Enable the Key Vault firewall.

C.Create an application security group.

D.Modify the access policy for the key vault.

Answer: B

Explanation:

Reference:
https://docs.microsoft.com/en-us/azure/security-center/defender-for-key-vault-usage

Question: 62 CertyIQ

HOTSPOT -
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.
Hot Area:

Answer Area

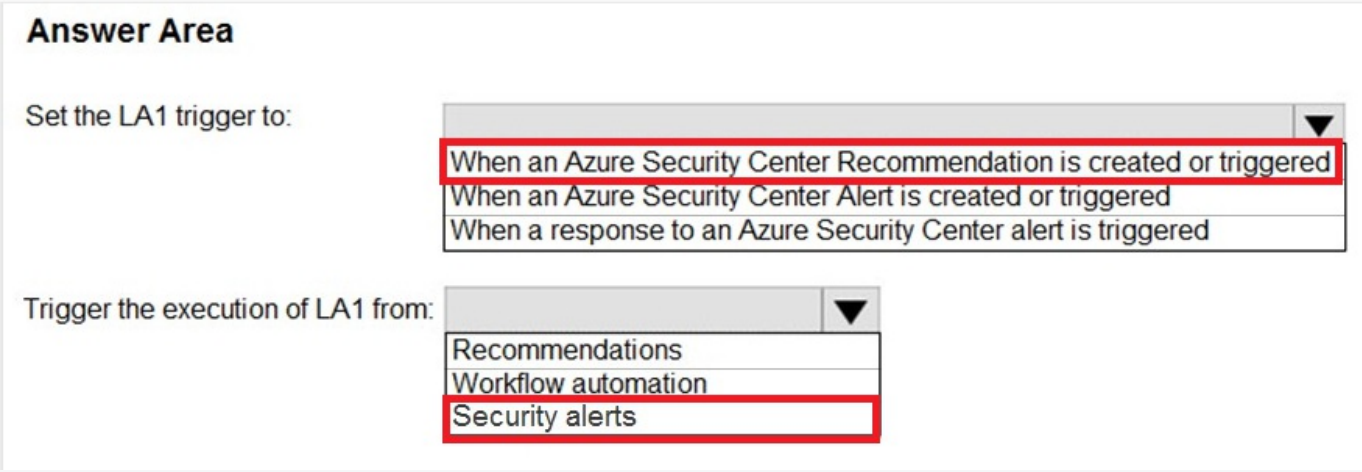
Set the LA1 trigger to:

- 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
- Security alerts

Answer:



Explanation:

When an Azure security center Recommendation is created or triggered.

security alerts.

Question: 63 CertyIQ

You have a Microsoft 365 subscription that uses Azure Defender.
You have 100 virtual machines in a resource group named RG1.
You assign the Security Admin roles to a new user named SecAdmin1.
You need to ensure that SecAdmin1 can apply quick fixes to the virtual machines by using Azure Defender. The solution must use the principle of least privilege.
Which role should you assign to SecAdmin1?

A.the Security Reader role for the subscription

B.the Contributor for the subscription

C.the Contributor role for RG1

D.the Owner role for RG1

Answer: C

Explanation:

To ensure that SecAdmin1 can apply quick fixes to the virtual machines by using Azure Defender, while also

following the principle of least privilege, you should assign the Contributor role for RG1 to SecAdmin1.The Contributor role for RG1 will allow SecAdmin1 to perform tasks such as deploying resources and modifying resource properties within RG1, but it will not grant them access to perform administrative tasks at the subscription level. This will allow SecAdmin1 to apply quick fixes to the virtual machines using Azure Defender, while still adhering to the principle of least privilege.

Question: 64 CertyIQ

You provision a Linux virtual machine in a new Azure subscription.
You enable Azure Defender and onboard the virtual machine to Azure Defender.
You need to verify that an attack on the virtual machine triggers an alert in Azure Defender.
Which two Bash commands should you run on the virtual machine? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

A.cp /bin/echo ./asc_alerttest_662jfi039n

B../alerttest testing eicar pipe

C.cp /bin/echo ./alerttest

D../asc_alerttest_662jfi039n testing eicar pipe

Answer: AD

Explanation:

Reference:
https://docs.microsoft.com/en-us/azure/security-center/security-center-alert-validation#simulate-alerts-on-your-azure-vms-linux-

Question: 65 CertyIQ

You create an Azure subscription named sub1.
In sub1, you create a Log Analytics workspace named workspace1.
You enable Azure Security Center and configure Security Center to use workspace1.
You need to collect security event logs from the Azure virtual machines that report to workspace1.
What should you do?

A.From Security Center, enable data collection

B.In sub1, register a provider.

C.From Security Center, create a Workflow automation.

D.In workspace1, create a workbook.

Answer: A

Explanation:

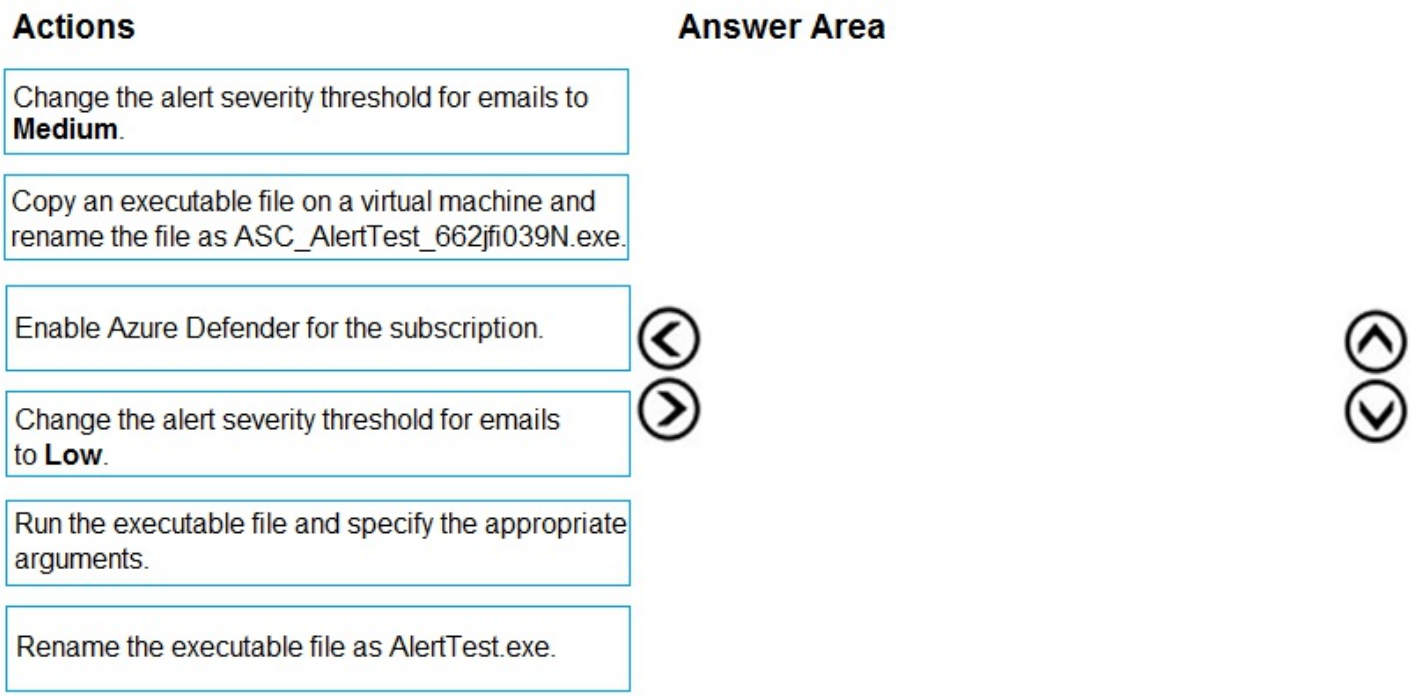
Data collectionStore additional raw data - Windows security eventsTo help audit, investigate, and analyze threats, you can collect raw events, logs, and additional security data and save it to your Log Analytics workspace.

Reference:

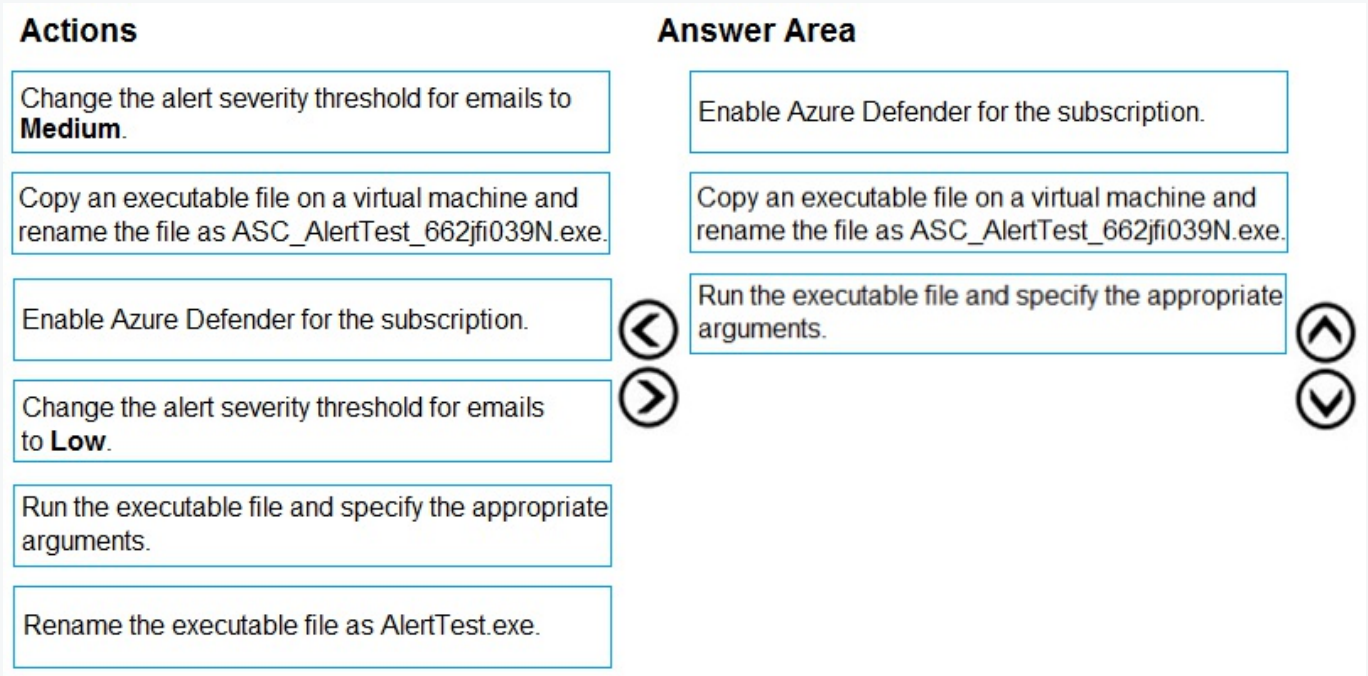
https://docs.microsoft.com/en-us/azure/security-center/security-center-enable-data-collection

Question: 66 CertyIQ

DRAG DROP -
You create a new Azure subscription and start collecting logs for Azure Monitor.
You need to configure Azure Security Center to detect possible threats related to sign-ins from suspicious IP addresses to Azure virtual machines. The solution must validate the configuration.
Which three actions should you perform in a sequence? To answer, move the appropriate actions from the list of action to the answer area and arrange them in the correct order.
Select and Place:



Answer:



Explanation:

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

Question: 67 CertyIQ

Your company uses Azure Security Center and Azure Defender.

The security operations team at the company informs you that it does NOT receive email notifications for security alerts.
What should you configure in Security Center to enable the email notifications?

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

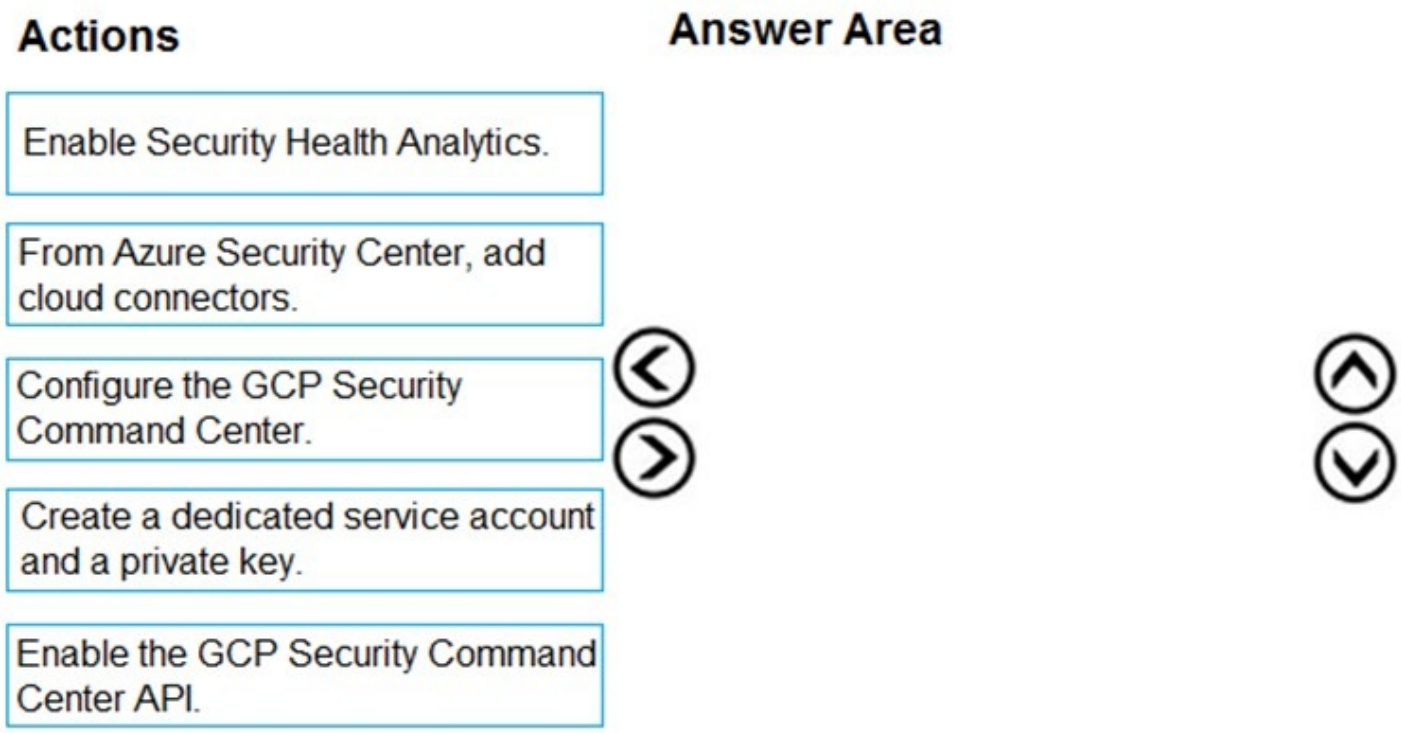
Answer: C

Explanation:

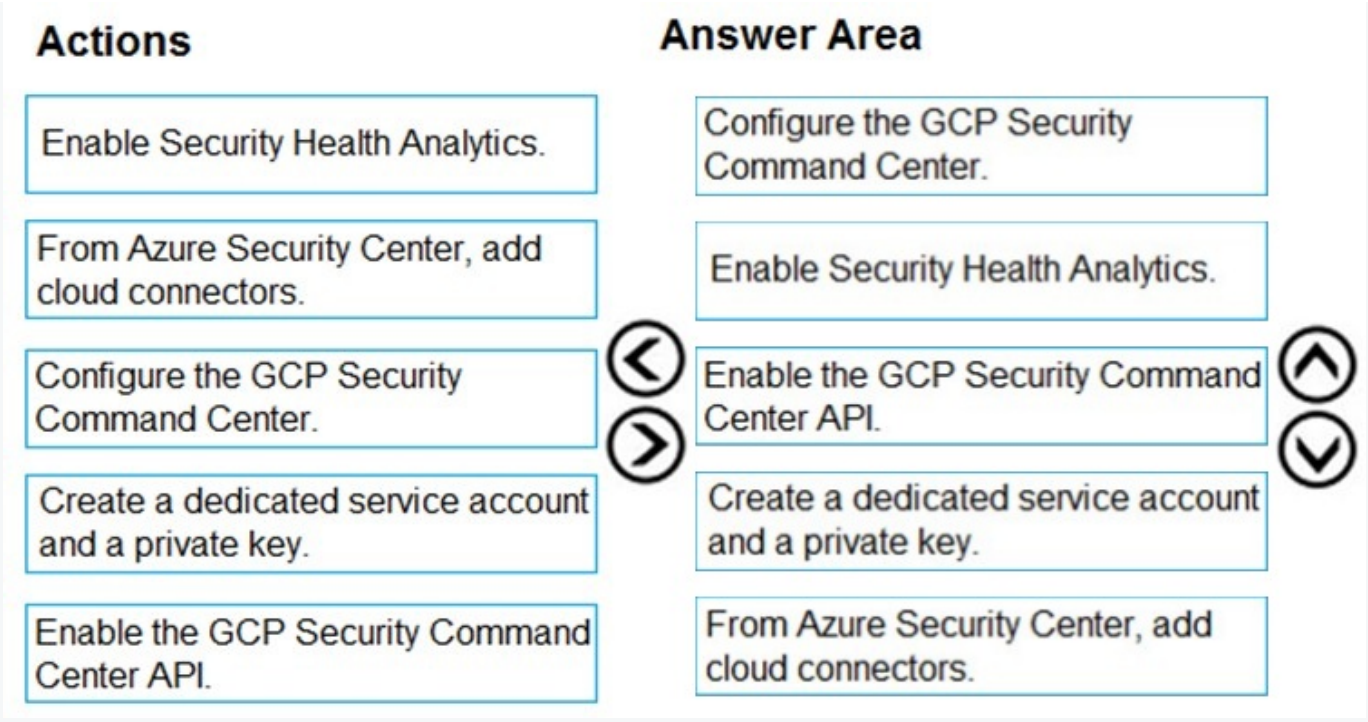
Reference:
https://docs.microsoft.com/en-us/azure/security-center/security-center-provide-security-contact-details

Question: 68 CertyIQ

DRAG DROP -
You have resources in Azure and Google cloud.
You need to ingest Google Cloud Platform (GCP) data into Azure Defender.
In which order should you perform the actions? To answer, move all actions from the list of actions to the answer area and arrange them in the correct order.
Select and Place:



Answer:



Explanation:

Reference:
https://docs.microsoft.com/en-us/azure/security-center/quickstart-onboard-gcp

Question: 69 CertyIQ

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You use Azure Security Center.
You receive a security alert in Security Center.
You need to view recommendations to resolve the alert in Security Center.
Solution: From Regulatory compliance, you download the report.
Does this meet the goal?

A.Yes
B.No

Answer: B

Explanation:

Based on the link, once you are on the full details page of one of the alerts,1. Click on “Next: Take Action”2. Select: “Prevent future attacks” - as this provides security recommendations

Reference:

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

Question: 70 CertyIQ

Note: This question is part of a series of questions that present the same scenario. Each question in the series

contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You use Azure Security Center.
You receive a security alert in Security Center.
You need to view recommendations to resolve the alert in Security Center.
Solution: From Security alerts, you select the alert, select Take Action, and then expand the Mitigate the threat section.
Does this meet the goal?

A.Yes

B.No

Answer: A

Explanation:

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

Question: 71 CertyIQ

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

Explanation:

Reference:
https://docs.microsoft.com/en-us/azure/security-center/continuous-export?tabs=azure-portal

Question: 72 CertyIQ

You are responsible for responding to Azure Defender for Key Vault alerts.
During an investigation of an alert, you discover unauthorized attempts to access a key vault from a Tor exit node.
What should you configure to mitigate the threat?

A.Key Vault firewalls and virtual networks

B.Azure Active Directory (Azure AD) permissions

C.role-based access control (RBAC) for the key vault

D.the access policy settings of the key vault

Answer: A

Explanation:

Answer is correct. To be able to prevent unauthorized access to the key vault through suspicious IPs you have to change the networking settings under the key vault resource

Reference:

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

Question: 73 CertyIQ

HOTSPOT -
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.
Hot Area:

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": "                    /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

Explanation:

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

Question: 74 CertyIQ

You have an Azure subscription that contains a Log Analytics workspace.
You need to enable just-in-time (JIT) VM access and network detections for Azure resources.
Where should you enable Azure Defender?

A.at the subscription level

B.at the workspace level

C.at the resource level

Answer: A

Explanation:

In Azure, -> Defender for Cloud -> Environment Settings -> select the subscription to enable all.

Reference:

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

Question: 75 CertyIQ

You use Azure Defender.
You have an Azure Storage account that contains sensitive information.
You need to run a PowerShell script if someone accesses the storage account from a suspicious IP address.
Which two actions should you perform? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

A.From Azure Security Center, enable workflow automation.

B.Create an Azure logic app that has a manual trigger.

C.Create an Azure logic app that has an Azure Security Center alert trigger.

D.Create an Azure logic app that has an HTTP trigger.

E.From Azure Active Directory (Azure AD), add an app registration.

Answer: AC

Explanation:

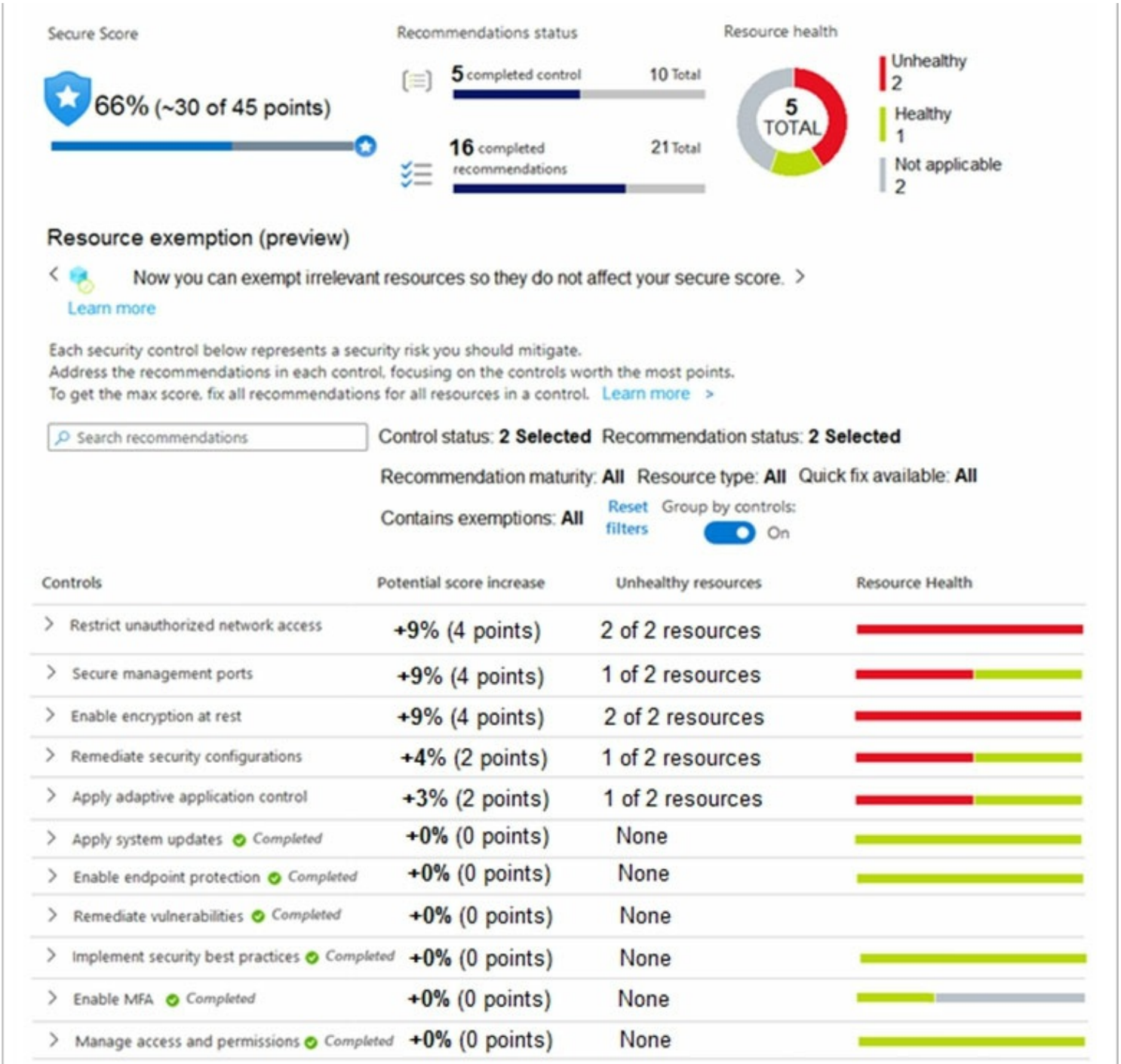
AC looks ok.Seems correct you want a security trigger for the login and you use this trigger to start the automation workflow with the powershellscript

Reference:

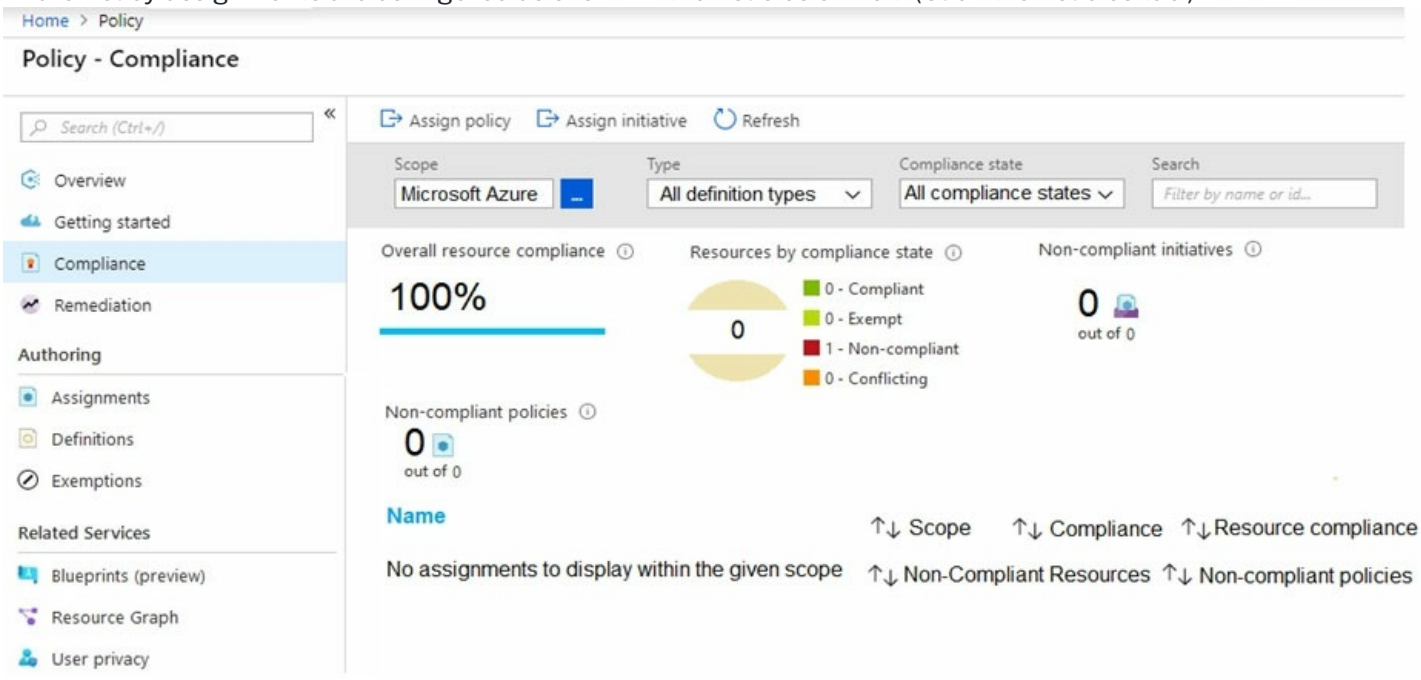
https://docs.microsoft.com/en-us/azure/storage/common/azure-defender-storage-configure?tabs=azure-security-center https://docs.microsoft.com/en-us/azure/security-center/workflow-automation

Question: 76 CertyIQ

HOTSPOT -
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.
Hot Area:

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:

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

Question: 77 CertyIQ

DRAG DROP -
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.
Select and Place:

Actions

- From Device Inventory, search for the CVE.
- Open the Threat Protection report.
- From Threat & Vulnerability Management, select **Weaknesses**, and search for the CVE.
- From Advanced hunting, search for `CveId` in the `DeviceTvmSoftwareInventoryVulnerabilitites` table.
- Create the remediation request.
- Select **Security recommendations**.

Answer Area

Answer:

Actions

- From Device Inventory, search for the CVE.
- Open the Threat Protection report.
- From Threat & Vulnerability Management, select **Weaknesses**, and search for the CVE.
- From Advanced hunting, search for `CveId` in the `DeviceTvmSoftwareInventoryVulnerabilitites` table.
- Create the remediation request.
- Select **Security recommendations**.

Answer Area

1. From Threat & Vulnerability Management, select **Weaknesses**, and search for the CVE.
2. Select **Security recommendations**.
3. Create the remediation request.

Explanation:

Reference:
https://techcommunity.microsoft.com/t5/core-infrastructure-and-security/microsoft-defender-atp-remediate-apps-using-mem/ba-p/1599271

Question: 78

CertyIQ

You use Azure Security Center.
You receive a security alert in Security Center.
You need to view recommendations to resolve the alert in Security Center.

What should you do?

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

Answer: B

Explanation:

it is B. With the 'Mitigate the threat' action you receive recommendations to mitigate this threat. The 'Prevent future attacks' action provides security recommendations to help reduce the attack surface, increase security posture, and thus prevent future attacks.

Reference:

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

Question: 79 CertyIQ

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: C

Explanation:

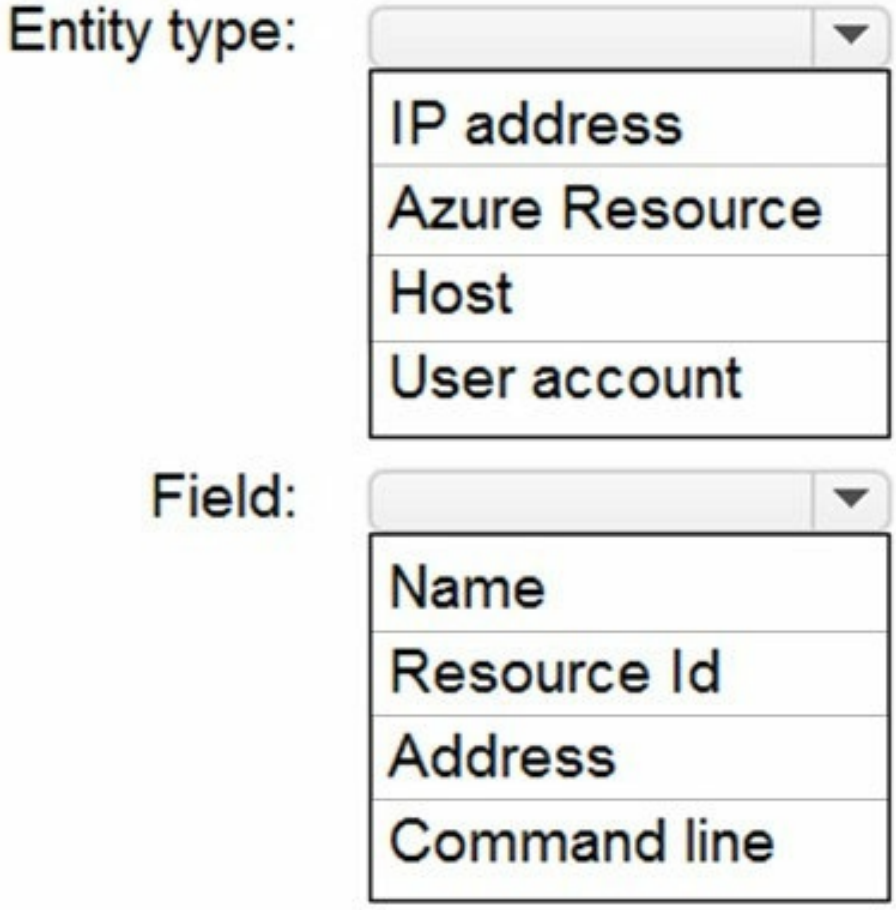
C is correct. You need to change the filter as it's only showing "Active, In Progress"

Azure Security Center, you should modify the filter for the Security alerts page. The suppression rule is designed to prevent alerts from being generated, so it should not be affecting the ability to view alerts. To modify the filter for the Security alerts

Question: 80 CertyIQ

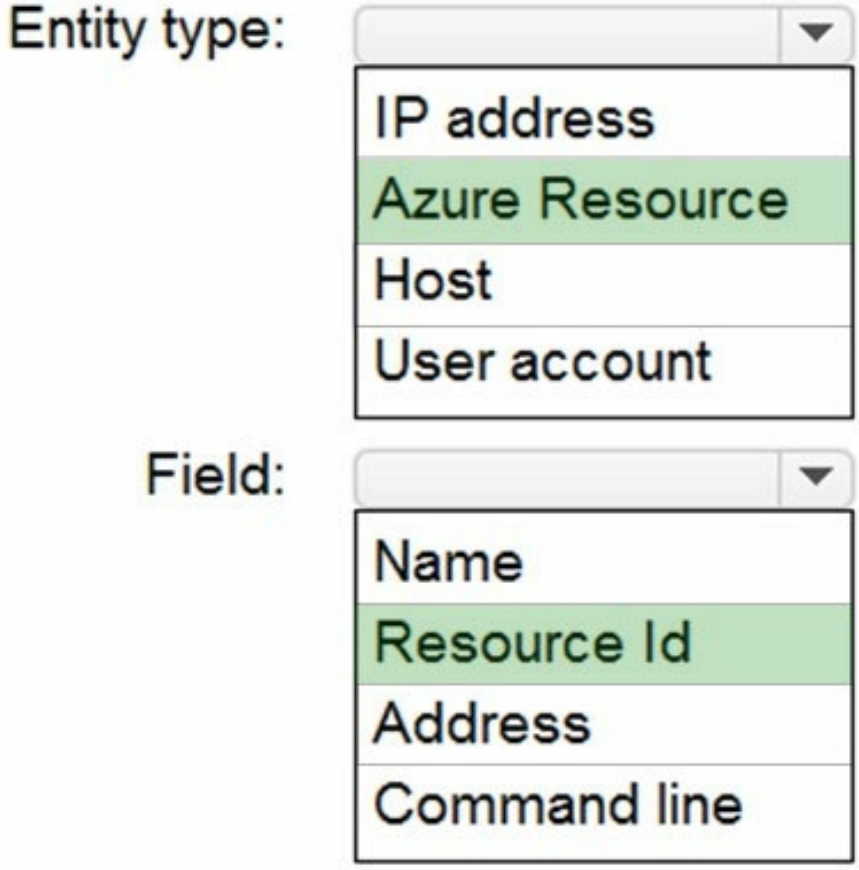
HOTSPOT -
You have an Azure Storage account that will be accessed by multiple Azure Function apps during the development of an application.
You need to hide Azure Defender alerts for the storage account.
Which entity type and field should you use in a suppression rule? To answer, select the appropriate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

Answer Area



Answer:

Answer Area



Explanation:

Entity Type = Azure Resource (Azure Storage is a Resource)Field = Resource ID (All Azure resources have an ID)Correct.

Reference:

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

Question: 81 CertyIQ

You create an Azure subscription.
You enable Azure Defender for the subscription.
You need to use Azure Defender to protect on-premises computers.
What should you do on the on-premises computers?

A.Install the Log Analytics agent.

B.Install the Dependency agent.

C.Configure the Hybrid Runbook Worker role.

D.Install the Connected Machine agent.

Answer: A

Explanation:
Security Center collects data from your Azure virtual machines (VMs), virtual machine scale sets, IaaS containers, and non-Azure (including on-premises) machines to monitor for security vulnerabilities and threats.
Data is collected using:
✑ The Log Analytics agent, which reads various security-related configurations and event logs from the machine and copies the data to your workspace for analysis. Examples of such data are: operating system type and version, operating system logs (Windows event logs), running processes, machine name, IP addresses, and logged in user.
✑ Security extensions, such as the Azure Policy Add-on for Kubernetes, which can also provide data to Security Center regarding specialized resource types.

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

Question: 82 CertyIQ

A security administrator receives email alerts from Azure Defender for activities such as potential malware uploaded to a storage account and potential successful brute force attacks.
The security administrator does NOT receive email alerts for activities such as antimalware action failed and suspicious network activity. The alerts appear in
Azure Security Center.
You need to ensure that the security administrator receives email alerts for all the activities.
What should you configure in the Security Center settings?

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

Answer: A

Explanation:

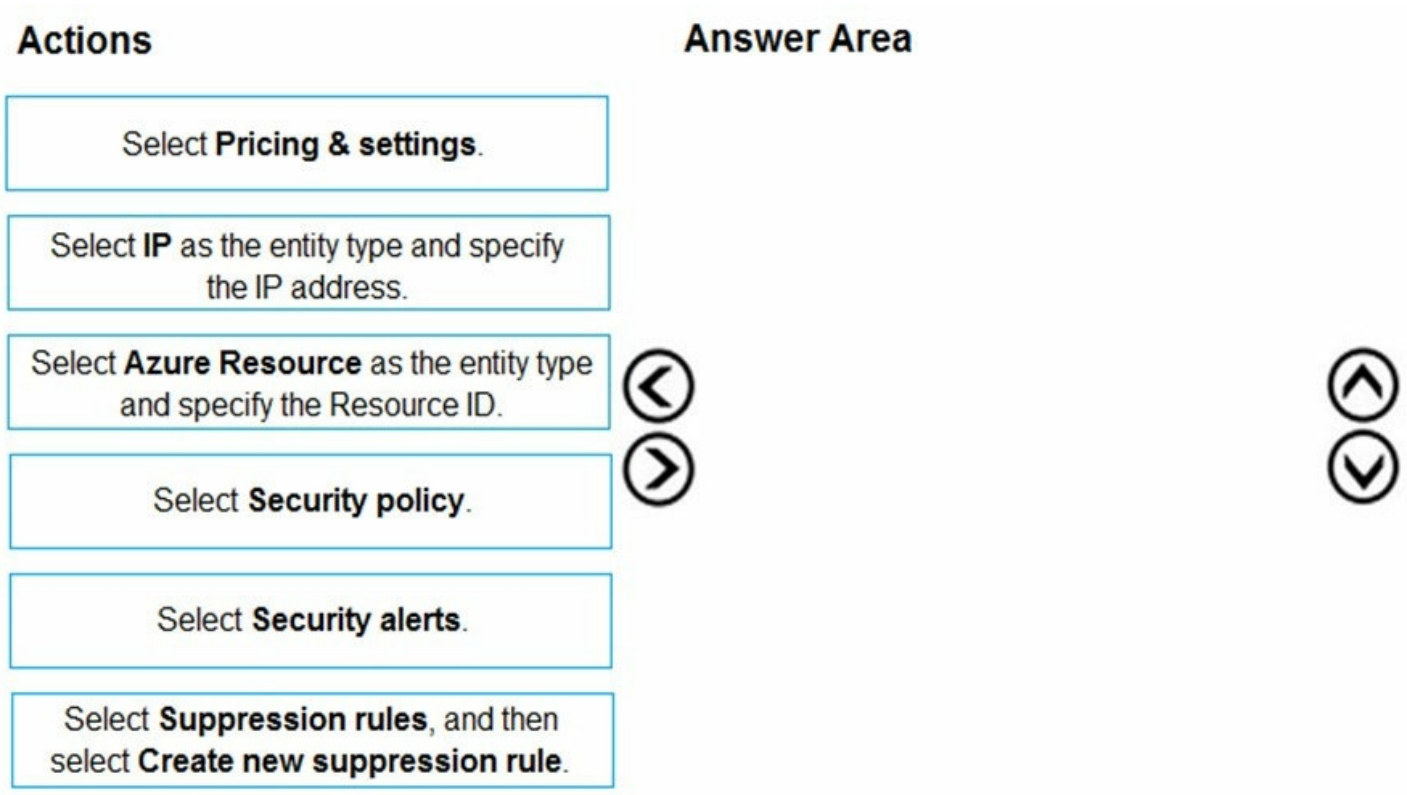
Email notifications are free; for security alerts, enable the enhanced security plans

Reference:

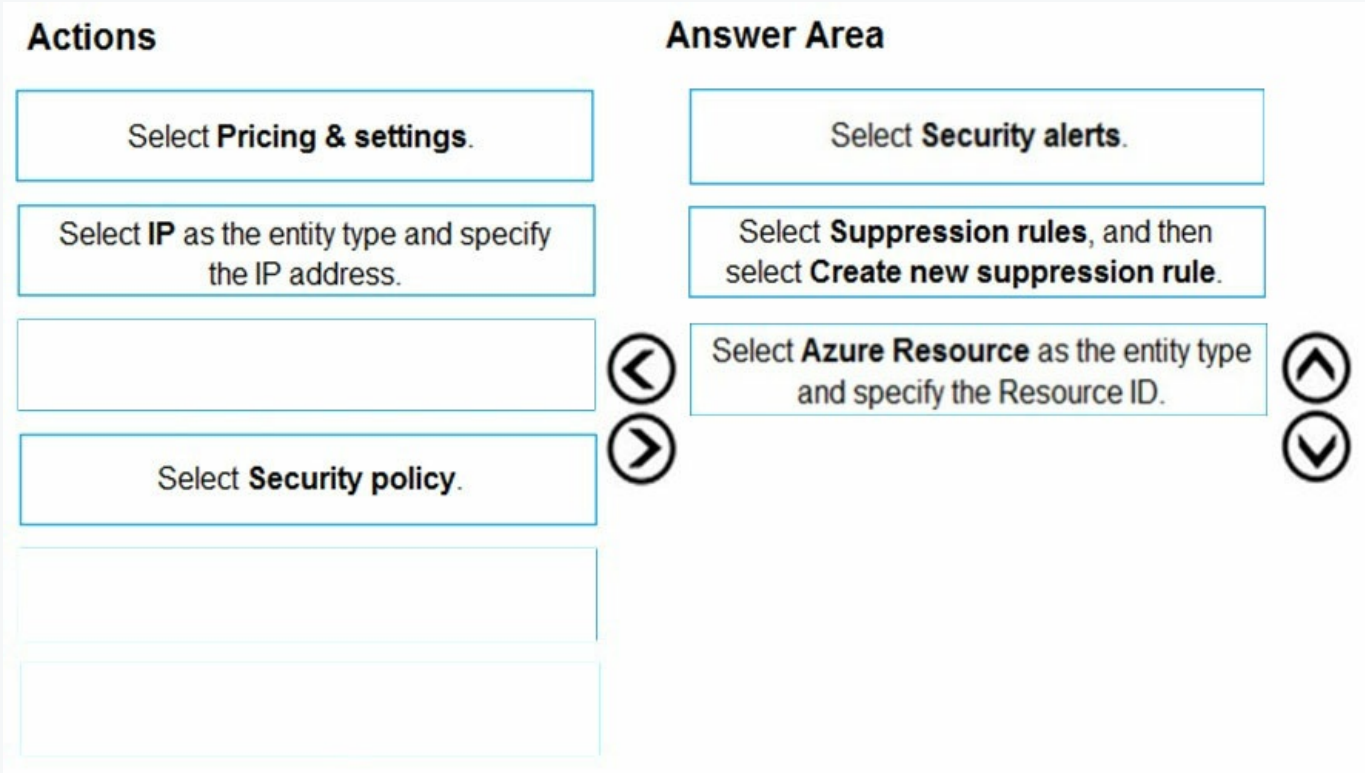
https://techcommunity.microsoft.com/t5/microsoft-365-defender/get-email-notifications-on-new-incidents-from-microsoft-365/ba-p/2012518

Question: 83 CertyIQ

DRAG DROP -
You have an Azure Functions app that generates thousands of alerts in Azure Security Center each day for normal activity.
You need to hide the alerts automatically in Security Center.
Which three actions should you perform in sequence in Security Center? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.
Select and Place:



Answer:



Explanation:

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

Question: 84

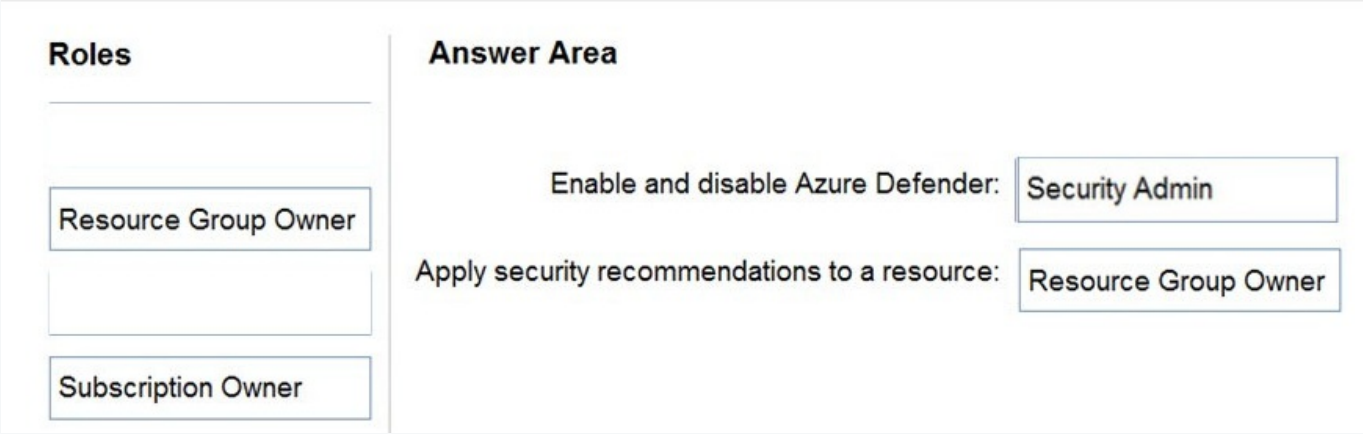
CertyIQ

DRAG DROP -
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.
Select and Place:

Answer:



Explanation:

Box1 : Security AdminBox2 : Resource Group Owner

https://learn.microsoft.com/en-us/azure/defender-for-cloud/permissions#roles-and-allowed-actions

Question: 85

CertyIQ

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

Answer Area

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:

Answer Area

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

Explanation:

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

Question: 86 CertyIQ

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

A.From Azure Security Center, add a workflow automation.

B.On VM1, run the Get-MPThreatCatalog cmdlet.

C.On VM1 trigger a PowerShell alert.

D.From Azure Security Center, export the alerts to a Log Analytics workspace.

Answer: C

Explanation:

C. trigger a PowerShell alert on VM1 to create a custom alert suppression rule that will suppress false positive alerts for suspicious use of PowerShell on VM1. After triggering the alert, you can use the information

provided in the alert to create a suppression rule that will prevent similar alerts from being generated in the future.

Reference:

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

Question: 87 CertyIQ

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: A

Explanation:

A. Yes, this meets the goal. By enabling Azure Arc and onboarding the Linux virtual machines to Azure Arc, you can monitor them using Azure Defender

You need both Azure Arc to see the VM and the LAW agent.Now, the agent can be automatically deployed after Azure Arc is deployed. Answer should be A) Yes.

Question: 88 CertyIQ

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You have Linux virtual machines on Amazon Web Services (AWS).
You deploy Azure Defender and enable auto-provisioning.
You need to monitor the virtual machines by using Azure Defender.
Solution: You manually install the Log Analytics agent on the virtual machines.
Does this meet the goal?

A.Yes
B.No

Answer: B

Explanation:

B is Correct. The full correct answer should be "You enable Azure Arc to onboard the virtual machines to Azure Arc, then you enable auto-provisioning to install the Log Analytics agent on the virtual machines

automatically."

Reference:

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

Question: 89 CertyIQ

You have five on-premises Linux servers.
You have an Azure subscription that uses Microsoft Defender for Cloud.
You need to use Defender for Cloud to protect the Linux servers.
What should you install on the servers first?

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

Answer: C

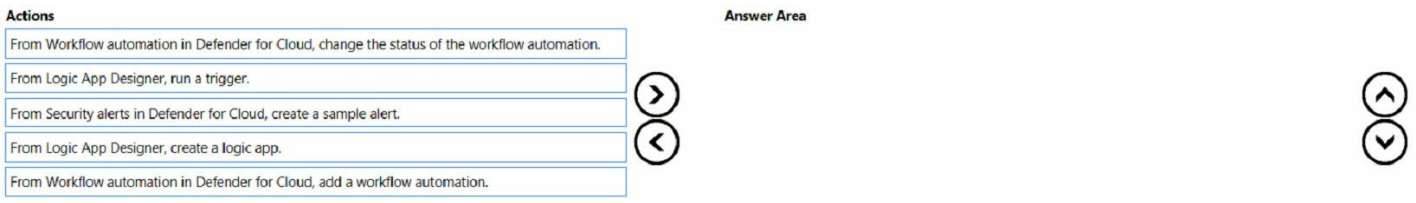
Explanation:

I will go with C first, then LA-Agent:https://learn.microsoft.com/en-us/azure/defender-for-cloud/plan-defender-for-servers-agents

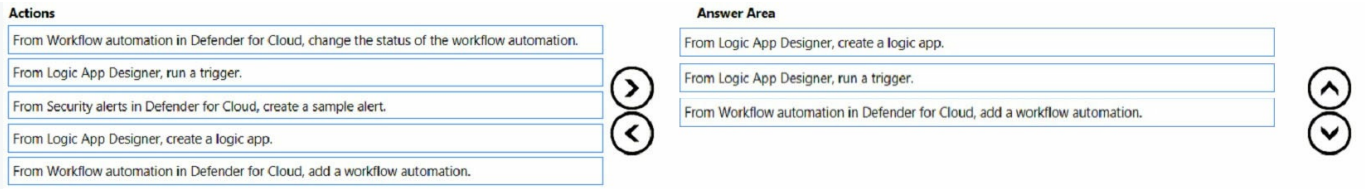
The Azure Connected Machine agent is required to connect the on-premises Linux servers to the Azure subscription and integrate them with Microsoft Defender for Cloud. The agent enables communication between the servers and the Defender for Cloud service, allowing security events and data to be collected and analyzed.Once the Azure Connected Machine agent is installed, you can then install the Log Analytics agent to collect security data from the servers and send it to the Log Analytics workspace in Azure. This will allow you to use Defender for Cloud to monitor the security of your Linux servers, identify threats, and respond to security incidents.

Question: 90 CertyIQ

DRAG DROP -
You have an Azure subscription. The subscription contains 10 virtual machines that are onboarded to Microsoft Defender for Cloud.
You need to ensure that when Defender for Cloud detects digital currency mining behavior on a virtual machine, you receive an email notification. The solution must generate a test email.
Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.
Select and Place:



Answer:



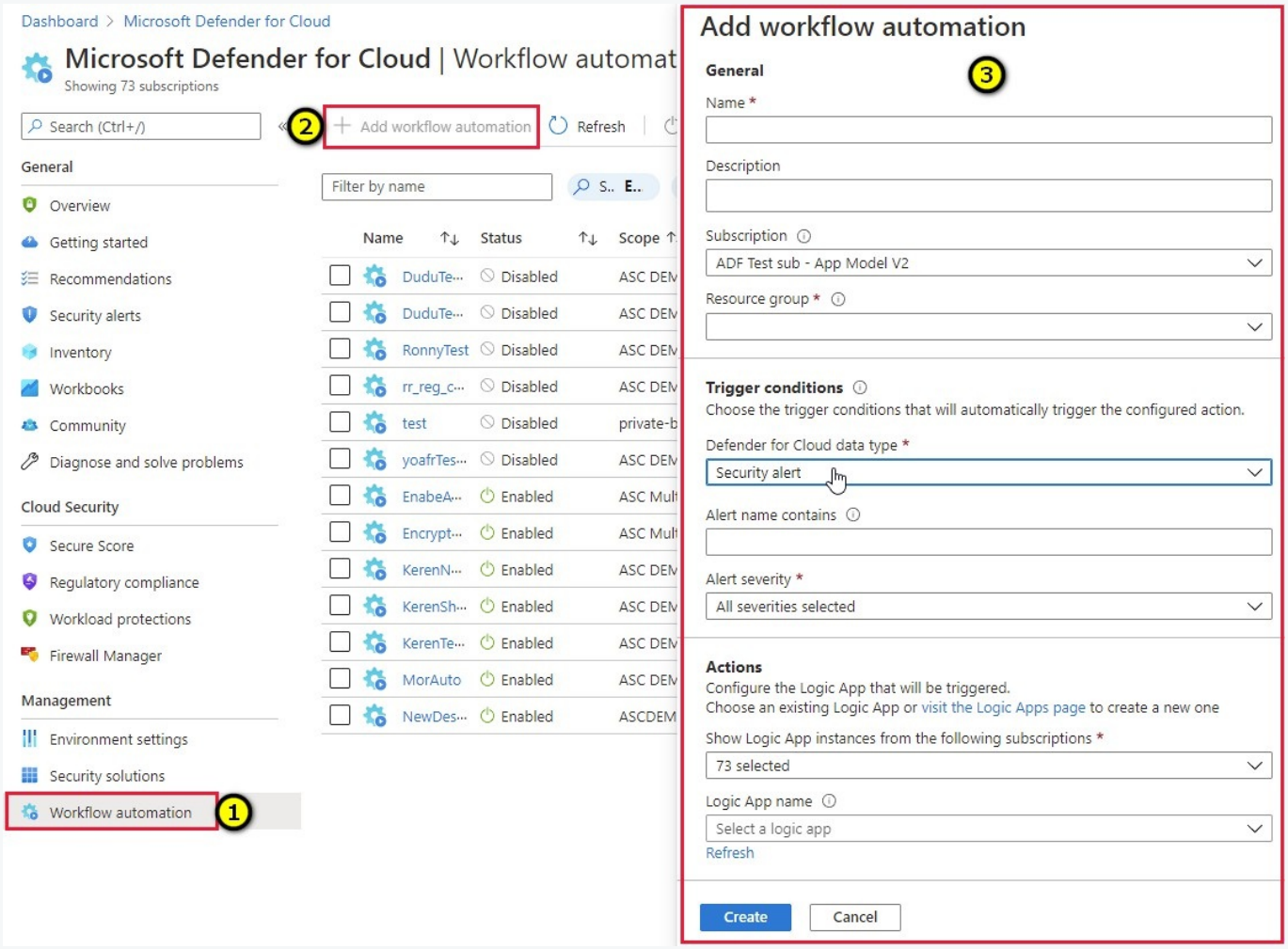
Explanation:

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

Question: 91 CertyIQ

DRAG DROP
-

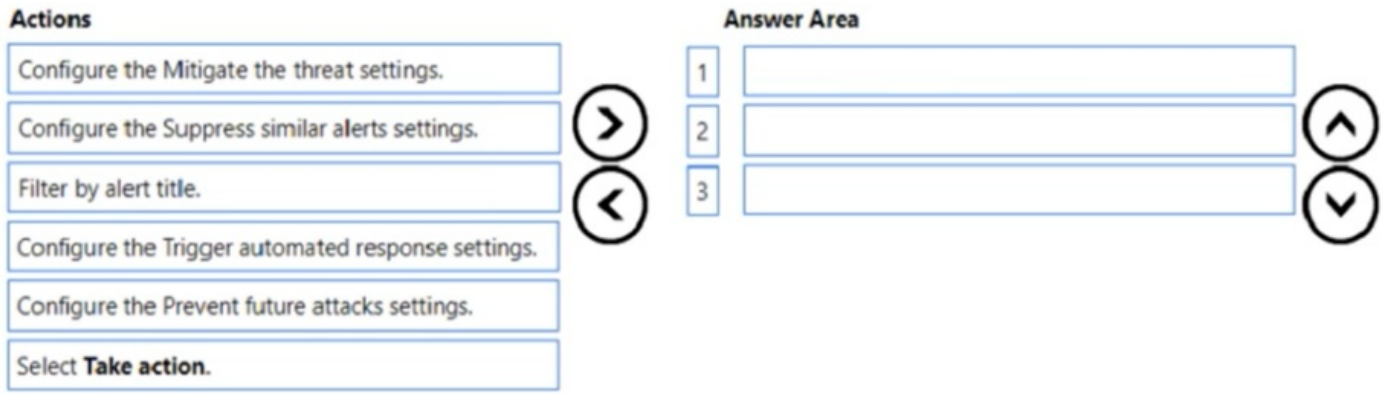
You have a Microsoft subscription that has Microsoft Defender for Cloud enabled.

You configure the Azure logic apps shown in the following table.

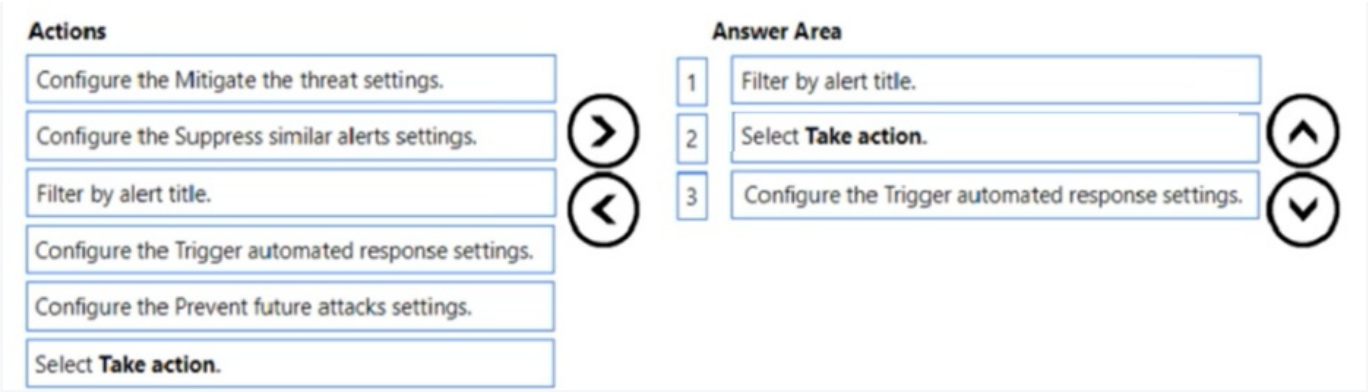
Name	Trigger	Action
LogicApp1	When a Defender for Cloud recommendation is created or triggered	Send an email
LogicApp2	When a Defender for Cloud alert is created or triggered	Send an email

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:

Filter by Alert Title TakeAction Trigger Automated Response

Question: 92 CertyIQ

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

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

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

What should you install first on Server1?

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

Answer: C

Explanation:

Azure Arc for servers installed on your EC2 instanceshttps://learn.microsoft.com/en-us/azure/defender-for-cloud/quickstart-onboard-aws?pivots=env-settings

In the following article, it is clearly indicated that installing Azure Arc is a prerequisite which is the first thing to dohttps://learn.microsoft.com/en-us/azure/defender-for-cloud/quickstart-onboard-aws?pivots=env-settings

Question: 93 CertyIQ

You have an Azure subscription that uses Microsoft Defender for Cloud and contains a storage account named storage1.

You receive an alert that there was an unusually high volume of delete operations on the blobs in storage1.

You need to identify which blobs were deleted.

What should you review?

A.the activity logs of storage1

B.the Azure Storage Analytics logs

C.the alert details

D.the related entities of the alert

Answer: B

Explanation:

Seems like the answer is actually correct."Azure Storage Analytics performs logging and provides metrics data for a storage account. You can use this data to trace requests, analyze usage trends, and diagnose issues with your storage account."

Question: 94 CertyIQ

You have an Azure subscription that uses Microsoft Defender 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

Explanation:

https://learn.microsoft.com/en-us/azure/defender-for-cloud/alerts-overview#how-are-alerts-classified

Question: 95 CertyIQ

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.Description

B.Intent

C.ExtendedProperies

D.Entities

Answer: B

Explanation:

B. Intenthttps://learn.microsoft.com/en-us/rest/api/defenderforcloud/alerts/list?tabs=HTTP#intent

The "Intent" key is part of the JSON format used by Microsoft Defender for Cloud to transmit security alert data to third-party security information and event management (SIEM) solutions. The "Intent" key provides information on the type of attack or tactic that the alert is related to, and can be used to identify alerts that are specifically related to the Privilege Escalation tactic.

Question: 96

CertyIQ

DRAG DROP
-

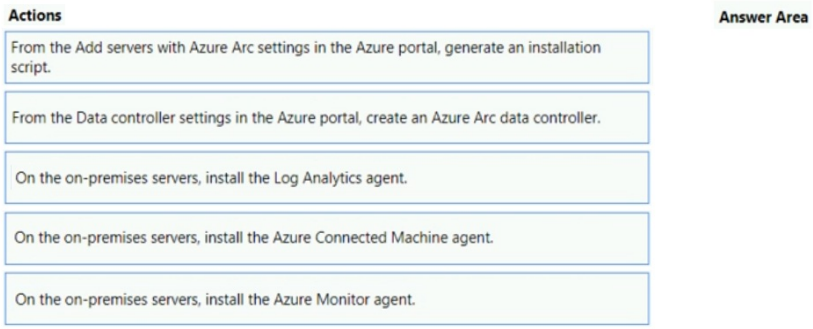
You have 50 on-premises servers.

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.

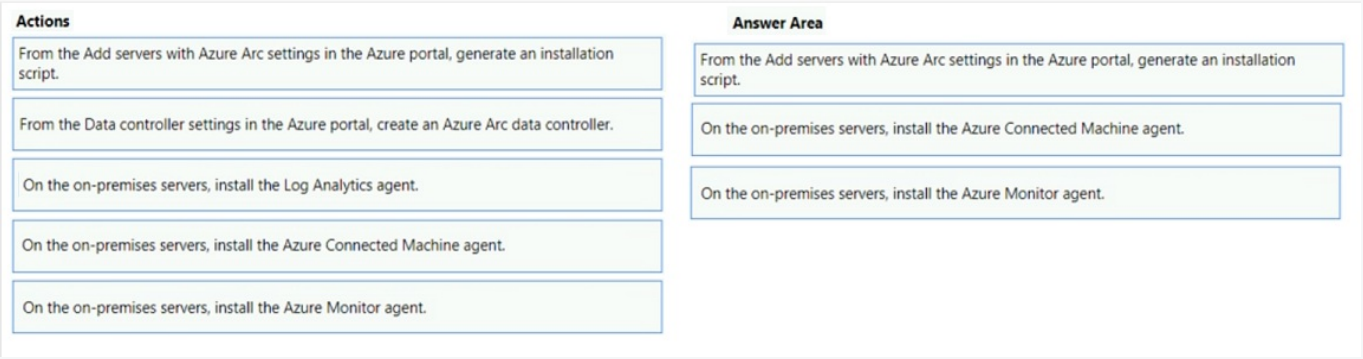
You need to configure Defender for Cloud to support the on-premises servers. The solution must meet the following requirements:

•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.



Answer:



Question: 97

CertyIQ

HOTSPOT
-

You have an Azure subscription that uses Microsoft Defender for Cloud and contains an Azure logic app named app1.

You need to ensure that app1 launches when a specific Defender for Cloud security alert is generated.
How should you complete the Azure Resource Manager (ARM) template? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

```
"resources": [
    {
      "type": [                                                    ▼
                Microsoft.Automation/automationAccounts",
                "Microsoft.Logic/workflows"',
                "Microsoft.Security/automations",
      "apiVersion": "2019-01-01-preview",
      "name": "[parameters('name')]",
      "location": "[resourceGroup().location]",
      "properties": {
        "description": "[format(variables('description'),'{0}', parameters('subscriptionId'))]",
        "isEnabled": true,
        "actions": [
          { "actionType": "LogicApp",
            "logicAppResourceId": "[resourceId('Microsoft.Logic/workflows', parameters('app1'))]",
            "uri": "[listCallbackURL(resourceId(parameters('subscriptionId'),parameters('resourceGroupName'),
                    'Microsoft.Logic/workflows/ [          ▼ ]
                                                    actions
                                                    contents
                                                    triggers
                    parameters('app1'),'manual'), '2019-05-01').value]"
          }
        ],
```

Answer:

Question: 98 CertyIQ

HOTSPOT
-

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

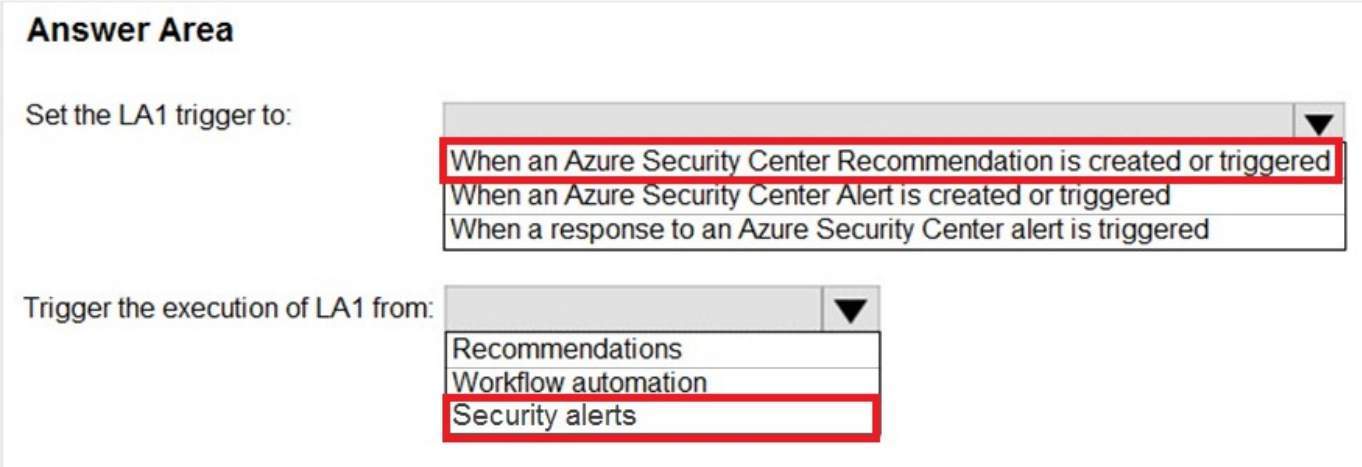
Set the LA1 trigger to:

- 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:



Explanation:

When a Defender for Cloud Recommendation is created or triggeredandSecurity alertsRegulatory Compliance Standards is based on pre-defined compliance standards and, while they can provide remediation to security risks, I think Security alerts better answers the question and offers the ability to customize.

Question: 99 CertyIQ

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

You have a virtual machine that runs Windows 10 and has the Log Analytics agent installed.

You need to simulate an attack on the virtual machine that will generate an alert.

What should you do first?

A.Run the Log Analytics Troubleshooting Tool.
B.Copy and executable and rename the file as ASC_AlertTest_662jfi039N.exe.
C.Modify the settings of the Microsoft Monitoring Agent.
D.Run the MMASetup executable and specify the –foo argument.

Answer: B

Explanation:

you can use the built-in ASC AlertTest tool.Here's what you should do first:Connect to the virtual

machine.Open a web browser and navigate to the Microsoft Defender Security Center portal.Click on the "Settings" tab in the left-hand menu.Click on the "Advanced features" link to expand the advanced features section.In the "Advanced features" section, click on the "Download" link next to the "ASC AlertTest" tool.Download and save the ASC AlertTest tool to the virtual machine.Double-click the downloaded ASC AlertTest executable to run it.Follow the on-screen prompts to generate an alert in Microsoft Defender for Cloud. You may need to specify the IP address or hostname of the virtual machine, as well as a description and category for the simulated attack.

Question: 100 CertyIQ

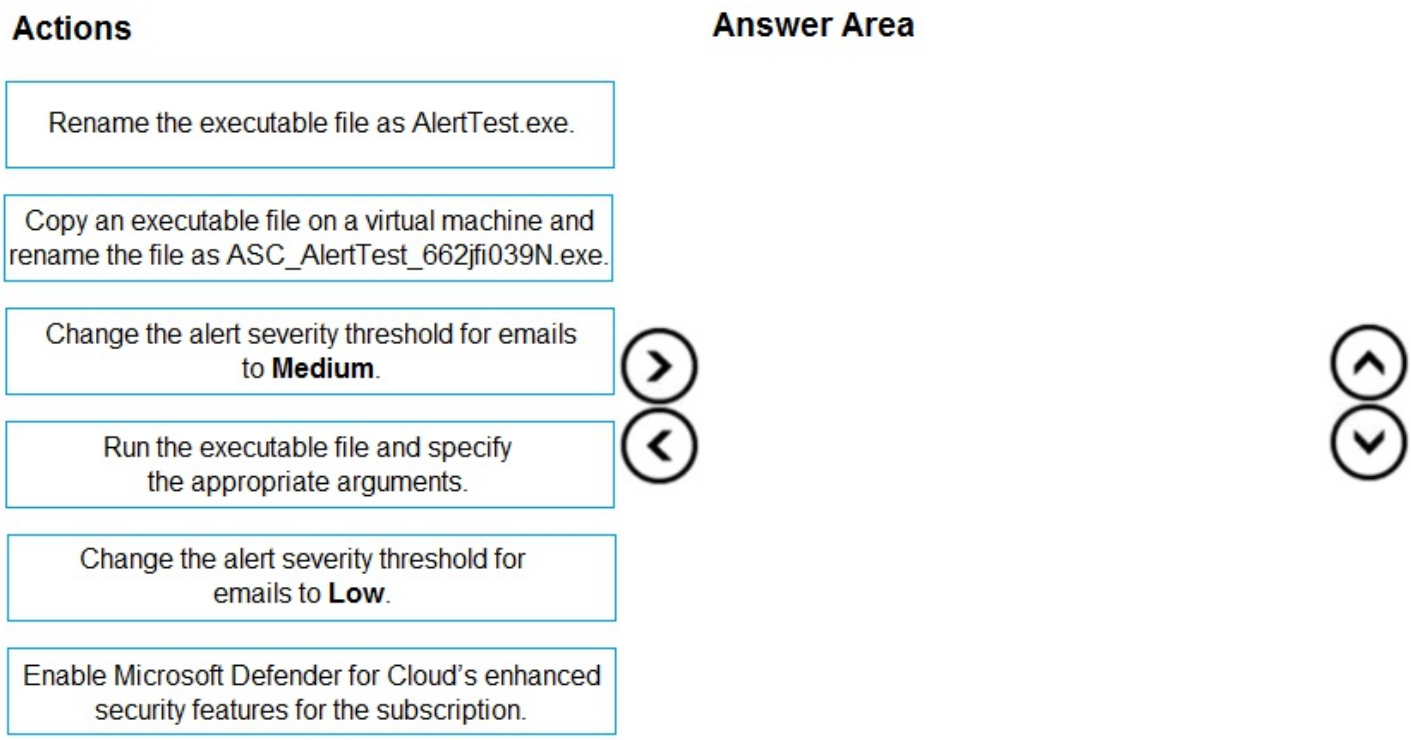
DRAG DROP
-

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

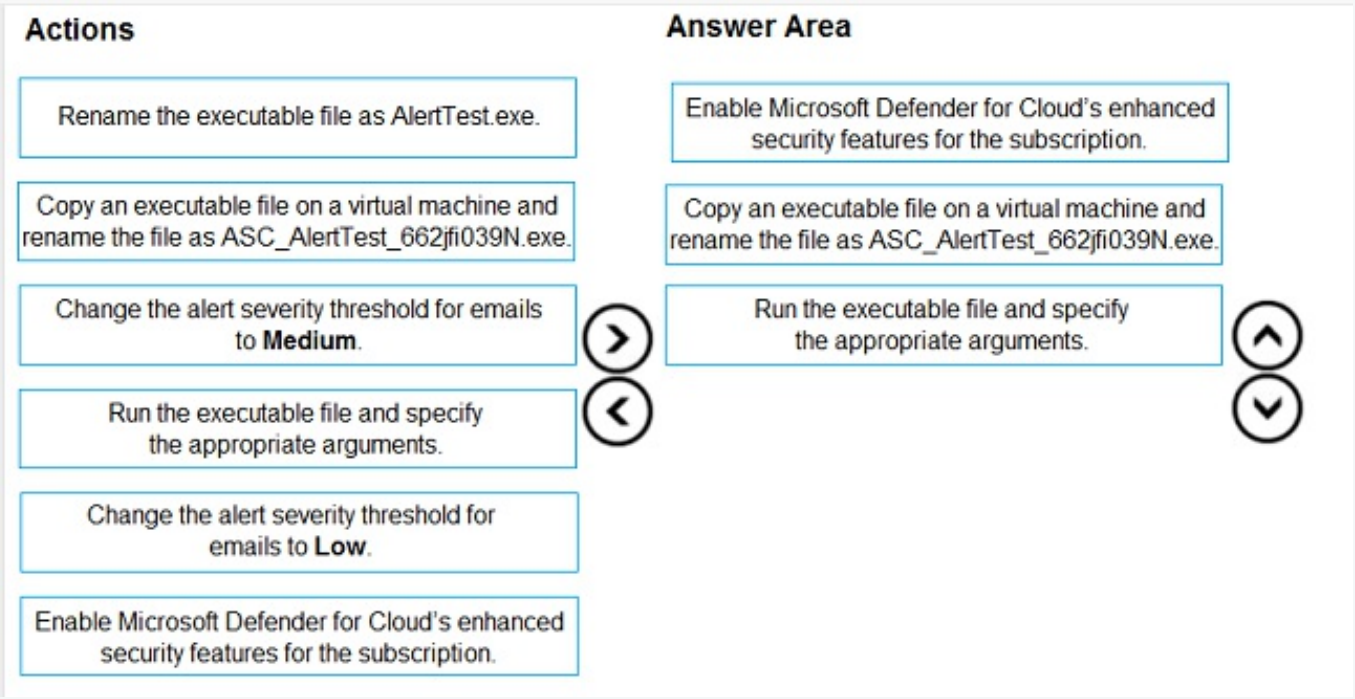
You need to validate that Microsoft Defender for Cloud will trigger an alert when a malicious file is present on an Azure virtual machine running Windows Server.

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

NOTE: More than one order of answer choices is correct. You will receive credit for any of the correct orders you select.



Answer:



Explanation:

1. Enable Microsoft Defender for cloud enhanced 2. Copy an executable file... 3. Run the executable

Question: 101 CertyIQ

You have an Azure subscription that uses Microsoft Defender for Cloud and contains 100 virtual machines that run Windows Server.

You need to configure Defender for Cloud to collect event data from the virtual machines. The solution must minimize administrative effort and costs.

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

NOTE: Each correct selection is worth one point.

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

Answer: AE

Explanation:

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

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

Question: 102 CertyIQ

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

You need to ensure that User1 can modify Microsoft Defender for Cloud security policies. The solution must use the principle of least privilege.

Which role should you assign to User1?

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

Answer: B

Explanation:

Security reader: Has rights to view Defender for Cloud items such as recommendations, alerts, policy, and health. Can't make changes.Security admin: Has the same view rights as security reader. Can also update the security policy and dismiss alerts.

Question: 103 CertyIQ

You have an Azure subscription that contains a user named User1.

User1 is assigned an Azure Active Directory Premium Plan 2 license.

You need to identify whether the identity of User1 was compromised during the last 90 days.

What should you use?

A.the risk detections report
B.the risky users report
C.Identity Secure Score recommendations
D.the risky sign-ins report

Answer: A

Explanation:

The risky users view shows a user's risk standing based on all past sign-ins.The risky sign-ins view shows at-risk signs in the last 30 days.The risk detections view shows risk detections made in the last 90 days.

Question: 104 CertyIQ

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

You have an Amazon Web Services (AWS) account that contains an Amazon Elastic Compute Cloud (EC2) instance named EC2-1.

You need to onboard EC2-1 to Defender for Cloud.

What should you install on EC2-1?

A.the Log Analytics agent
B.the Azure Connected Machine agent
C.the unified Microsoft Defender for Endpoint solution package

D.Microsoft Monitoring Agent

Answer: B

Explanation:

Answer is BPlease check the video below at 04:15 As you can see, server is already onboarded using Azure Arc agent and there is a recommendation to also install Log Analytics agent.So FIRST you need to install Arc agenthttps://www.youtube.com/watch?v=uogTZe6p7nc

Question: 105 CertyIQ

You have an Azure subscription that uses Microsoft Defender for Cloud and contains a resource group named RG1. RG1 contains 20 virtual machines that run Windows Server 2019.

You need to configure just-in-time (JIT) access for the virtual machines in RG1. The solution must meet the following requirements:

•Limit the maximum request time to two hours.
•Limit protocols access to Remote Desktop Protocol (RDP) only.
•Minimize administrative effort.

What should you use?

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

Answer: C

Explanation:

To meet the given requirements, you should use Azure Bastion to configure just-in-time (JIT) access for the virtual machines in RG1.Azure Bastion provides secure and seamless RDP and SSH access to virtual machines over a web browser and eliminates the need for a public IP address. It simplifies the process of connecting to virtual machines by allowing users to connect directly to virtual machines through the Azure portal.To enable JIT access with Azure Bastion, you can create a JIT policy that defines the rules for access, including limiting access to specific protocols like RDP and setting the maximum request time to two hours. This can be done using the Azure portal or Azure CLI, and once the policy is created, Azure Bastion will automatically enforce the access rules when users try to connect to the virtual machines.

Question: 106 CertyIQ

HOTSPOT
-

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

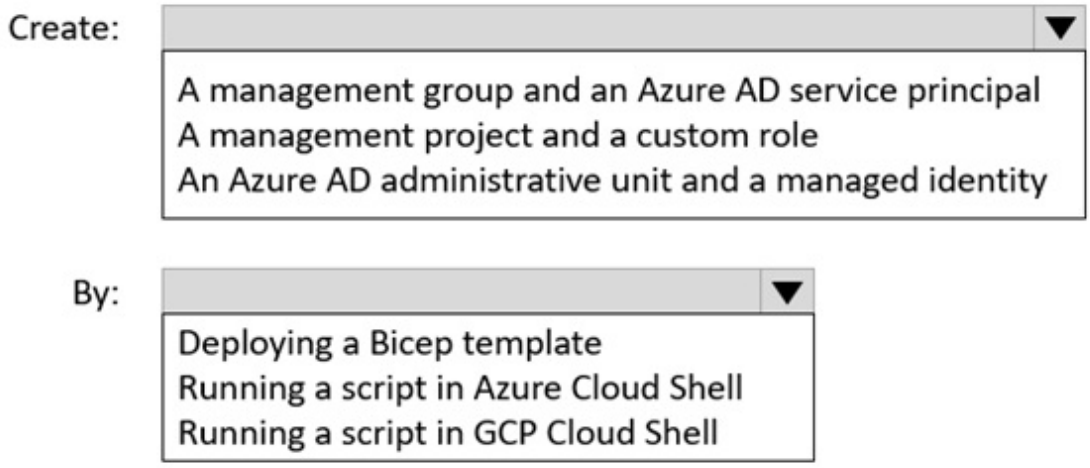
You create a Google Cloud Platform (GCP) organization named GCP1.

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.

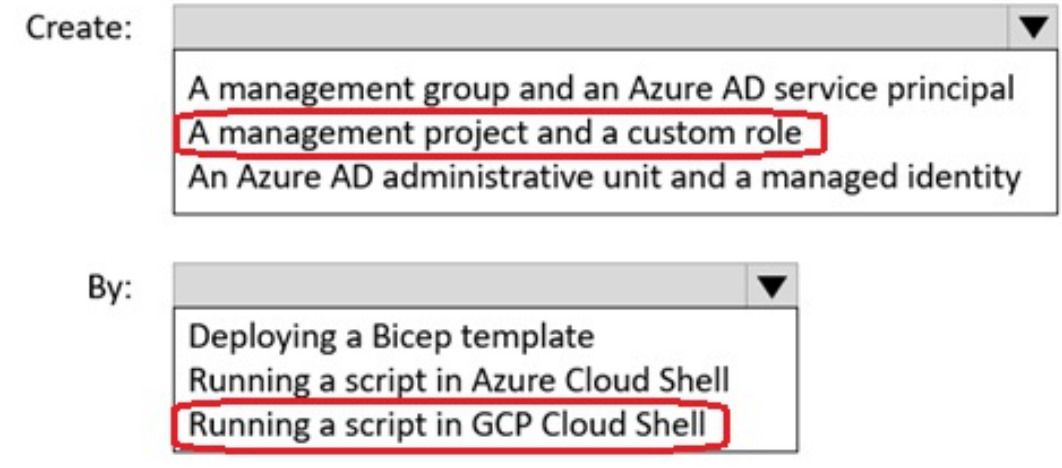
NOTE: Each correct selection is worth one point.

Answer Area



Answer:

Answer Area



Question: 107 CertyIQ

You have an Azure subscription that contains a virtual machine named VM1 and uses Microsoft Defender for Cloud.

Microsoft Defender for Cloud has automatic provisioning configured to use Azure Monitor Agent.

You need to create a custom alert suppression rule that will suppress false positive alerts for suspicious use of PowerShell on VM1.

What should you do first?

A.From Microsoft Defender for Cloud, export the alerts to a Log Analytics workspace.

B.From Microsoft Defender for Cloud, add a workflow automation.

C.On VM1, trigger a PowerShell alert.

D.On VM1, run the Get-MPThreatCatalog cmdlet.

Answer: C

Explanation:

On VM1, trigger a PowerShell alert.

Question: 108 CertyIQ

HOTSPOT
-

Case study
-

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 conta`in 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
-

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:

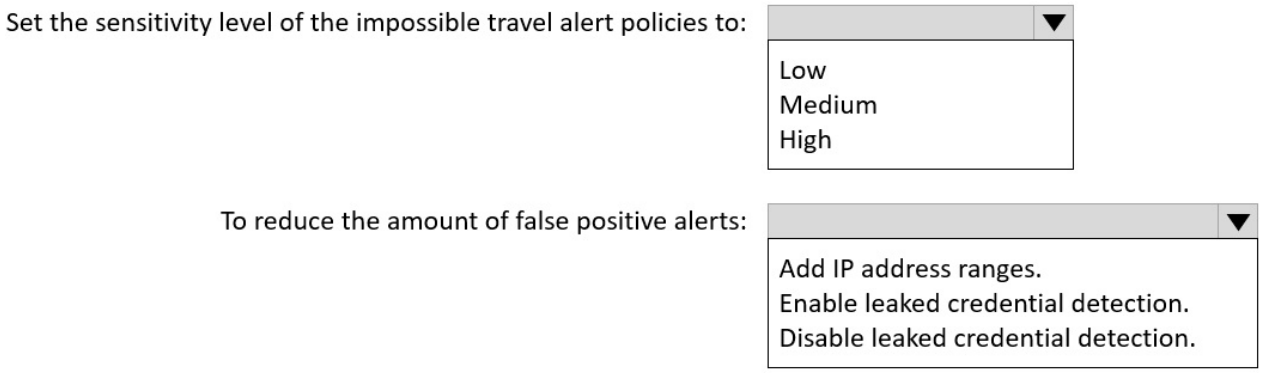
•Query for NXDOMAIN DNS requests from the last seven days by using built-in Advanced Security Information Model (ASIM) unifying parsers.
•From AWS EC2 instances, collect Windows Security event log entries that include local group membership changes.
•Identify anomalous activities of Azure AD users by 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 meet the Microsoft Defender for Cloud Apps requirements.

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

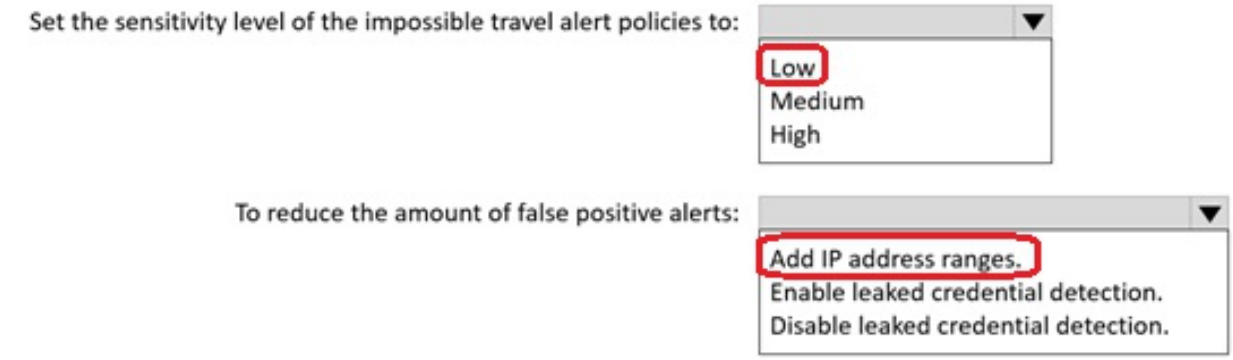
NOTE: Each correct selection is worth one point.

Answer Area



Answer:

Answer Area



Question: 109

CertyIQ

HOTSPOT
-

Case study
-

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 conta`in 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
-

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.

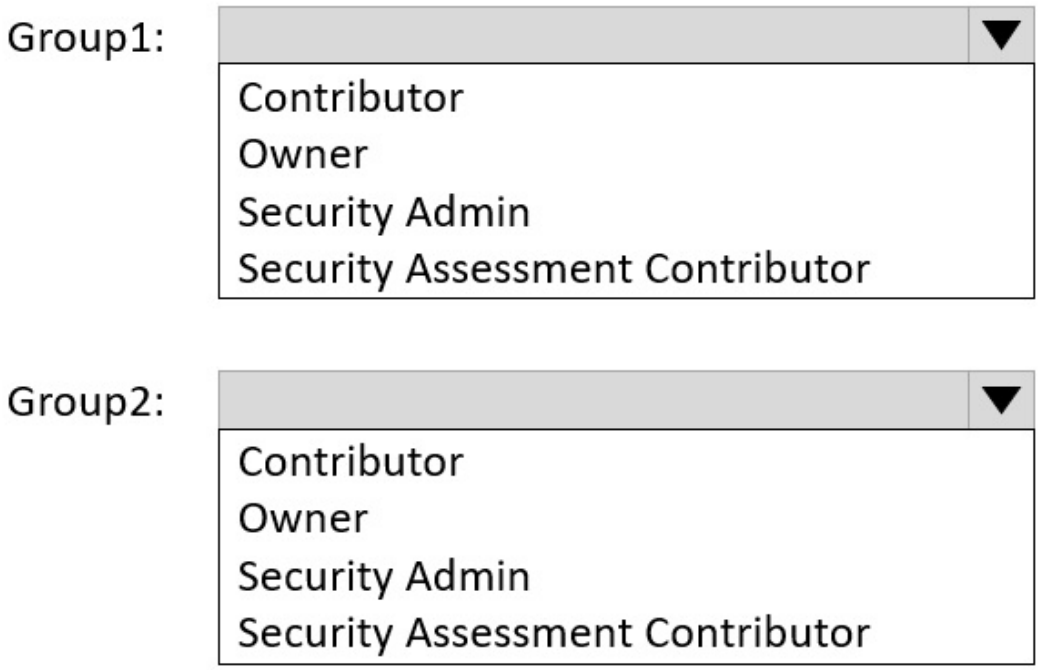
•Maximize the performance of data queries.
•Minimize the amount of collected data.

You need to assign role-based access control (RBAC) roles to Group1 and Group2 to meet the Microsoft Defender for Cloud requirements and the business requirements.

Which role should you assign to each group? To answer, select the appropriate options in the answer area.

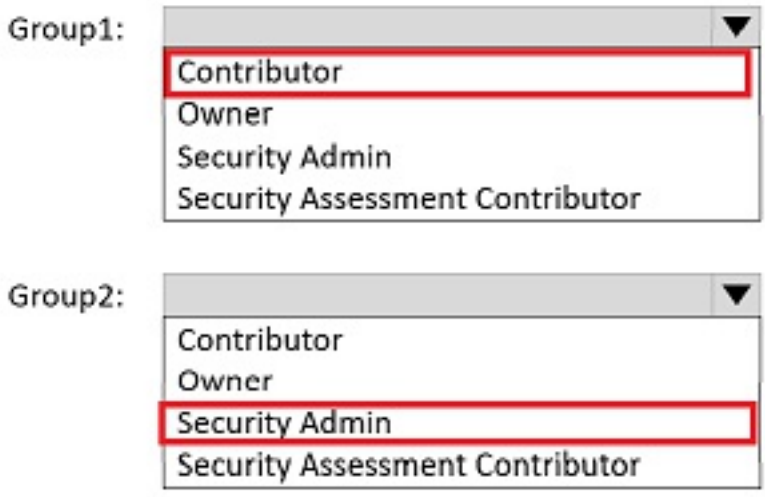
NOTE: Each correct selection is worth one point.

Answer Area



Answer:

Answer Area



Explanation:

Contributor

Security Admin

Question: 110 CertyIQ

Case study -

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 -

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 deploy the native cloud connector to Account 1 to meet the Microsoft Defender for Cloud requirements.

What should you do in Account1 first?

A.Create an AWS user for Defender for Cloud.

B.Configure AWS Security Hub.

C.Deploy the AWS Systems Manager (SSM) agent.

D.Create an Access control (IAM) role for Defender for Cloud.

Answer: A

Explanation:

https://learn.microsoft.com/en-us/defender-cloud-apps/connect-aws

Question: 111

CertyIQ

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

Explanation:

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

Question: 112 CertyIQ

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

You have a GitHub account named Account1 that contains 10 repositories.

You need to ensure that Defender for Cloud can access the repositories in Account1.

What should you do first in the Microsoft Defender for Cloud portal?

A.Enable integrations.
B.Enable a plan.
C.Add an environment.
D.Enable security policies.

Answer: C

Explanation:

To add an environment, you need to sign in to the Azure portal, go to Microsoft Defender for Cloud > Environment settings, select Add environment, and then select GitHub. You also need to enter a name, select your subscription, resource group, and region.

Question: 113 CertyIQ

HOTSPOT
-

You have an Azure subscription named Sub1 that uses Microsoft Defender for Cloud.

You have an Azure DevOps organization named AzDO1.

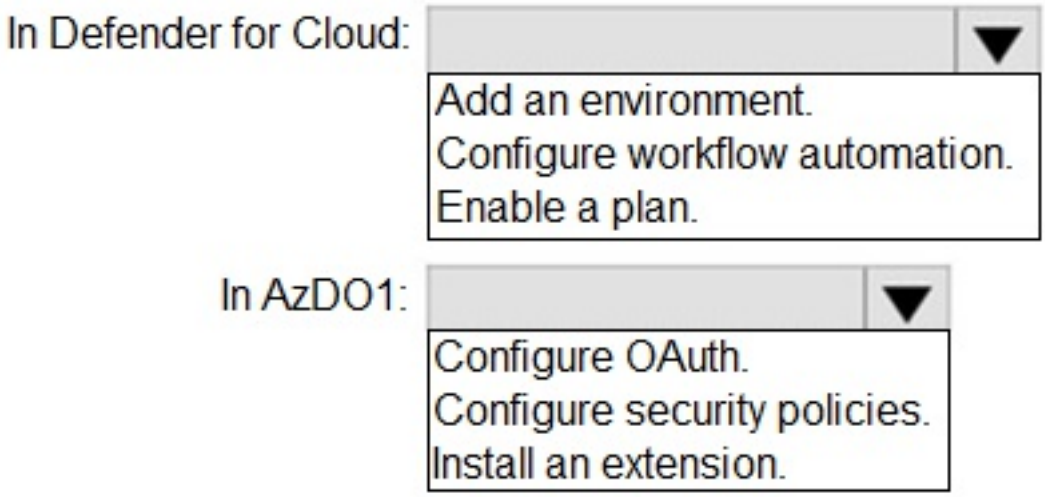
You need to integrate Sub1 and AzDO1. The solution must meet the following requirements:

•Detect secrets exposed in pipelines by using Defender for Cloud.
•Minimize administrative effort.

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

NOTE: Each correct selection is worth one point.

Answer Area



Answer:

Answer Area

In Defender for Cloud:

- Add an environment.
- Configure workflow automation.
- Enable a plan.

In AzDO1:

- Configure OAuth.
- Configure security policies.
- Install an extension.

Question: 114 CertyIQ

DRAG DROP
-

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

You need to create a workflow that will send a Microsoft Teams message to the IT department of your company when a new Microsoft Secure Score action is generated.

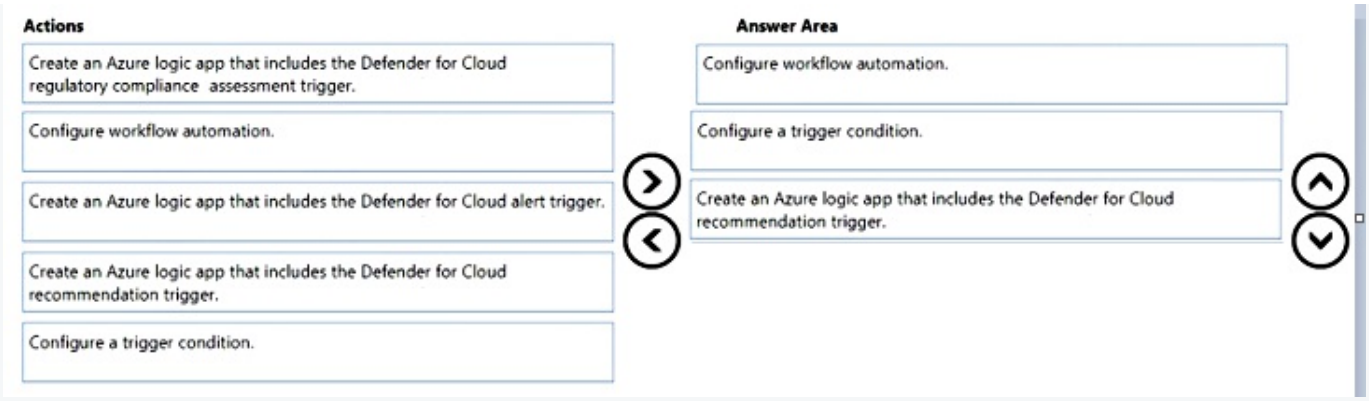
Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

Actions

- Create an Azure logic app that includes the Defender for Cloud regulatory compliance assessment trigger.
- Configure workflow automation.
- Create an Azure logic app that includes the Defender for Cloud alert trigger.
- Create an Azure logic app that includes the Defender for Cloud recommendation trigger.
- Configure a trigger condition.

Answer Area

Answer:



Explanation:

1. Configure workflow automation.

2. Configure a trigger condition.

3. Create an azure logic app that includes the Defender for Cloud recommendation trigger.

Reference:

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

Question: 115 CertyIQ

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: AE

Explanation:

A. Configure auto-provisioning by setting the security event storage to Common.

E. From Defender for Cloud in the Azure portal, enable Microsoft Defender for Servers.

Question: 116 CertyIQ

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

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

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

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

NOTE: Each correct answer is worth one point.

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

Answer: CE

Explanation:

A. is incorrect because agentless scanning is an optional feature. B. is incorrect because "when you enable Defender for Servers, Defender for Cloud automatically deploys a Defender for Endpoint extension." there is no need to onboard the machines with Defender for endpoint. D. is incorrect because virtual machine agent has nothing to doFor me the correct answers are: C. From Defender for Cloud, configure the AWS connector. E. From Defender for Cloud, configure auto-provisioning.

https://learn.microsoft.com/en-us/azure/defender-for-cloud/plan-defender-for-servers?source=recommendations

Question: 117 CertyIQ

HOTSPOT
-

You have an Azure subscription named Sub1 and an Azure DevOps organization named AzDO1. AzDO1 uses Defender for Cloud and contains a project that has a YAML pipeline named Pipeline1.

Pipeline1 outputs the details of discovered open source software vulnerabilities to Defender for Cloud.

You need to configure Pipeline to output the results of secret scanning to Defender for Cloud.

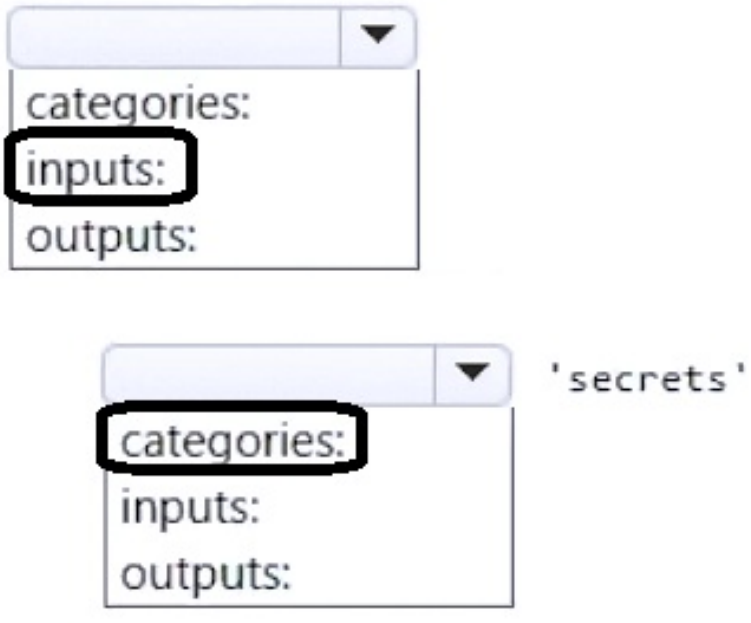
What should you add to Pipeline1? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Answer:

Answer Area



Explanation:

1. inputs

2. categories

Reference:

https://learn.microsoft.com/en-us/azure/defender-for-cloud/detect-exposed-secrets

Question: 118 CertyIQ

You create an Azure subscription named sub1.

In sub1, you create a Log Analytics workspace named workspace1.

You enable Microsoft Defender for Cloud and configure Defender for Cloud to use workspace1.

You need to collect security event logs from the Azure virtual machines that report to workspace1.

What should you do?

A.From Defender for Cloud, modify Microsoft Defender for Servers plan settings.
B.In sub1, register a provider.
C.From Defender for Cloud, create a workflow automation.
D.In workspace1, create a workbook.

Answer: A

Explanation:

From Defender for Cloud, modify Microsoft Defender for Servers plan settings.

Question: 119 CertyIQ

Case study -

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 -

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.

What should you configure for Server2?

A.the Microsoft Antimalware extension

B.the Azure Automanage machine configuration extension for Windows

C.an Azure resource lock

D.an Azure resource tag

Answer: D

Explanation:

Correct answer is D:an Azure resource tag.

Question: 120 CertyIQ

Case study -

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 -

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

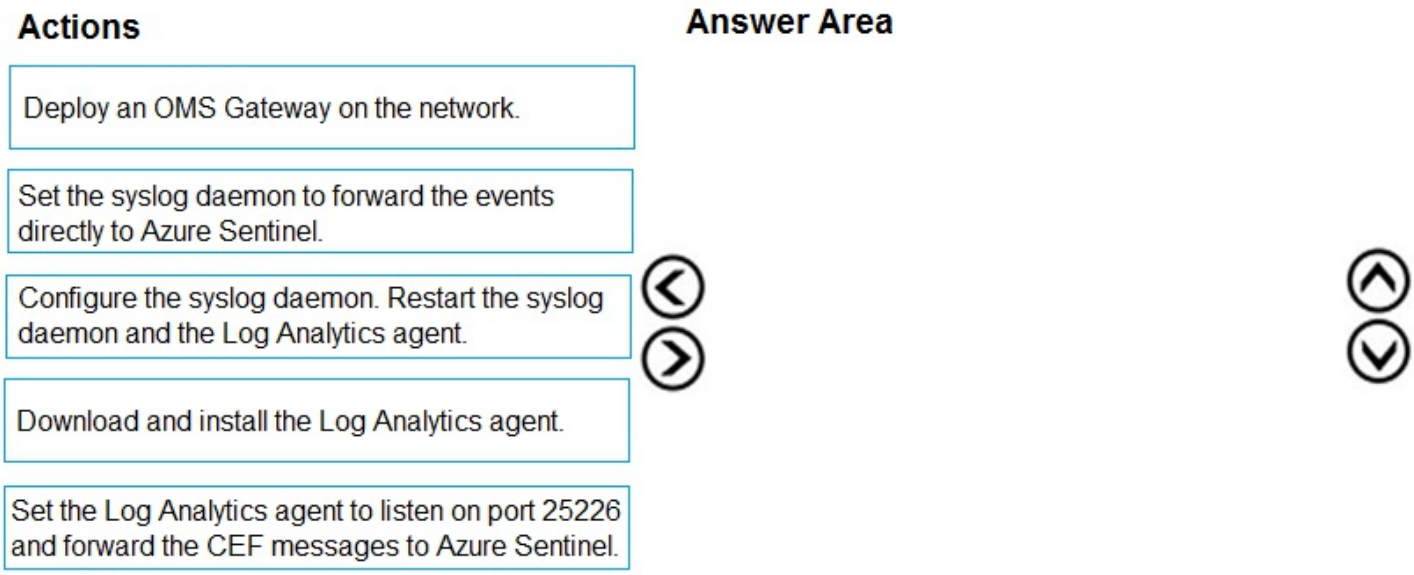
Answer: D

Explanation:

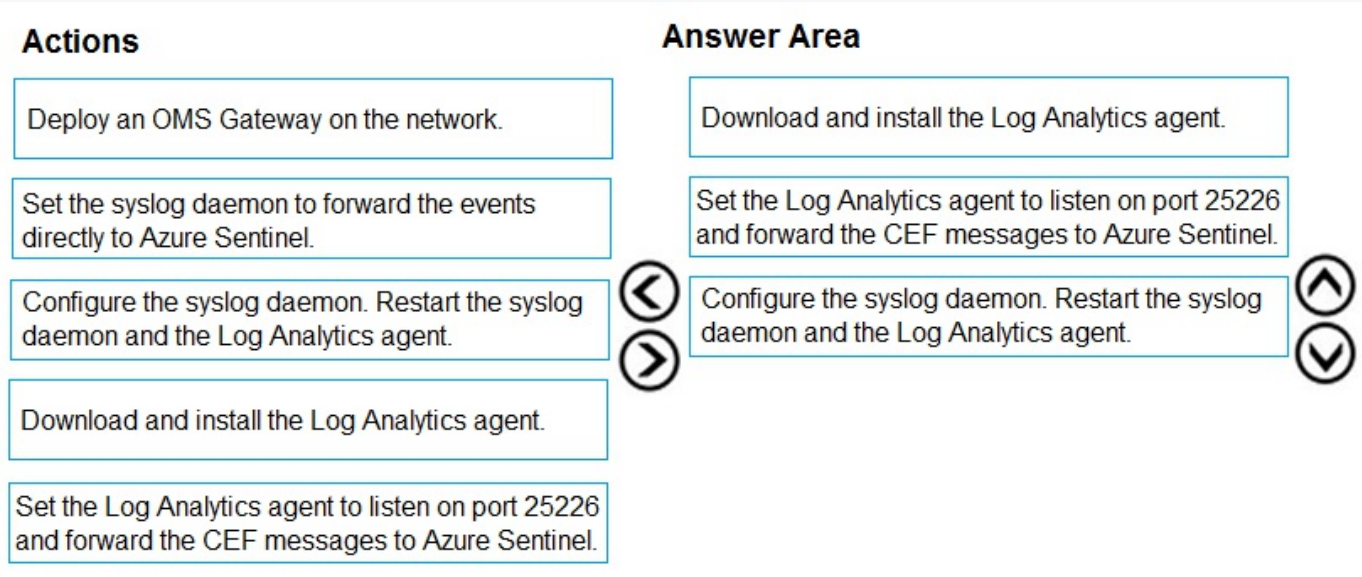
Only user that can assign initiatives. Owner is correct.

Question: 121 CertyIQ

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:

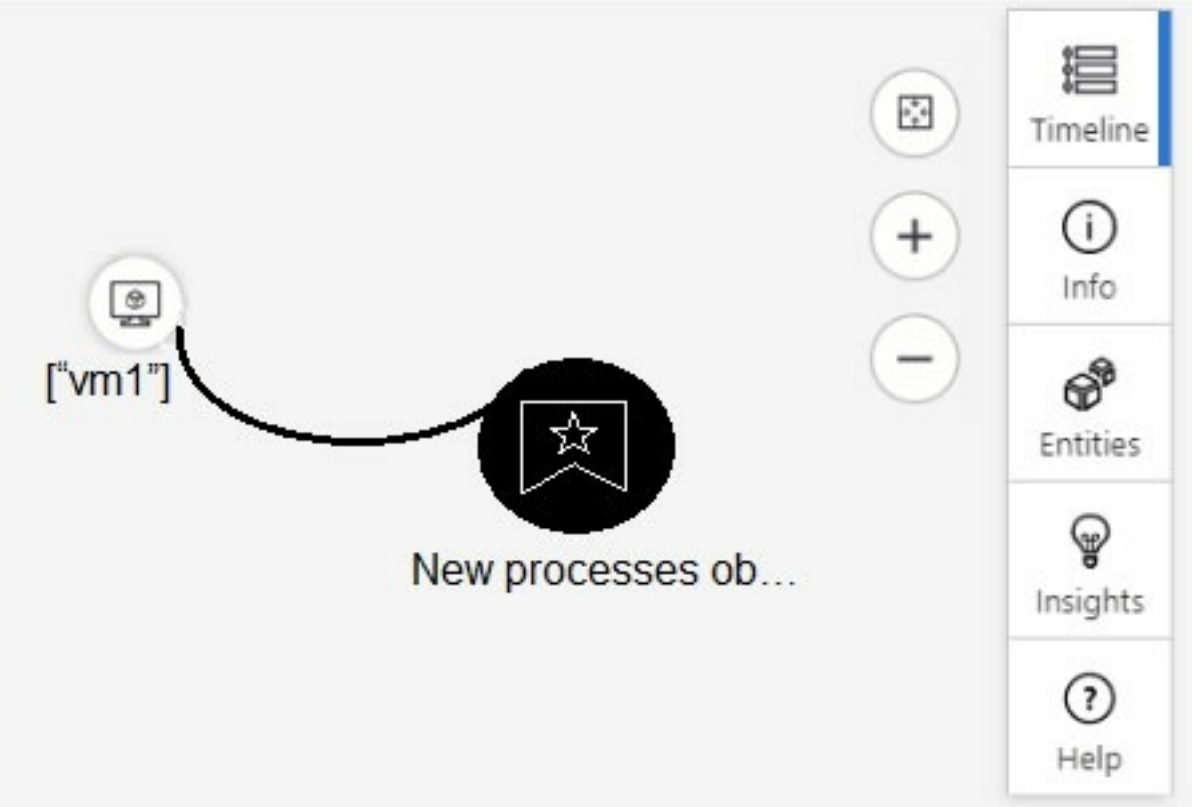


Explanation:

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

Question: 122 CertyIQ

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

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 items related to the incident.

- Entities
- Info
- Insights
- Timeline

Answer:

Answer Area

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 items related to the incident.

- **Entities**
- Info
- Insights
- Timeline

Explanation:

Correct answer is Processes and Entities

Question: 123 CertyIQ

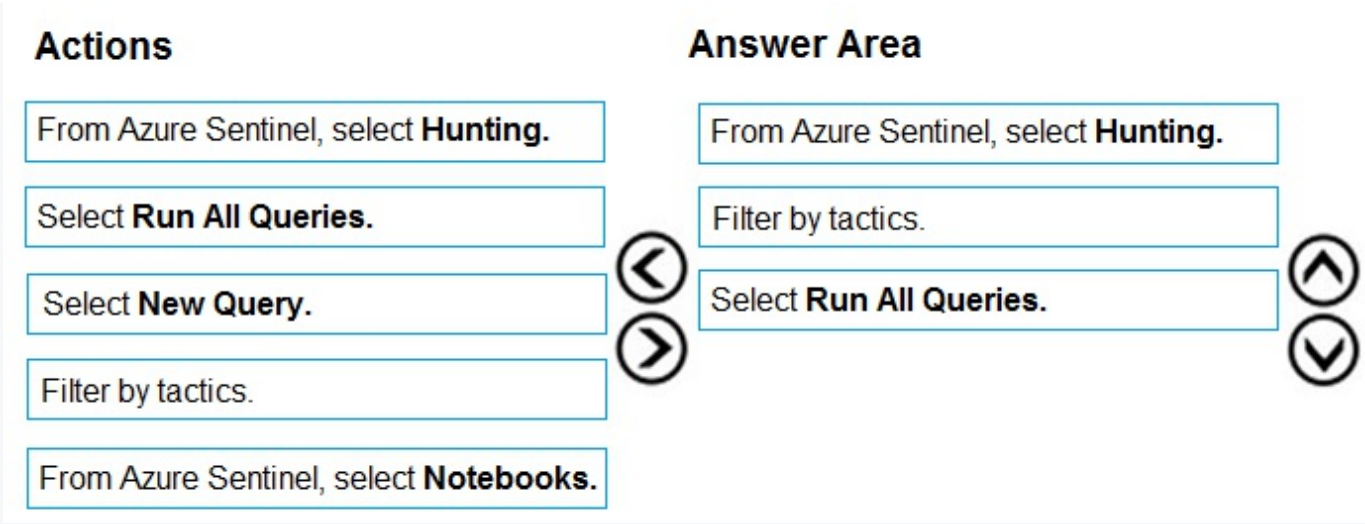
DRAG DROP -
You have an Azure Sentinel deployment.
You need to query for all suspicious credential access activities.
Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.
Select and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

Actions

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

Answer Area

Answer:



Explanation:

Reference:
https://davemccollough.com/2020/11/28/threat-hunting-with-azure-sentinel/

Question: 124 CertyIQ

You have an existing Azure logic app that is used to block Azure Active Directory (Azure AD) users. The logic app is triggered manually.
You deploy Azure Sentinel.
You need to use the existing logic app as a playbook in Azure Sentinel.
What should you do first?

A.And a new scheduled query rule.

B.Add a data connector to Azure Sentinel.

C.Configure a custom Threat Intelligence connector in Azure Sentinel.

D.Modify the trigger in the logic app.

Answer: D

Explanation:

the answer is D. Modify the trigger in the logic app.The logic app is currently triggered manually, but to use it as a playbook in Azure Sentinel, it needs to be triggered automatically when certain conditions are met. This requires modifying the trigger in the logic app so that it is triggered based on an event or a schedule in Azure Sentinel. For example, you could trigger the logic app when a new user is created in Azure AD, or when a specific security alert is generated in Azure Sentinel.Once the trigger in the logic app has been modified, you can proceed to the next steps, which may include adding a data connector to Azure Sentinel, configuring a custom Threat Intelligence connector, and creating a scheduled query rule.

Question: 125 CertyIQ

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

A.built-in queries

B.livestream

C.notebooks

D.bookmarks

Answer: C

Explanation:

Jupyter notebooks allow you to supercharge your threat hunting and investigation by enabling documents that contain live code, visualizations, and narrative text. These documents can be codified and served for specialized visualizations, an investigation guide, and sophisticated threat hunting.Additionally, notebooks can be used in security big data analytics for fast data processing on large datasets.

Reference:

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

Question: 126 CertyIQ

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 an alert and modify the action.

Answer: D

Explanation:

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

Question: 127 CertyIQ

You provision Azure Sentinel for a new Azure subscription.
You are configuring the Security Events connector.
While creating a new rule from a template in the connector, you decide to generate a new alert for every event.
You create the following rule query.

```
let timeframe = 1d;
SecurityEvent
| where TimeGenerated >= ago(timeframe)
| where EventID == 1102 and EventSourceName == "Microsoft-Windows-Eventlog"
| summarize StartTimeUtc = min(TimeGenerated), EndTimeUtc = max(TimeGenerated),
EventCount = count() by
Computer, Account, EventID, Activity
| extend timestamp = StartTimeUtc, AccountCustomEntity = Account,
HostCustomEntity = Computer
```

By which two components can you group alerts into incidents? Each correct answer presents a complete solution.
NOTE: Each correct selection is worth one point.

A.user

B.resource group

C.IP address

D.computer

Answer: AD

Explanation:

1. A. user and D. computer.To group alerts into incidents in Azure Sentinel, you can use any combination of the available grouping fields. In this case, since the rule query does not include information on resource groups or IP addresses, only user and computer can be used to group alerts into incidents.Grouping alerts by user and computer can help you identify patterns of activity and better understand the scope and impact of potential security threats. By grouping alerts into incidents, you can also more easily manage and track your response to security incidents.
2. To group alerts into incidents in Azure Sentinel, you can use the "user" and "computer" components in the rule query.

Question: 128 CertyIQ

Your company stores the data of every project in a different Azure subscription. All the subscriptions use the same Azure Active Directory (Azure AD) tenant.
Every project consists of multiple Azure virtual machines that run Windows Server. The Windows events of the virtual machines are stored in a Log Analytics workspace in each machine's respective subscription.
You deploy Azure Sentinel to a new Azure subscription.
You need to perform hunting queries in Azure Sentinel to search across all the Log Analytics workspaces of all the subscriptions.
Which two actions should you perform? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

A.Add the Security Events connector to the Azure Sentinel workspace.

B.Create a query that uses the workspace expression and the union operator.

C.Use the alias statement.

D.Create a query that uses the resource expression and the alias operator.

E.Add the Azure Sentinel solution to each workspace.

Answer: BE

Explanation:

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

Question: 129 CertyIQ

You have an Azure Sentinel workspace.
You need to test a playbook manually in the Azure portal.
From where can you run the test in Azure Sentinel?

A.Playbooks

B.Analytics

C.Threat intelligence

D.Incidents

Answer: D

Explanation:

Reference:
https://docs.microsoft.com/en-us/azure/sentinel/tutorial-respond-threats-playbook#run-a-playbook-on-demand

Question: 130 CertyIQ

You have a custom analytics rule to detect threats in Azure Sentinel.
You discover that the analytics rule stopped running. The rule was disabled, and the rule name has a prefix of AUTO DISABLED.
What is a possible cause of the issue?

A.There are connectivity issues between the data sources and Log Analytics.

B.The number of alerts exceeded 10,000 within two minutes.

C.The rule query takes too long to run and times out.

D.Permissions to one of the data sources of the rule query were modified.

Answer: D

Explanation:

Correct answer is DPermanent failure - rule auto-disable due to the following reasons The target workspace (on which the rule query operated) has been deleted.The target table (on which the rule query operated) has been deleted.Microsoft Sentinel had been removed from the target workspace.A function used by the rule query is no longer valid; it has been either modified or removed.Permissions to one of the data sources of the rule query were changed.One of the data sources of the rule query was deleted or disconnected.

Reference:

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

Question: 131 CertyIQ

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

A.Azure Sentinel Responder

B.Logic App Contributor

C.Azure Sentinel Contributor

D.Azure Sentinel Reader

Answer: A

Explanation:

Answer is correct. Using the least privilege principle Microsoft Sentinel Responder is the best role to assign this user

Reference:

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

Question: 132 CertyIQ

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: B

Explanation:

Correct - add data connectors to bring in source data for rules, notebooks, playbooks to query/take action against.

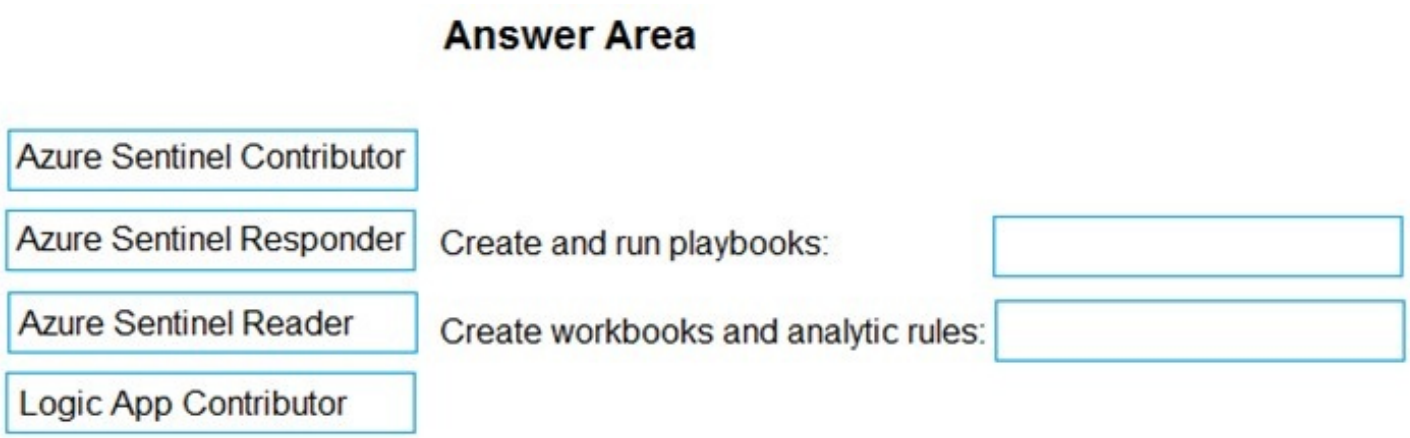
Reference:

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

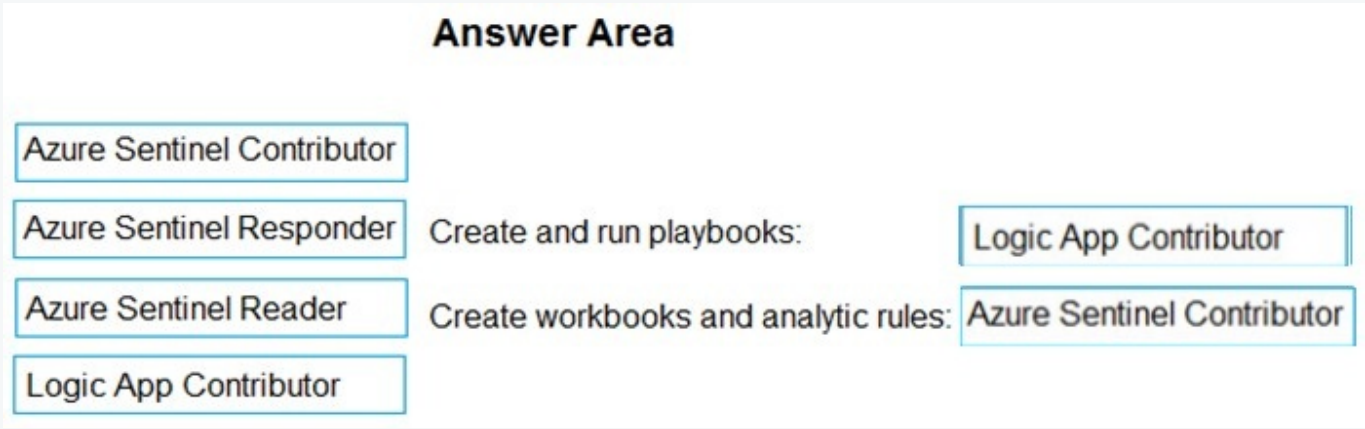
Question: 133 CertyIQ

DRAG DROP -
Your company deploys Azure Sentinel.
You plan to delegate the administration of Azure Sentinel to various groups.
You need to delegate the following tasks:
- Create and run playbooks
- Create workbooks and analytic rules.

The solution must use the principle of least privilege.
Which role should you assign for each task? To answer, drag the appropriate roles to the correct tasks. Each role may be used once, more than once, or not at all.
You may need to drag the split bar between panes or scroll to view content.
NOTE: Each correct selection is worth one point.
Select and Place:



Answer:



Explanation:

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

Question: 134 CertyIQ

A company uses Azure Sentinel.
You need to create an automated threat response.
What should you use?

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

Answer: B

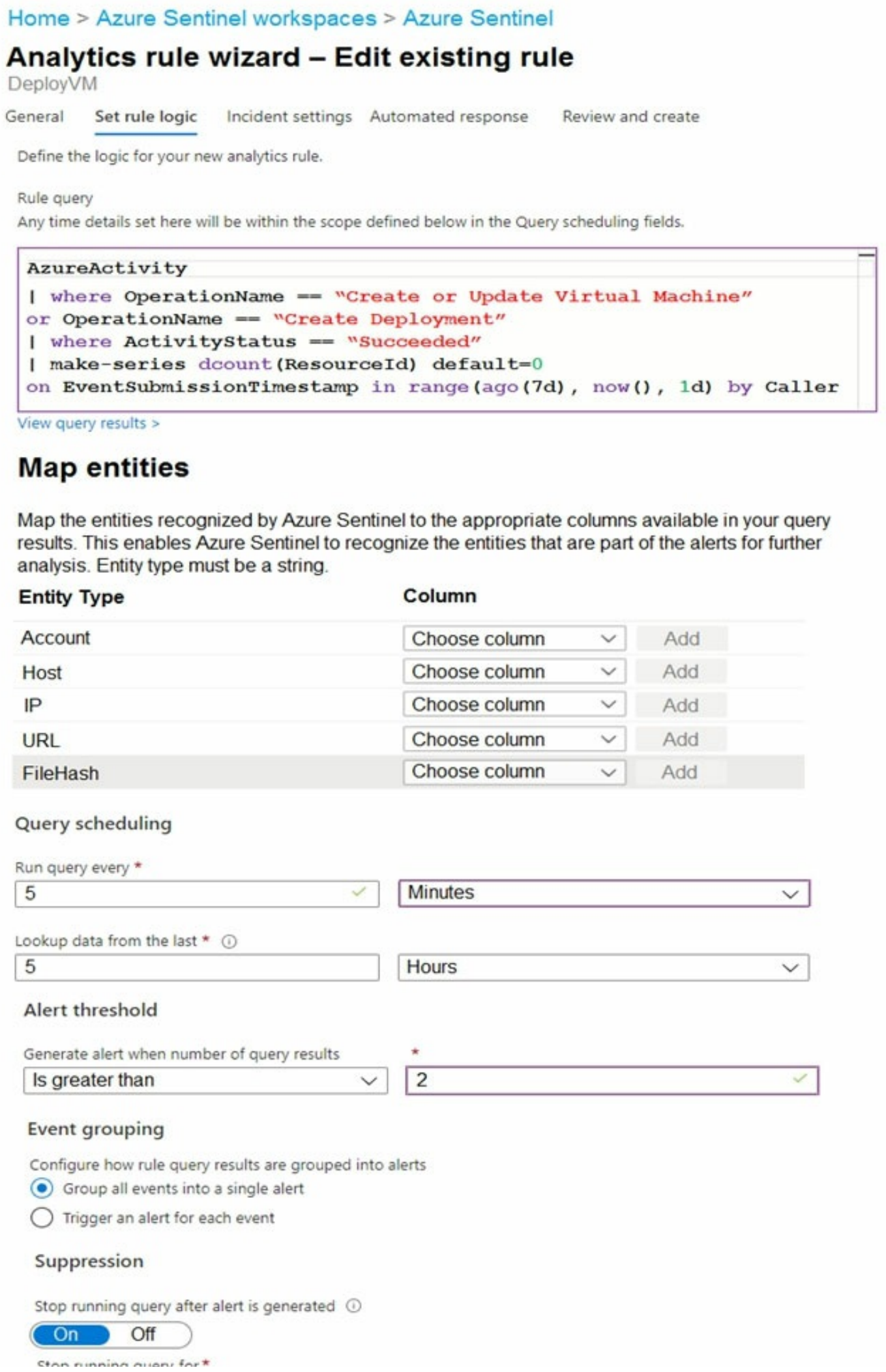
Explanation:

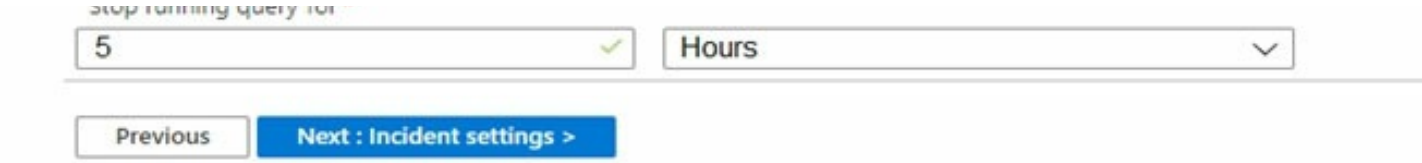
Reference:
https://docs.microsoft.com/en-us/azure/sentinel/tutorial-respond-threats-playbook

Question: 135 CertyIQ

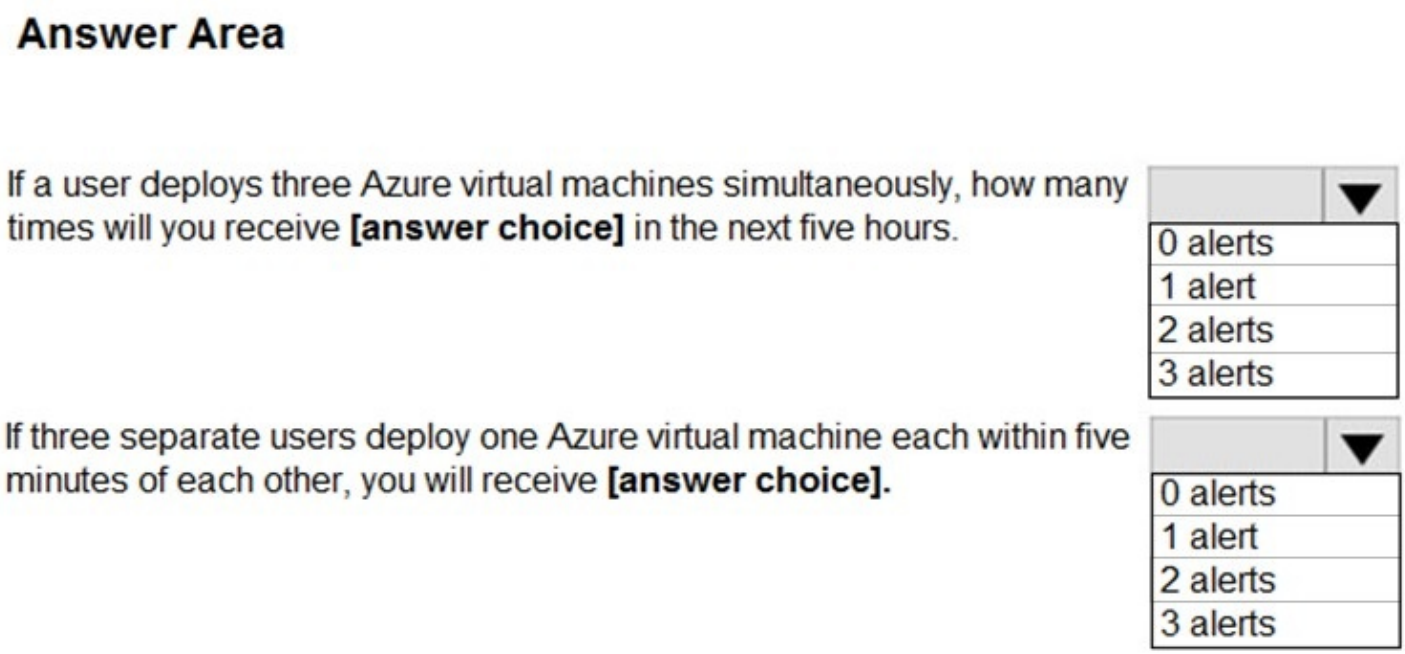
HOTSPOT -
You use Azure Sentinel to monitor irregular Azure activity.

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

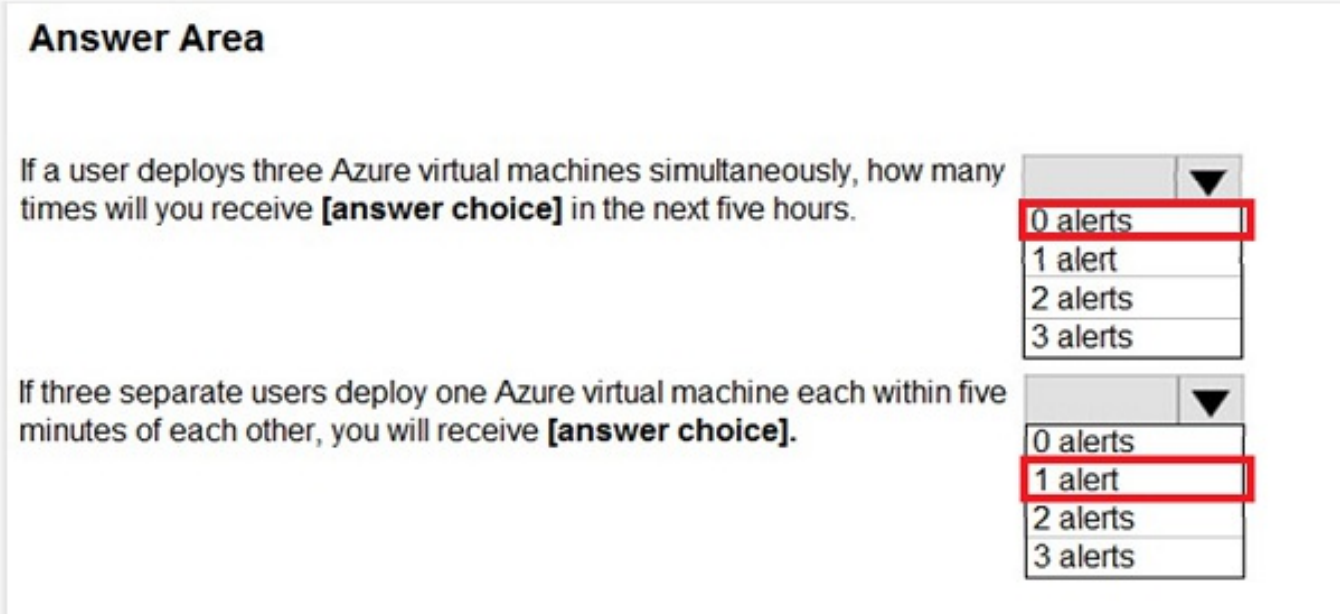




You do NOT define any incident settings as part of the rule definition.
Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.
NOTE: Each correct selection is worth one point.
Hot Area:



Answer:



Explanation:

0,1The first scenario will not generate any alerts, as each series by Caller generates a single result; there is only one caller, therefore 1 result, which is below the threshold (results > 2).In the second scenario, there will be 3 results (one for each caller), so one alert will be generated (as this is above the threshold and the results are grouped into a single alert).

Question: 136 CertyIQ

You have an Azure Sentinel deployment in the East US Azure region.
You create a Log Analytics workspace named LogsWest in the West US Azure region.
You need to ensure that you can use scheduled analytics rules in the existing Azure Sentinel deployment to generate alerts based on queries to LogsWest.
What should you do first?

A.Deploy Azure Data Catalog to the West US Azure region.

B.Modify the workspace settings of the existing Azure Sentinel deployment.

C.Add Azure Sentinel to a workspace.

D.Create a data connector in Azure Sentinel.

Answer: C

Explanation:

Correct answer - C.Cross-workspace queries can now be included in scheduled analytics rules. You can use cross-workspace analytics rules in a central SOC, and across tenants (using Azure Lighthouse) as in the case of an MSSP, subject to the following limitations:* Up to 20 workspaces can be included in a single query.* Azure Sentinel must be deployed on every workspace referenced in the query.* Alerts generated by a cross-workspace analytics rule, and the incidents created from them, exist only in the workspace where the rule was defined. They will not be displayed in any of the other workspaces referenced in the query

Reference:

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

Question: 137 CertyIQ

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

A.The rule query takes too long to run and times out.

B.The target workspace was deleted.

C.Permissions to the data sources of the rule query were modified.

D.There are connectivity issues between the data sources and Log Analytics

Answer: AD

Explanation:
Incorrect Answers:
B: This would cause it to fail every time, not just intermittently.
C: This would cause it to fail every time, not just intermittently.

Question: 138 CertyIQ

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

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

A.Yes

B.No

Answer: A

Explanation:

When you configure a scheduled query on "Set rule logic" and "incident settings", you can define if raise alert and how you group into incident.NB: create a Microsoft incident creation rule is part of a scheduled query.Microsoft wording for this question is weird...I don't understand why all these NO in the discussion. If someone have a good explanation, please don't hesitate.

Question: 139 CertyIQ

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You are configuring Azure Sentinel.
You need to create an incident in Azure Sentinel when a sign-in to an Azure virtual machine from a malicious IP address is detected.
Solution: You create a hunting bookmark.
Does this meet the goal?

A.Yes

B.No

Answer: B

Explanation:

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

Question: 140 CertyIQ

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You are configuring Azure Sentinel.
You need to create an incident in Azure Sentinel when a sign-in to an Azure virtual machine from a malicious IP address is detected.
Solution: You create a Microsoft incident creation rule for a data connector.
Does this meet the goal?

A.Yes

B.No

Answer: A

Explanation:

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

Question: 141 CertyIQ

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

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

Answer: B

Explanation:

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

Question: 142 CertyIQ

You are configuring Azure Sentinel.
You need to send a Microsoft Teams message to a channel whenever a sign-in from a suspicious IP address is detected.
Which two actions should you perform in Azure Sentinel? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

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

Answer: AB

Explanation:

A. Add a playbookB. Associate a playbook to an incidentTo send a Microsoft Teams message to a channel whenever a sign-in from a suspicious IP address is detected in Azure Sentinel, you will need to perform two actions:Add a playbook: A playbook is a set of actions that can be triggered in response to an incident, such as sending a message to a channel in Microsoft Teams. To add a playbook, you will need to navigate to the Playbooks tab in Azure Sentinel and create a new playbook that includes an action to send a message to a Microsoft Teams channel.Associate a playbook to an incident: After creating the playbook, you will need to associate it with an incident in Azure Sentinel. This can be done by navigating to the Incidents tab in Azure Sentinel and selecting the incident that you want to associate the playbook with. Then, select the "Associate Playbook" button and select the playbook that you created.

Reference:

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

Question: 143 CertyIQ

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

Explanation:

A. notebooks in Azure SentinelTo visualize Azure Sentinel data and enrich it by using third-party data sources to identify indicators of compromise (IoC), you can use notebooks in Azure Sentinel.Notebooks in Azure Sentinel are interactive documents that allow you to run queries, create visualizations, and perform data analysis on your Azure Sentinel data. They also allow you to connect to other data sources, such as third-party threat intelligence feeds, to enrich the data and identify indicators of compromise (IoCs).Once you have connected to the third-party data source, you can use Azure Sentinel notebook to blend the data, and create visualizations, and perform data analysis to identify the potential attack.

Reference:

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

Question: 144 CertyIQ

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: C

Explanation:

C is correct yes. Either summarize count() or count() should be usedhttps://techcommunity.microsoft.com/t5/azure-sentinel/azure-sentinel-workbooks-101-with-sample-workbook/ba-p/1409216

Reference:

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

Question: 145 CertyIQ

You use Azure 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: AD

Explanation:

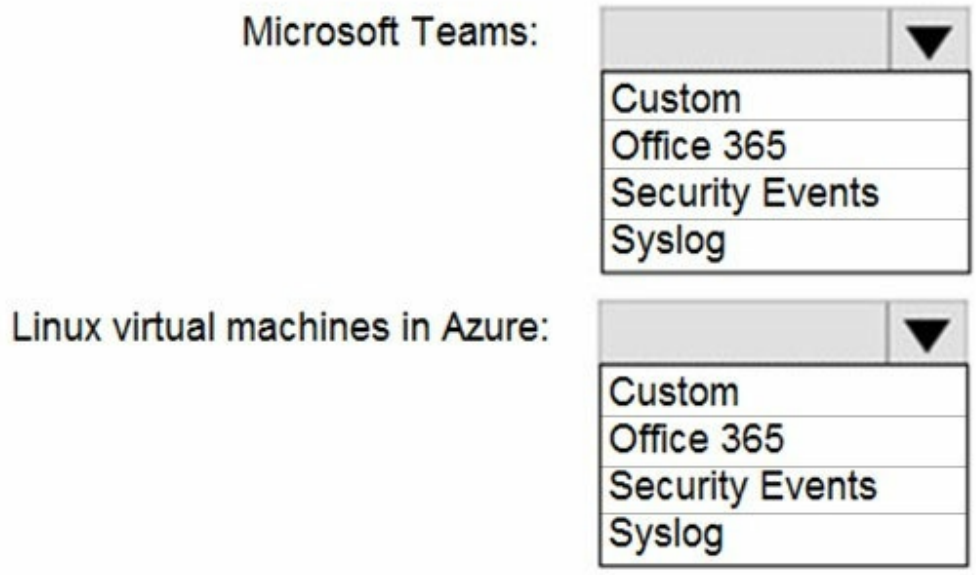
Use hunting livestream to create interactive sessions that let you test newly created queries as events occur, get notifications from the sessions when a match is found, and launch investigations if necessary. You can quickly create a livestream session using any Log Analytics query.

Sentinel needs data connectors to get data from other Azure Resources, so Add a data connector would make sense, but i think they would have said "you just deployed sentinel to your organization" then Adding a data connector would make sense. Here they point that you already use Azure Sentinel therefore i think the direct way to answer the question creating first the hunting query, and then use it on a livestream. (btw i've readed an answer where it's said livestream don't create alerts, and it's wrong) info here: Elevate a livestream session to an alertYou can promote a livestream session to a new alert by selecting Elevate to alert from the command bar on the relevant livestream session:https://learn.microsoft.com/en-us/azure/sentinel/livestream

Question: 146 CertyIQ

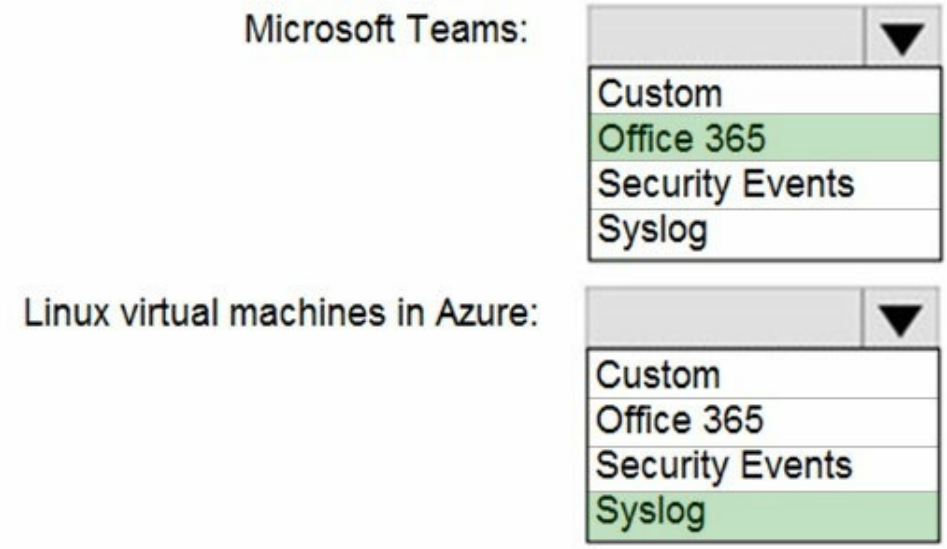
HOTSPOT -
You deploy Azure Sentinel.
You need to implement connectors in Azure Sentinel to monitor Microsoft Teams and Linux virtual machines in Azure. The solution must minimize administrative effort.
Which data connector type should you use for each workload? To answer, select the appropriate options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

Answer Area



Answer:

Answer Area



Explanation:

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

Question: 147

CertyIQ

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

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

A.Create a Microsoft incident creation rule

B.Share the incident URL

C.Create a scheduled query rule

D.Assign the incident

Answer: D

Explanation:

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

Question: 148 CertyIQ

You are configuring Azure Sentinel.
You need to send a Microsoft Teams message to a channel whenever an incident representing a sign-in risk event is activated in Azure Sentinel.
Which two actions should you perform in Azure Sentinel? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

A.Enable Entity behavior analytics.

B.Associate a playbook to the analytics rule that triggered the incident.

C.Enable the Fusion rule.

D.Add a playbook.

E.Create a workbook.

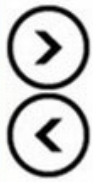
Answer: BD

Explanation:
1. Add a playbook to Azure Sentinel that includes the action to send a message to a Microsoft Teams channel.Associate the playbook to the analytics rule that triggers the incident.
2. Answer is D Add a playbookB Associate a playbook to the analytics rule that triggered the incident.UEBA also requires data sources from Azure and/or Thirdparty and will be able to help analyze and investigate an incident. This is not relevant to the question. So we have to assume data connectors are in place.

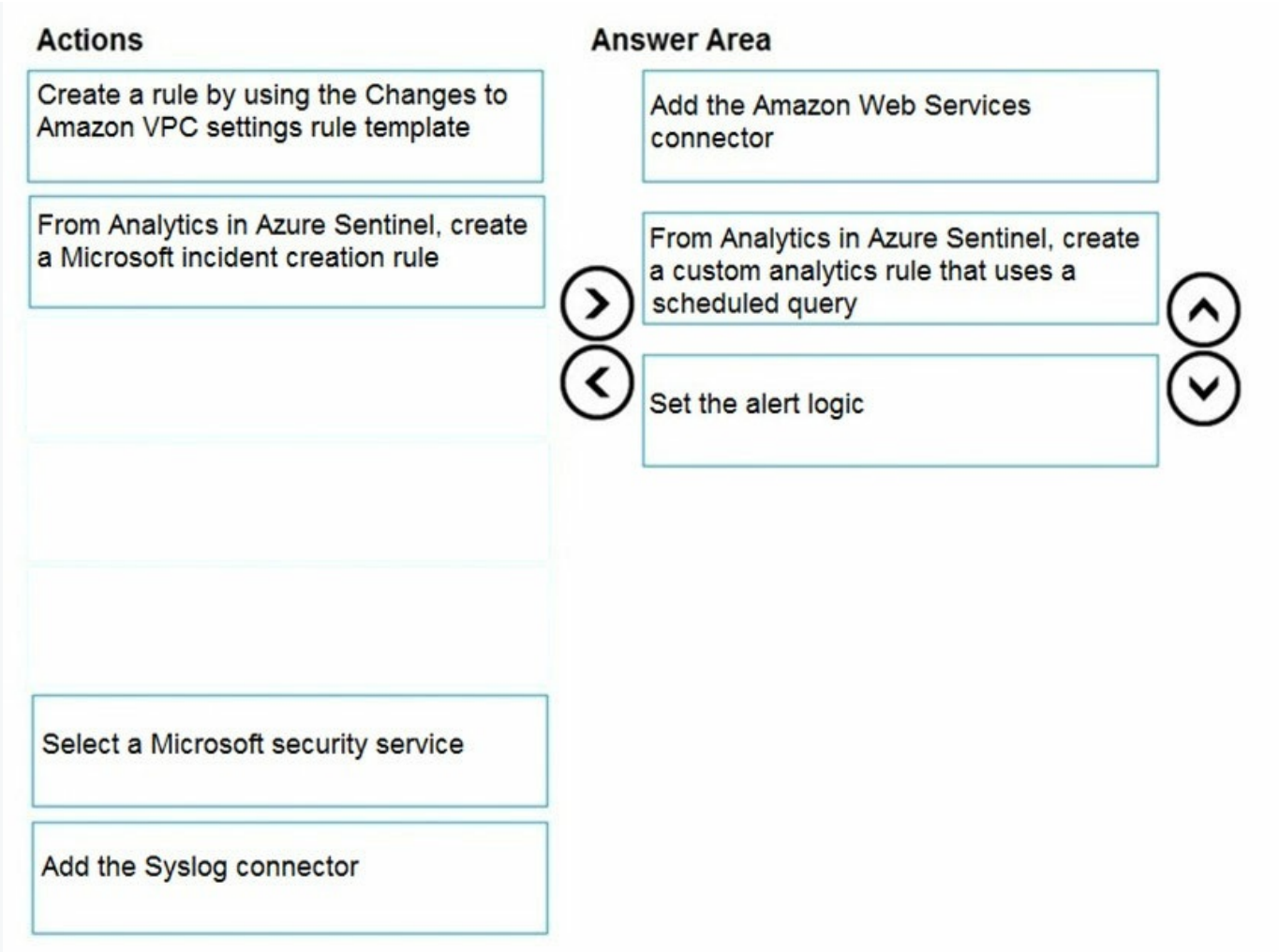
Question: 149 CertyIQ

DRAG DROP -
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.
Select and Place:

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:

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

Question: 150 CertyIQ

You have the following environment:

Azure Sentinel -

- A Microsoft 365 subscription
- Microsoft Defender for Identity
- An Azure Active Directory (Azure AD) tenant

You configure Azure Sentinel to collect security logs from all the Active Directory member servers and domain controllers.
You deploy Microsoft Defender for Identity by using standalone sensors.
You need to ensure that you can detect when sensitive groups are modified in Active Directory.
Which two actions should you perform? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

A.Configure the Advanced Audit Policy Configuration settings for the domain controllers.

B.Modify the permissions of the Domain Controllers organizational unit (OU).

C.Configure auditing in the Microsoft 365 compliance center.

D.Configure Windows Event Forwarding on the domain controllers.

Answer: AD

Explanation:

Answer is correct.A: Configure the Advanced Audit Policy Configuration settings for the domain controllersFor the correct events to be audited and included in the Windows Event Log, your domain controllers require accurate Advanced Audit Policy settings.https://learn.microsoft.com/en-us/defender-for-identity/configure-windows-event-collectionD: Configure Windows Event Forwarding on the domain controllers.To enhance detection capabilities, Defender for Identity needs the Windows events listed in Configure event collection. These can either be read automatically by the Defender for Identity sensor or in case the Defender for Identity sensor is not deployed, it can be forwarded to the Defender for Identity standalone sensor in one of two ways, by configuring the Defender for Identity standalone sensor to listen for SIEM events or by configuring Windows Event Forwarding.https://learn.microsoft.com/en-us/defender-for-identity/configure-event-forwarding

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

Question: 151 CertyIQ

You use Azure Sentinel.
You need to use a built-in role to provide a security analyst with the ability to edit the queries of custom Azure Sentinel workbooks. The solution must use the principle of least privilege.
Which role should you assign to the analyst?

A.Azure Sentinel Contributor
B.Security Administrator
C.Azure Sentinel Responder
D.Logic App Contributor

Answer: A

Explanation:
Azure Sentinel Contributor can create and edit workbooks, analytics rules, and other Azure Sentinel resources.

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

Question: 152 CertyIQ

You create a hunting query in Azure Sentinel.
You need to receive a notification in the Azure portal as soon as the hunting query detects a match on the query.
The solution must minimize effort.
What should you use?

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

Answer: C

Explanation:

Use livestream to run a specific query constantly, presenting results as they come in.

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

Question: 153 CertyIQ

You have an Azure subscription named Sub1 and a Microsoft 365 subscription. Sub1 is linked to an Azure Active Directory (Azure AD) tenant named contoso.com.
You create an Azure Sentinel workspace named workspace1. In workspace1, you activate an Azure AD connector for contoso.com and an Office 365 connector for the Microsoft 365 subscription.
You need to use the Fusion rule to detect multi-staged attacks that include suspicious sign-ins to contoso.com followed by anomalous Microsoft Office 365 activity.
Which two actions should you perform? Each correct answer present part of the solution.
NOTE: Each correct selection is worth one point.

A.Create custom rule based on the Office 365 connector templates.

B.Create a Microsoft incident creation rule based on Azure Security Center.

C.Create a Microsoft Cloud App Security connector.

D.Create an Azure AD Identity Protection connector.

Answer: AD

Explanation:

Thinking logically, there question gives no mention of MCAS and there are only two connectors active, AD (not identity protection) and O365. AD connector can give only what happened not what's suspicious, so you would need Azure AD Identity protection connector for that so D is certain.C is a no go as there is no log upload etc setup nor we talking about custom or third party apps or Shadow IT of any kind.B should not be the case as we are talking about identity compromise and then actions followed in O365, not on-prem so Azure Security center is out. Question is not talking about Incident generation either but fusion rule.Coming to A, there are samples of analytics rules about Log4J activities and other type of suspicious patterns, but there is nothing sort of specific about covering everything, so nothing is there built-in but all logs are there to capture any kind of activities in O365 and their pattern, so a custom rule makes sense which would need to cover relevant scenariosMy pick would be A & D

A. Create custom rule based on the Office 365 connector templates.D. Create an Azure AD Identity Protection connector.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 will need to perform two actions:Create custom rule based on the Office 365 connector templates: By creating a custom rule based on the Office 365 connector templates, you can monitor Office 365 activity for suspicious behavior, such as anomalous login attempts, or unusual activity from a specific IP address.Create an Azure AD Identity Protection connector: Azure AD Identity Protection is a security solution that provides visibility, control, and protection for Azure AD identities. By creating an Azure AD Identity Protection connector, you can monitor Azure AD activity for suspicious behavior, such as suspicious sign-ins, or unusual activity from a specific IP address.

Question: 154 CertyIQ

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not

appear in the review screen.
You are configuring Azure Sentinel.
You need to create an incident in Azure Sentinel when a sign-in to an Azure virtual machine from a malicious IP address is detected.
Solution: You create a livestream from a query.
Does this meet the goal?

A.Yes

B.No

Answer: B

Explanation:

No,You create a Microsoft incident creation rule for a data connector.

Reference:

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

Question: 155 CertyIQ

HOTSPOT -
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.
Hot Area:

Answer Area

```
SecurityIncident
| [ project / sort / summarize ] [ arg_max / limit / top ] (LasModifiedTime,*) by IncidentNumber
```

Answer:

Answer Area

```
SecurityIncident

| [ project / sort / summarize ] [ arg_max / limit / top ] (LasModifiedTime,*) by IncidentNumber
```

Explanation:

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

Question: 156 CertyIQ

DRAG DROP -
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.
Select and Place:

Resources

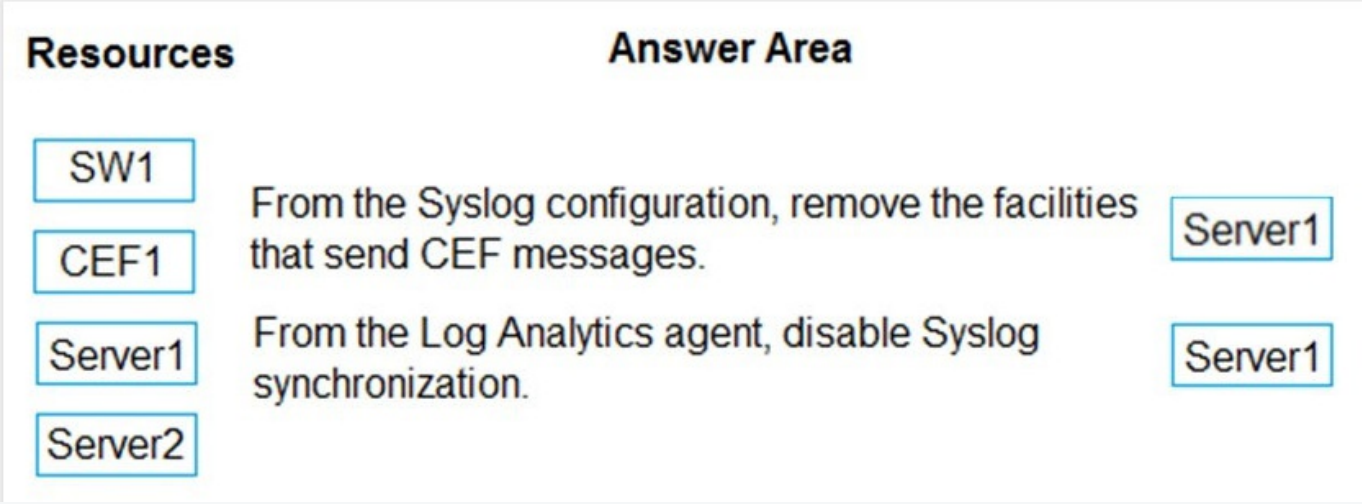
SW1
CEF1
Server1
Server2

Answer Area

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

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

Answer:



Explanation:

Server 1 & Server 1

https://docs.microsoft.com/en-us/azure/sentinel/connect-log-forwarder?tabs=rsyslog#run-the-deployment-script :Using the same machine to forward both plain Syslog and CEF messagesIf you plan to use this log forwarder machine to forward Syslog messages as well as CEF, then in order to avoid the duplication of events to the Syslog and CommonSecurityLog tables:**On each source machine that sends logs to the forwarder in CEF format**, 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. See Configure Syslog on Linux agent for detailed instructions on how to do this.You must run the following command **on those machines** 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.

Question: 157 CertyIQ

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

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

Answer: CD

Explanation:

C. Microsoft Sentinel automation rulesD. Microsoft Sentinel playbooksMicrosoft Sentinel's Automation rules can be used to automatically trigger actions or playbooks in response to detected security incidents. This reduces the need for manual intervention and minimizes administrative effort.Playbooks in Microsoft Sentinel can be used to automate incident response tasks and remediation steps, such as quarantining an affected machine or disabling a compromised account. This allows you to quickly and consistently take action on security incidents, further reducing administrative effort.

Reference:

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

Question: 158 CertyIQ

You have a Microsoft Sentinel workspace named workspace1 that contains custom Kusto queries.
You need to create a Python-based Jupyter notebook that will create visuals. The visuals will display the results of the queries and be pinned to a dashboard. The solution must minimize development effort.
What should you use to create the visuals?

A.plotly
B.TensorFlow
C.msticpy
D.matplotlib

Answer: C

Explanation:
msticpy is a library for InfoSec investigation and hunting in Jupyter Notebooks. It includes functionality to: query log data from multiple sources. enrich the data with Threat Intelligence, geolocations and Azure resource data. extract Indicators of Activity (IoA) from logs and unpack encoded data.
MSTICPy reduces the amount of code that customers need to write for Microsoft Sentinel, and provides:
Data query capabilities, against Microsoft Sentinel tables, Microsoft Defender for Endpoint, Splunk, and other data sources.
Threat intelligence lookups with TI providers, such as VirusTotal and AlienVault OTX.
Enrichment functions like geolocation of IP addresses, Indicator of Compromise (IoC) extraction, and WhoIs lookups.
Visualization tools using event timelines, process trees, and geo mapping.
Advanced analyses, such as time series decomposition, anomaly detection, and clustering.

Reference:
https://docs.microsoft.com/en-us/azure/sentinel/notebook-get-started https://msticpy.readthedocs.io/en/latest/

Question: 159 CertyIQ

HOTSPOT -
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.
Hot Area:

```
[ ▼ ]
```

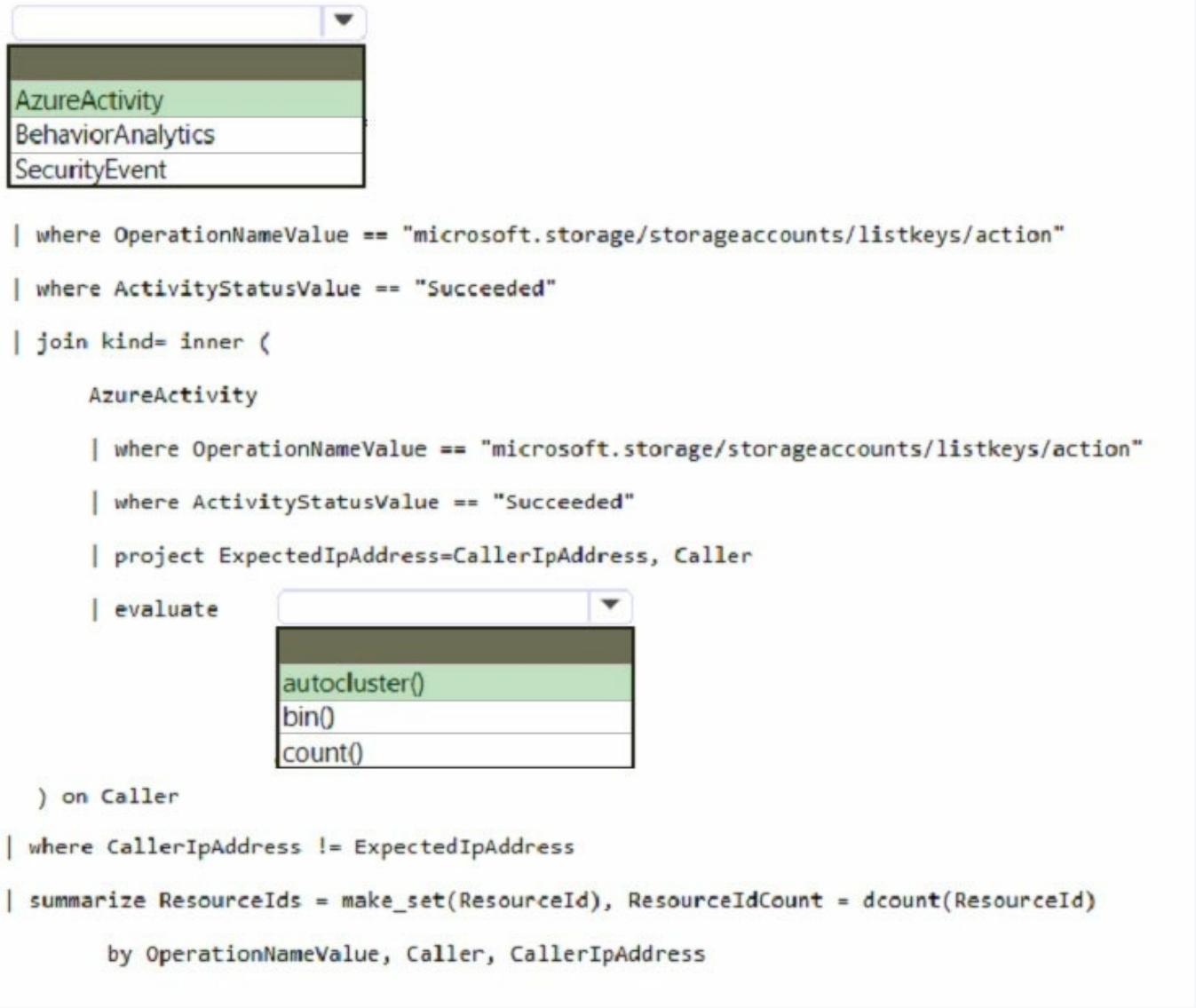
- AzureActivity
- BehaviorAnalytics
- SecurityEvent

```
| 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

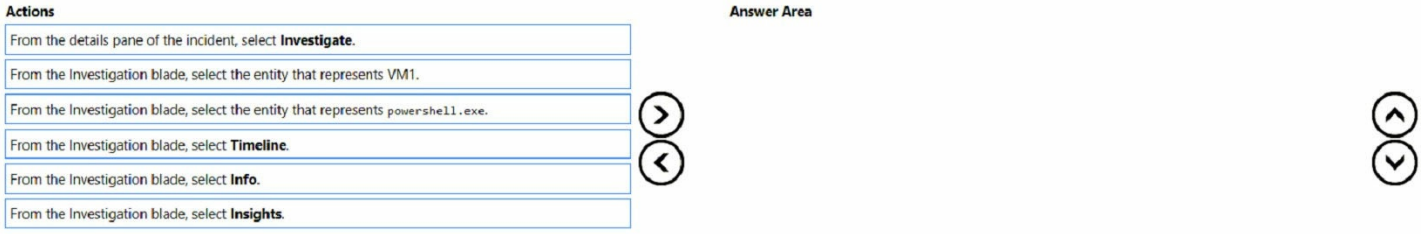
```
| evaluate autocluster()
) on Caller
| where CallerIpAddress != ExpectedIpAddress
| summarize StartTime = min(TimeGenerated), EndTime = max(TimeGenerated), ResourceIds =
make_set(ResourceId), ResourceIdCount = dcount
(ResourceId) by OperationNameValue, Caller, CallerIpAddress
| extend timestamp = StartTime, AccountCustomEntity = Caller, IPCustomEntity = CallerIpAddress
```

Reference:
https://github.com/Azure/Azure-Sentinel/blob/master/Hunting%20Queries/AzureActivity/Anomalous_Listing_Of_Storage_Keys.yaml

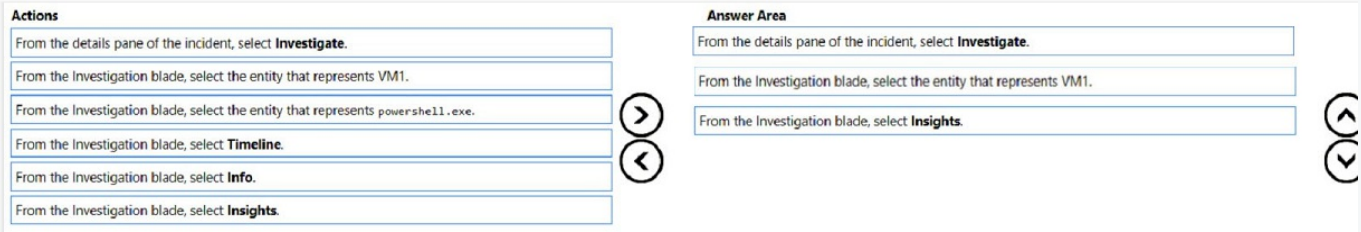
Question: 160 CertyIQ

DRAG DROP -
You have a Microsoft Sentinel workspace named workspace1 and an Azure virtual machine named VM1.
You receive an alert for suspicious use of PowerShell on VM1.
You need to investigate the incident, identify which event triggered the alert, and identify whether the following actions occurred on VM1 after the alert:
The modification of local group memberships
- The purging of event logs

Which three actions should you perform in sequence in the Azure portal? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.
Select and Place:



Answer:



Explanation:

Step 1:From the details pane of the incident, select Investigate

Step 2: From the Investigation blade, select the entity that represents VM1.

The Investigation Insights workbook is broken up into 2 main sections, Incident Insights and Entity Insights.

Incident Insights -

The Incident Insights gives the analyst a view of ongoing Sentinel Incidents and allows for quick access to their associated metadata including alerts and entity information.

Entity Insights -

The Entity Insights allows the analyst to take entity data either from an incident or through manual entry and

explore related information about that entity. This workbook presently provides view of the following entity types:

IP Address -

Account -

Host -

URL -

Step 3: From the Investigation blade, select Insights

Question: 161 CertyIQ

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 AccountCustomEntity entity associated with the incident.

D.From Investigation, review insights on the incident entity.

Answer: B

Explanation:
1. B. From Incidents, review the details of the IPCustomEntity entity associated with the incident.The IPCustomEntity entity associated with the incident should provide the IP address that triggered the brute force attack. You can then use a geolocation lookup tool to determine the country or region associated with that IP address
2. In the details of an incident, if you click on the IP entity it shows you the information under Geolocation information

Question: 162 CertyIQ

You have two Azure subscriptions that use Microsoft Defender for Cloud.
You need to ensure that specific Defender for Cloud security alerts are suppressed at the root management group level. The solution must minimize administrative effort.
What should you do in the Azure portal?

A.Create an Azure Policy assignment.

B.Modify the Workload protections settings in Defender for Cloud.

C.Create an alert rule in Azure Monitor.

D.Modify the alert settings in Defender for Cloud.

Answer: A

Explanation:
1. To suppress alerts at the management group level, use Azure Policy
2. A. Create an Azure Policy assignment.By creating an Azure Policy assignment at the root management group level, you can define a policy to suppress specific Defender for Cloud security alerts. This allows you to

ensure that the policy applies to all subscriptions and resources under the management group, without the need to modify the settings for each individual subscription.

Question: 163 CertyIQ

You have an Azure subscription that has the enhanced security features in Microsoft Defender for Cloud enabled and contains a user named User1.
You need to ensure that User1 can export alert data from Defender for Cloud. The solution must use the principle of least privilege.
Which role should you assign to User1?

A.User Access Administrator
B.Owner
C.Contributor
D.Reader

Answer: B

Explanation:

https://learn.microsoft.com/en-us/azure/defender-for-cloud/continuous-export?tabs=azure-portal#availability

Question: 164 CertyIQ

You have an Azure subscription that contains an Azure logic app named app1 and a Microsoft Sentinel workspace that has an Azure Active Directory (Azure AD) connector.
You need to ensure that app1 launches when Microsoft Sentinel detects an Azure AD-generated alert.
What should you create first?

A.a repository connection
B.a watchlist
C.an analytics rule
D.an automation rule

Answer: D

Explanation:

To ensure that app1 launches when Microsoft Sentinel detects an Azure AD-generated alert, you should create an automation rule first.

Question: 165 CertyIQ

You have a Microsoft Sentinel workspace.
You need to identify which rules are used to detect advanced multistage attacks that comprise two or more alerts or activities. The solution must minimize administrative effort.
Which rule type should you query?

A.Fusion
B.Microsoft Security

C.ML Behavior Analytics

D.Scheduled

Answer: A

Explanation:

Fusion rules in Microsoft Sentinel are rules that are used to detect advanced multistage attacks by combining alerts and activities from different sources. Fusion rules can be used to identify attacks that may not be detectable by a single alert or activity, making them particularly useful for detecting complex attacks that involve multiple stages.

Question: 166 CertyIQ

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 following requirements:
✑ Minimize administrative effort.
✑ Minimize the parsing required to read fog data.
What should you configure?

A.a Log Analytics Data Collector API

B.REST API integration

C.a Common Evert Format (CEF) connector

D.a Syslog connector

Answer: C

Explanation:

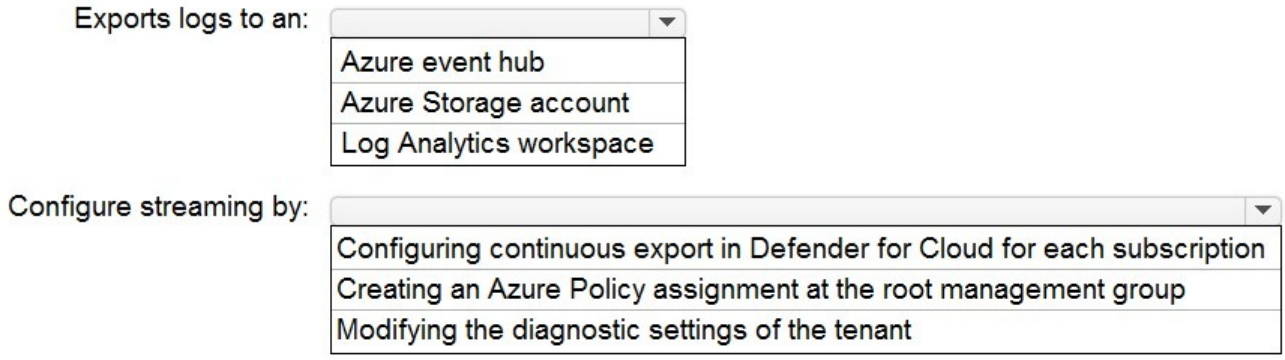
C. Common Event Format connector.Minimize the parsing required to read fog data. CEF connector sends Common Event Format data which means easy to read. As for administrative effort. You only need to configure the CEF server to listen for syslog from all the linux vms and then send the CEF data to Sentinel.

Minimize the parsing required to read fog data.

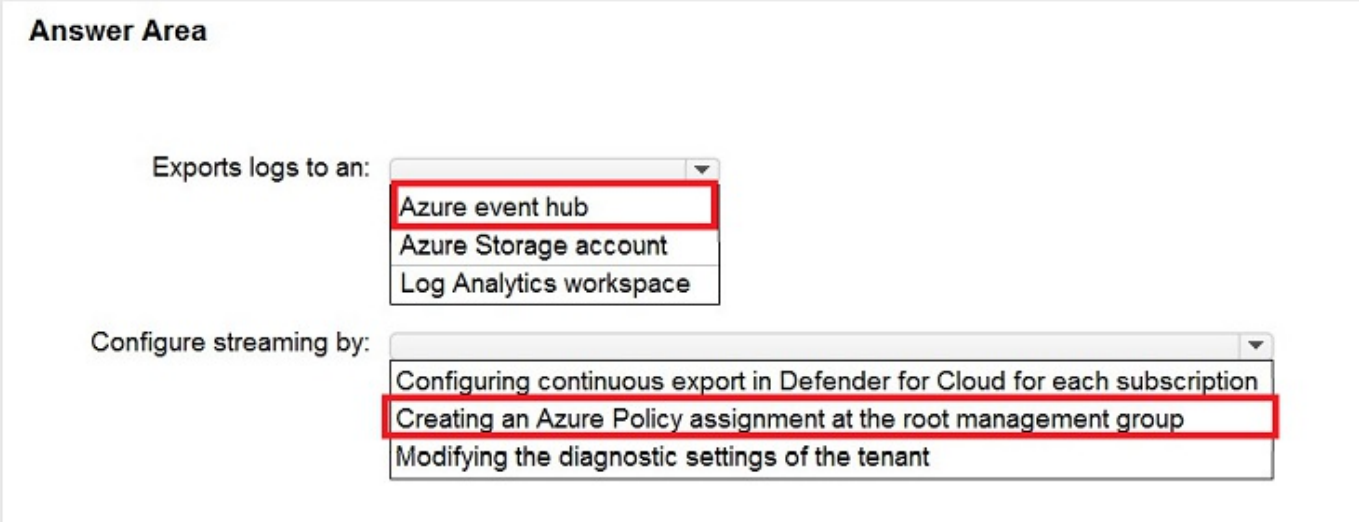
Question: 167 CertyIQ

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

Answer Area



Answer:



Explanation:

1 - Event Hub: https://docs.microsoft.com/en-us/azure/defender-for-cloud/export-to-siem#stream-alerts-with-continuous-export2 - Azure Policy - https://docs.microsoft.com/en-us/azure/defender-for-cloud/continuous-export?tabs=azure-policy#configure-continuous-export-at-scale-using-the-supplied-policies

Question: 168

CertyIQ

DRAG DROP -
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.
Select and Place:

Actions	Answer area
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:

Actions	Answer area
	Add Microsoft Sentinel to a workspace.
	Install the Log Analytics agent for Linux on the virtual machines.
	Add a Syslog connector to the workspace.
Add an Microsoft Sentinel workbook.	
Add a Syslog connector to the workspace.	

Question: 169

CertyIQ

You have an Azure subscription that uses Microsoft Sentinel.

You detect a new threat by using a hunting query.

You need to ensure that Microsoft Sentinel automatically detects the threat. The solution must minimize administrative effort.

What should you do?

A.Create an analytics rule.

B.Add the query to a workbook.

C.Create a watchlist.

D.Create a playbook.

Answer: A

Explanation:

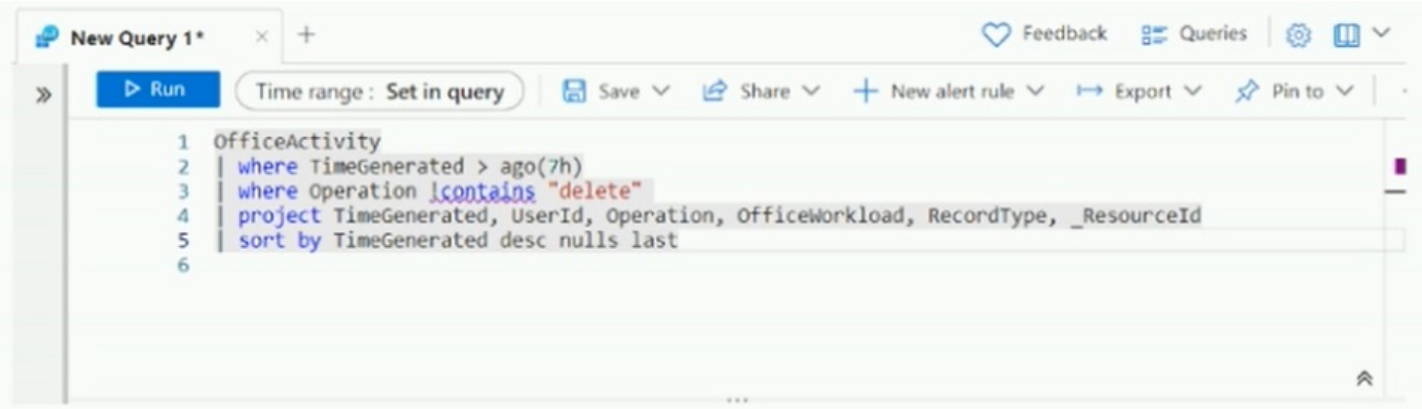
1. The fact that I'm paying contributor access to have these easy questions with a wrong answer really triggers me... This being said, the answer is clearly A.

2. Please somebody fixes the answer.

Question: 170 CertyIQ

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 Parser1.

You need to use Query1 in Parser1.

What should you do first?

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

Answer: B

Explanation:

B due to Parsing happens at query time, hense Query time parsing meaning we cannot parse a specific time.

Question: 171 CertyIQ

You have an Azure subscription that uses Microsoft Sentinel.

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

What should you create first?

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

Answer: B

Explanation:

B. a workbook.A Workbook is a collection of visualizations and data that can be used to analyze and report on

data in Azure Sentinel. It can be used to create custom reports that visualize sign-in information over time.

Question: 172 CertyIQ

You have a Microsoft Sentinel workspace.

You receive multiple alerts for failed sign-in attempts to an account.

You identify that the alerts are false positives.

You need to prevent additional failed sign-in alerts from being generated for the account. The solution must meet the following requirements:

• Ensure that failed sign-in alerts are generated for other accounts.
• Minimize administrative effort

What should do?

A.Modify the analytics rule.

B.Create a watchlist.

C.Add an activity template to the entity behavior.

D.Create an automation rule.

Answer: D

Explanation:

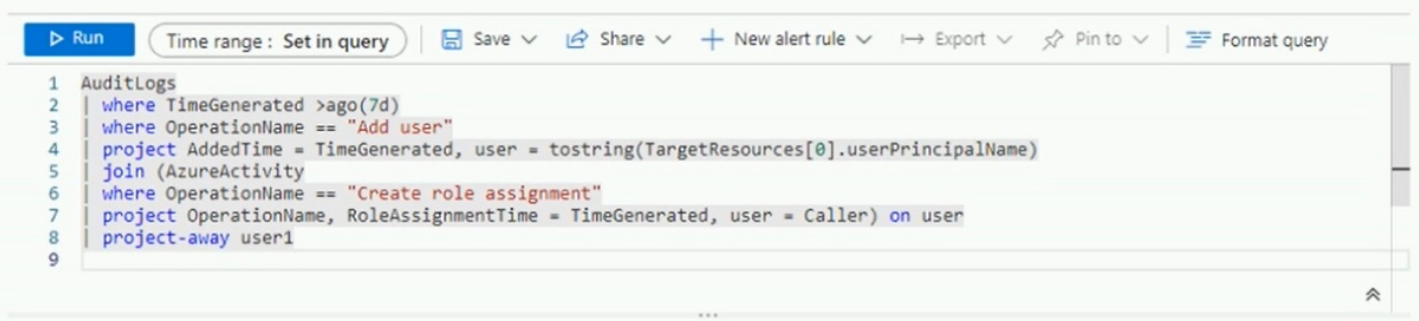
Agree: AUTOMATION RULES are a way to centrally manage automation in Microsoft Sentinel, by allowing you to define and coordinate a small set of rules that can apply across different scenarios.

Question: 173 CertyIQ

HOTSPOT
-

You have a Microsoft 365 E5 subscription that contains two users named User1 and User2.

You have the hunting query shown in the following exhibit.



The users perform the following actions:

• User1 assigns User2 the Global administrator role.
• User1 creates a new user named User3 and assigns the user a Microsoft Teams license.
• User2 creates a new user named User4 and assigns the user the Security reader role.
• User2 creates a new user named User5 and assigns the user the Security operator role.

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

NOTE: Each correct selection is worth one point.

Answer Area

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

Answer:

Answer Area

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

Explanation:

with operator projet-away the query result wont't show anything for User1so the answer should be N,N,Y

Question: 174 CertyIQ

HOTSPOT
-

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, '
    IPCustomEntity = case(IPMatch == "SourceIP", SourceIP, IPMatch == "DestinationIP", DestinationIP, "None")
```

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

NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
The `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:

yes

no

yes

Question: 175

CertyIQ

HOTSPOT
-

You have a Microsoft Sentinel workspace.

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

You need to validate Schema1.

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

NOTE: Each correct selection is worth one point.

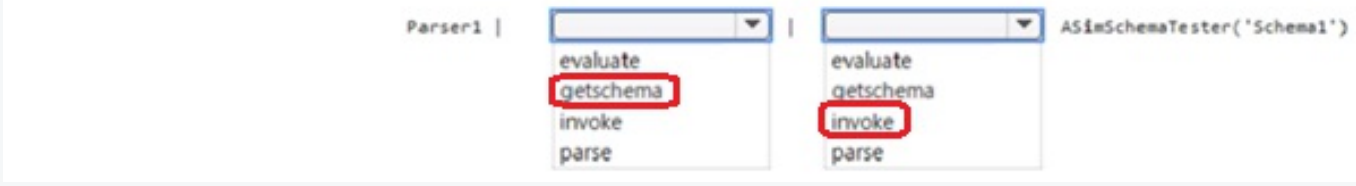
Answer Area

```
Parser1 | [ ▼ ] | [ ▼ ] ASimSchemaTester('Schema1')
```

evaluate	evaluate
getschema	getschema
invoke	invoke
parse	parse

Answer:

Answer Area



Question: 176

CertyIQ

HOTSPOT
-

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

Answer:

Answer Area

Explanation:

Join kind = inner, IdentityInfohttps://learn.microsoft.com/en-us/azure/sentinel/investigate-with-ueba#embed-identityinfo-data-in-your-analytics-rules-public-preview

Question: 177 CertyIQ

HOTSPOT
-

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 Area

```
let timeframe = ago(3h);
let threshold = 5;
[                    ▼]
    imAuthentication
    imNetworkSession
    imProcessCreate
    imWebSession
| 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(  [                    ▼]  ) by TargetUserId, TargetUserPrincipalName, TargetUserType
    DstGeoCountry
    SrcGeoCountry
    SrcGeoRegion
| where NumOfCountries >= threshold
| extend timestamp = StartTime, AccountCustomEntity = TargetUserPrincipalName
```

Answer:

Answer Area

```
let timeframe = ago(3h);
let threshold = 5;
[ imAuthentication ▼ ]
    imAuthentication
    imNetworkSession
    imProcessCreate
    imWebSession
| 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( [ SrcGeoRegion ▼ ] ) by TargetUserId, TargetUserPrincipalName, TargetUserType
    DstGeoCountry
    SrcGeoCountry
    SrcGeoRegion
| where NumOfCountries >= threshold
| extend timestamp = StartTime, AccountCustomEntity = TargetUserPrincipalName
```

Question: 178

CertyIQ

HOTSPOT
-

You have an Azure subscription.

You plan to implement a Microsoft Sentinel workspace. You anticipate that you will ingest 20 GB of security log data per day.

You need to configure storage for the workspace. The solution must meet the following requirements:

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

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

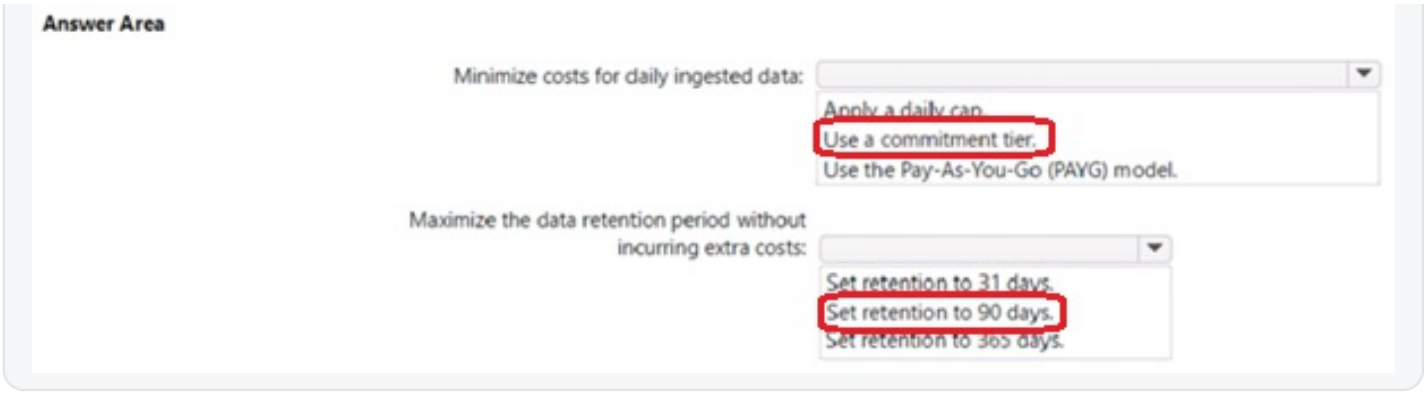
NOTE: Each correct selection is worth one point.

Answer Area

Minimize costs for daily ingested data: [▼]
- Apply a daily cap.
- Use a commitment tier.
- Use the Pay-As-You-Go (PAYG) model.

Maximize the data retention period without incurring extra costs: [▼]
- Set retention to 31 days.
- Set retention to 90 days.
- Set retention to 365 days.

Answer:



Question: 179 CertyIQ

HOTSPOT
-

You have a Microsoft Sentinel workspace named sws1.

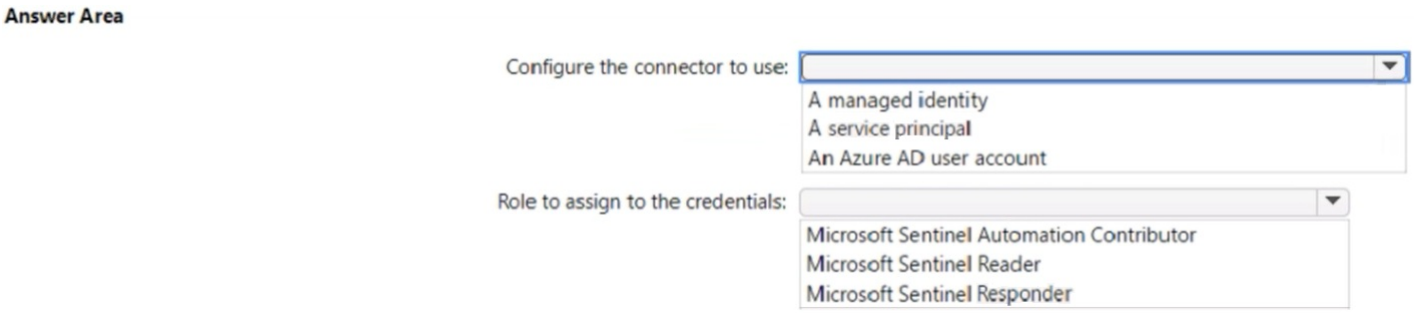
You plan to create an Azure logic app that will raise an incident in an on-premises IT service management system when an incident is generated in sws1.

You need to configure the Microsoft Sentinel connector credentials for the logic app. The solution must meet the following requirements:

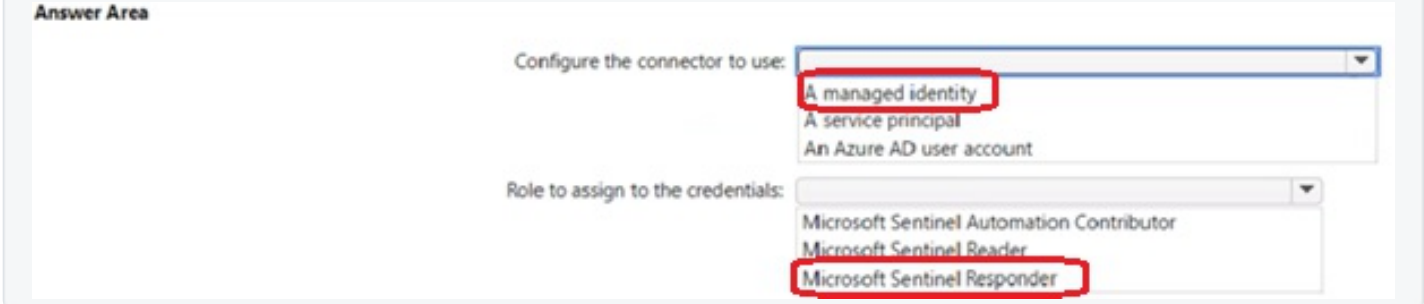
• Minimize administrative effort.
• Use the principle of least privilege.

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:



Question: 180 CertyIQ

You have a Microsoft Sentinel workspace.

You need to prevent a built-in Advanced Security Information Model (ASIM) parser from being updated automatically.

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

NOTE: Each correct selection is worth one point.

A.Create a hunting query that references the built-in parser.

B.Build a custom unifying parser and include the built-in parser version.

C.Redeploy the built-in parser and specify a CallerContext parameter of Any and a SourceSpecificParser parameter of Any.

D.Redeploy the built-in parser and specify a CallerContext parameter of Built-in.

E.Create an analytics rule that includes the built-in parser.

Answer: BC

Explanation:

https://learn.microsoft.com/en-us/azure/sentinel/normalization-manage-parsershttps://learn.microsoft.com/en-us/azure/sentinel/normalization-manage-parsers#prevent-an-automated-update-of-a-built-in-parser

Question: 181 CertyIQ

You have a custom Microsoft Sentinel workbook named Workbook1.

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

What should you do?

A.In the grid query, include the take operator.

B.In the grid query, include the project operator.

C.In the query editor interface, configure Settings.

D.In the query editor interface, select Advanced Editor.

Answer: A

Explanation:

A. In the grid query, include the take operator.The take operator allows you to limit the number of rows returned by a query. By including the take operator in the grid query and specifying a maximum of 100 rows, you can ensure that the grid in Workbook1 contains a maximum of 100 rows.For example, you could use the following query:| take 100

A. In the grid query, include the take operator.By including the take operator in the grid query, we can limit the number of rows displayed to a maximum of 100. The take operator allows us to specify the number of rows to retrieve from the data source.

Question: 182 CertyIQ

HOTSPOT
-

You have a Microsoft Sentinel workspace named SW1.

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

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

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

NOTE: Each correct selection is worth one point.

Answer Area

```
SecurityAlert
| where TimeGenerated >= ago(30d)
| summarize count() by ProviderName, [ ▼ ] (TimeGenerated, 1d)
| [ ▼ ]  timechart
```

[▼] options: bin, series_add, series_fill_linear, take

[▼] options: materialize, project, render

Answer:

Answer Area

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

[bin ▼] options: bin, series_add, series_fill_linear, take

[render ▼] options: materialize, project, render

Explanation:

https://techcommunity.microsoft.com/t5/microsoft-sentinel-blog/azure-sentinel-workbooks-101-with-sample-workbook/ba-p/1409216

Question: 183 CertyIQ

You have a Microsoft Sentinel workspace named Workspace1.

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

What should you create in Workspace1?

A.an analytic rule

B.a watchlist

C.a workbook

D.a hunting query

Answer: B

Explanation:

https://learn.microsoft.com/en-us/azure/sentinel/normalization-manage-parsers

Question: 184 CertyIQ

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

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

What should you create first?

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

Answer: B

Explanation:

Logic Apps are a dependency for creating a playbook

Question: 185 CertyIQ

HOTSPOT
-

You have a Microsoft Sentinel workspace named Workspace1.

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.

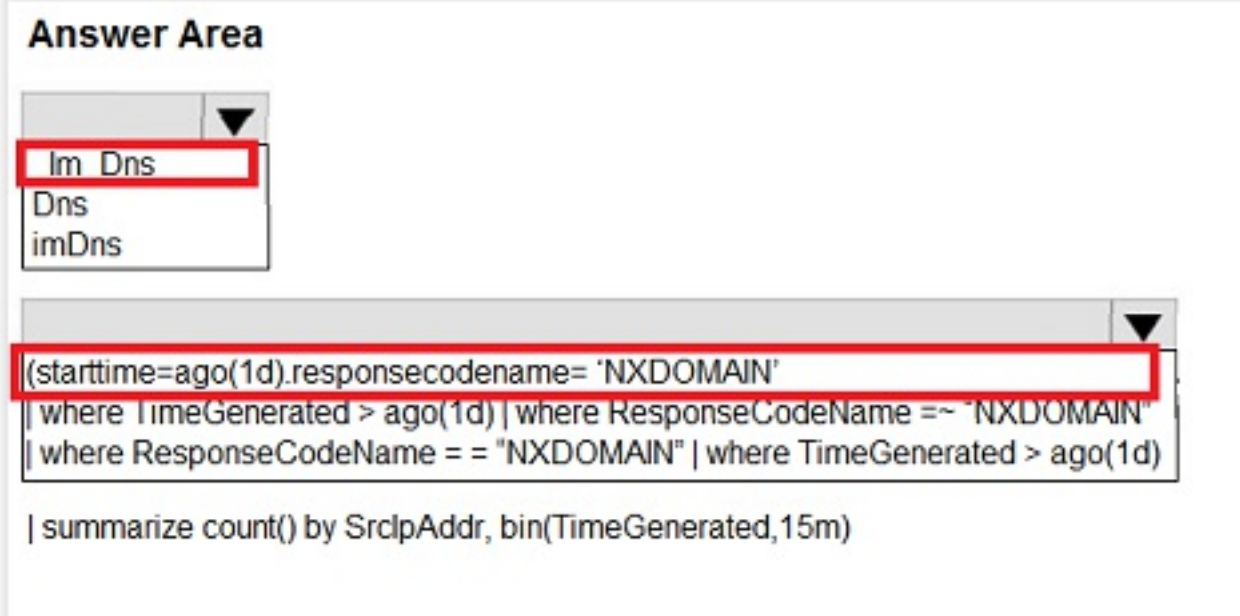
Answer Area

_Im_Dns
Dns
imDns

(starttime=ago(1d).responsecodename= 'NXDOMAIN'
| where TimeGenerated > ago(1d) | where ResponseCodeName =~ "NXDOMAIN"
| where ResponseCodeName = = "NXDOMAIN" | where TimeGenerated > ago(1d)

| summarize count() by SrcIpAddr, bin(TimeGenerated,15m)

Answer:



Explanation:

First box is correct, second option should be (and correct me if I'm wrong)(starttime=ago(1d), responsecodename='NXDOMAIN')Question states: 'from the last 24 hrs' and 'The solution must maximize query performance'Both the second and third option in the second box give 'TimeGenerate>ago(1d)', for me that reads as events generated greater than the last 24 hours - not what we're looking for.so the query is: _Im_Dns(starttime=ago(1d), responsecodename='NXDOMAIN') | summarize count() by SrcIpAddr, bin(TimeGenerated,15m)using the link Albonzi giveshttps://learn.microsoft.com/en-us/azure/sentinel/normalization-about-parsers#optimizing-parsing-using-parametersEvery schema that supports filtering parameters supports at least the starttime and endtime parameters and using them is often critical for optimizing performance

Question: 186 CertyIQ

HOTSPOT
-

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 Area

On the servers, install the:
- Azure Connected Machine agent
- Log Analytics agent
- Microsoft Dependency agent

Configure custom log settings by using the:
- Data connectors page of Microsoft Sentinel
- Log Analytics workspace settings of Microsoft Sentinel
- Logs blade of Microsoft Sentinel

Answer:

Answer Area

On the servers, install the: Log Analytics agent

Configure custom log settings by using the: Data connectors page of Microsoft Sentinel

Question: 187 CertyIQ

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 Data Collection Rule (DCR).
C. Modify the properties of the connector.
D. Create a scheduled query rule.

Answer: D

Explanation:

D is correct: https://learn.microsoft.com/en-us/azure/sentinel/customize-alert-details

Question: 188 CertyIQ

You have a Microsoft Sentinel workspace named Workspace1 and 200 custom Advanced Security Information Model (ASIM) parsers based on the DNS schema.

You need to make the 200 parses available in Workspace1. The solution must minimize administrative effort.

What should you do first?

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

Answer: D

Explanation:

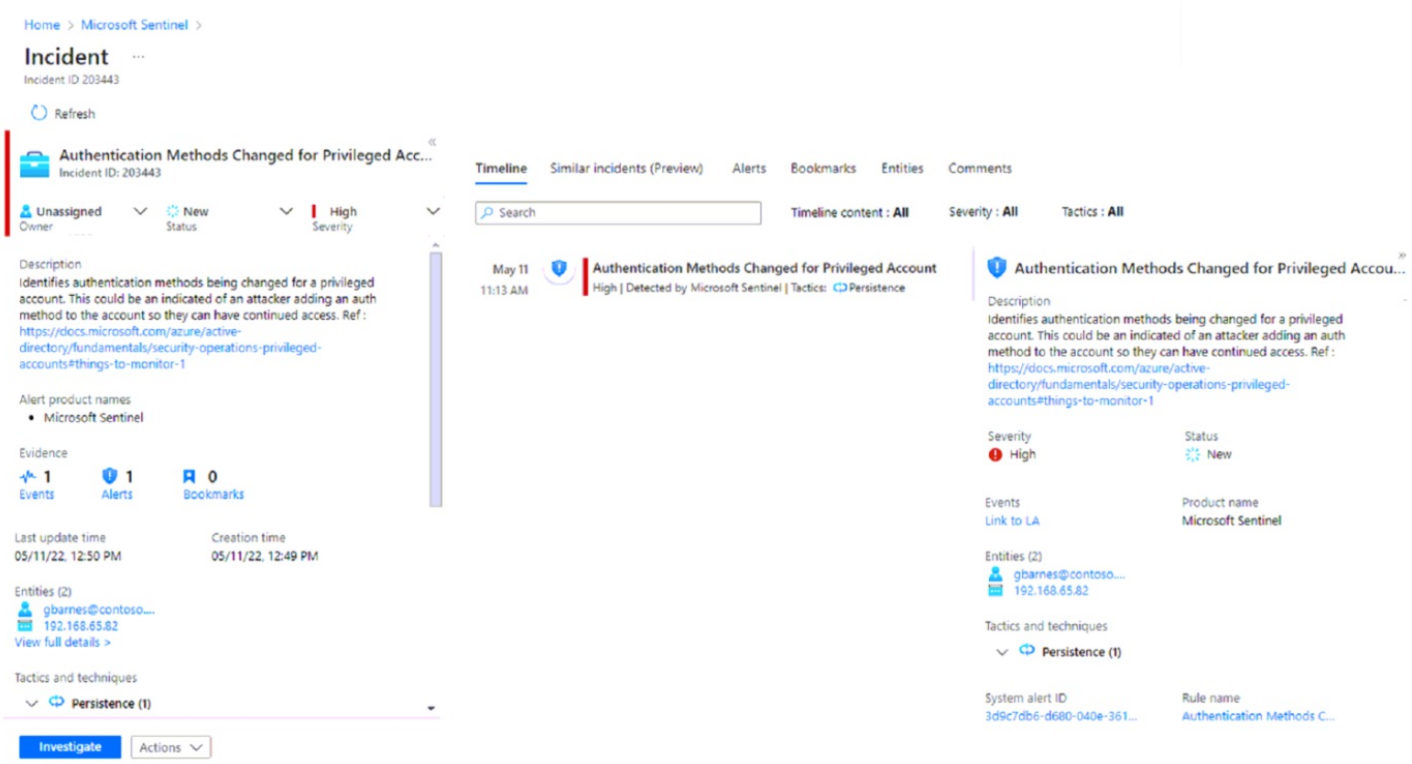
D is correct for a large number of parsers: https://learn.microsoft.com/en-us/azure/sentinel/normalization-develop-parsers#deploy-parsers

Question: 189 CertyIQ

HOTSPOT
-

You have a Microsoft Sentinel workspace.

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



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

NOTE: Each correct selection is worth one point.

Answer Area

A map of the entities connected to the alert can be viewed by selecting

- Alerts
- Entities
- Investigate

A list of the activities performed during the investigation can be viewed by selecting

- Alerts
- Bookmarks
- Comments
- Status

Answer:

Answer Area

A map of the entities connected to the alert can be viewed by selecting

A list of the activities performed during the investigation can be viewed by selecting

Explanation:

Investigate,Alerts

https://learn.microsoft.com/en-us/azure/sentinel/investigate-cases

Question: 190 CertyIQ

DRAG DROP
-

Case study
-

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
-

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

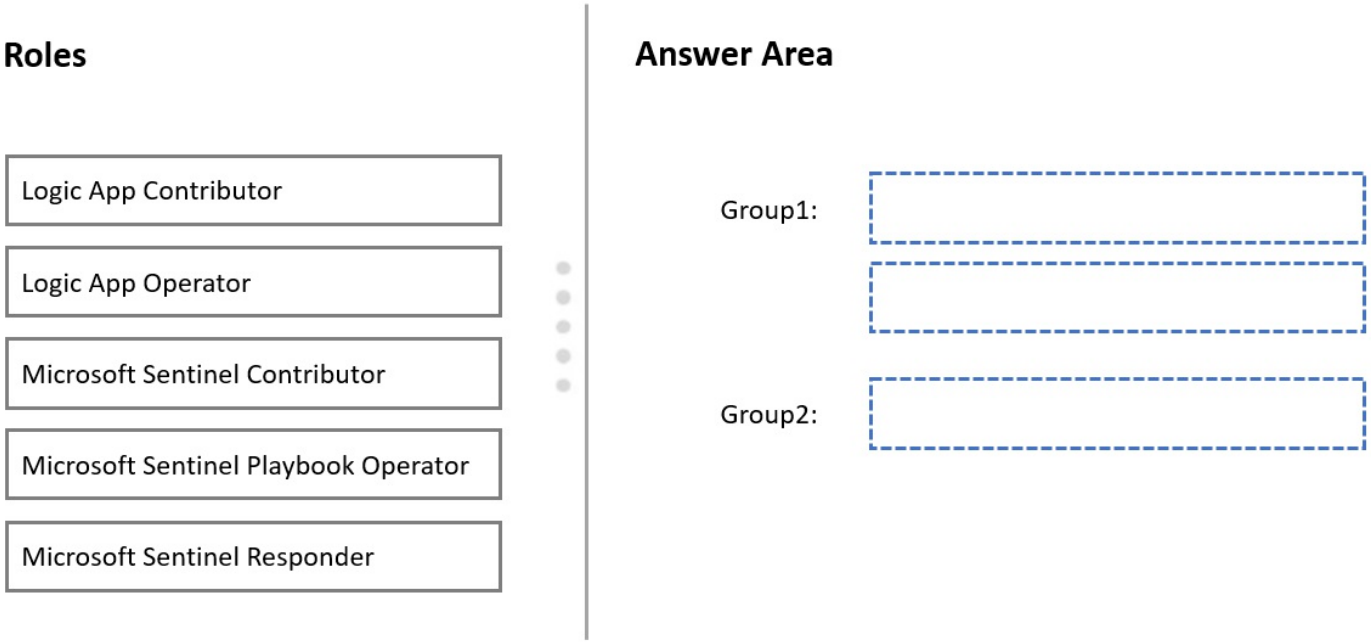
Fabrikam identifies the following Microsoft Sentinel requirements:

•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.

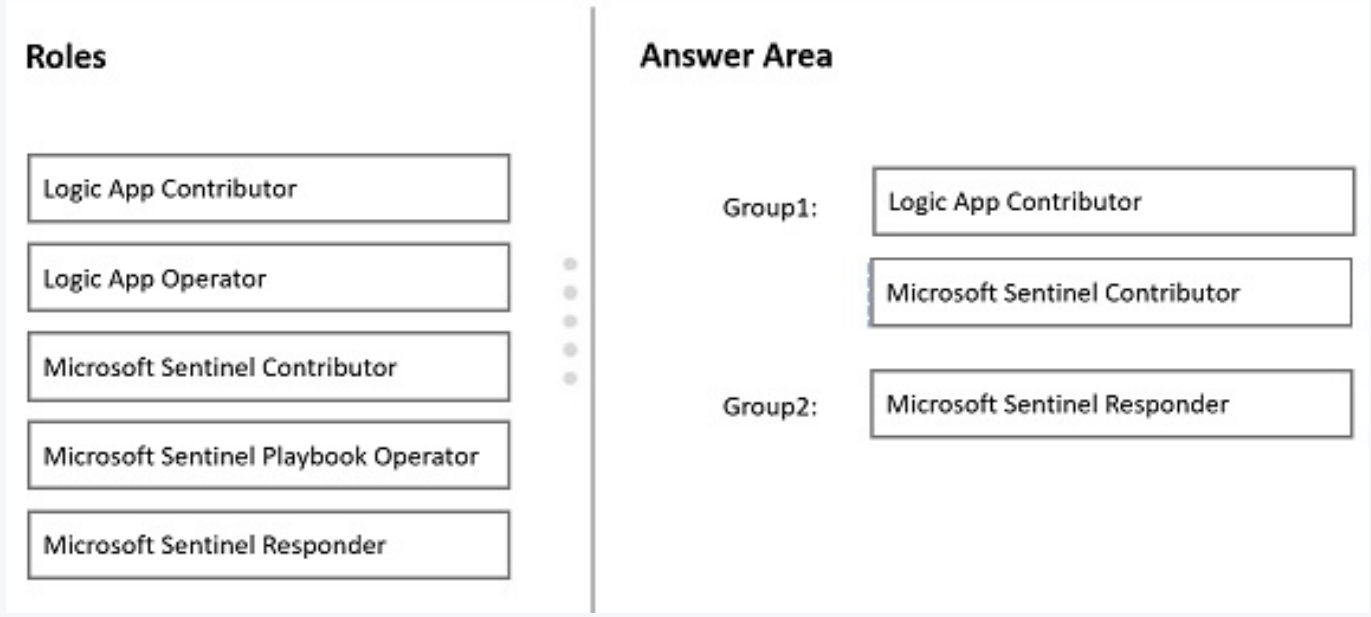
You need to assign role-based access control (RBAC) roles to Group1 and Group2 to meet the Microsoft Sentinel requirements and the business requirements.

Which role should you assign to each group? To answer, drag the appropriate roles to the correct groups. 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:

1- Logic App Contributor, Microsoft Sentinel Contributor2- Microsoft Sentinel Responder

Question: 191

CertyIQ

Case study -

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 -

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.IdentityInfo

B.AADRiskyUsers

C.SentinelAudit

D.IdentityDirectoryEvents

Answer: A

Explanation:

Identity Info

Question: 192 CertyIQ

Case study -

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 -

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 meet the Microsoft Sentinel requirements for App1.

What should you configure for App1?

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

Answer: A

Explanation:

a trigger

Question: 193 CertyIQ

Case study -

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 -

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 ensure that you can run hunting queries to meet the Microsoft Sentinel requirements.

Which type of workspace should you create?

A.Azure Synapse Analytics
B.Azure Machine Learning
C.Log Analytics
D.Azure Databricks

Answer: B

Explanation:

PrerequisitesAn Azure subscription. If you don't have an Azure subscription, create a free account before you begin.A Machine Learning workspace. See Create workspace resources.Your user identity must have access to your workspace's default storage account. Whether you can read, edit, or create notebooks depends on your access level to your workspace. For example, a Contributor can edit the notebook, while a Reader could only view it.

Question: 194 CertyIQ

Case study -

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 -

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: C

Explanation:

C. Security Operations Efficiency

https://learn.microsoft.com/en-us/azure/sentinel/manage-soc-with-incident-metrics

Question: 195 CertyIQ

HOTSPOT
-

Case study
-

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 conta`in 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
-

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:

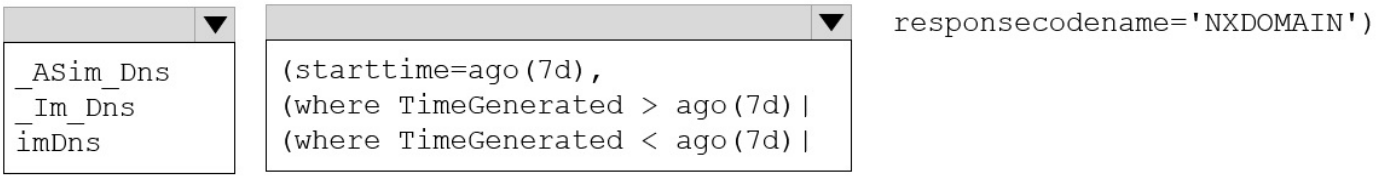
•Query for NXDOMAIN DNS requests from the last seven days by using built-in Advanced Security Information Model (ASIM) unifying parsers.
•From AWS EC2 instances, collect Windows Security event log entries that include local group membership changes.
•Identify anomalous activities of Azure AD users by 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 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.

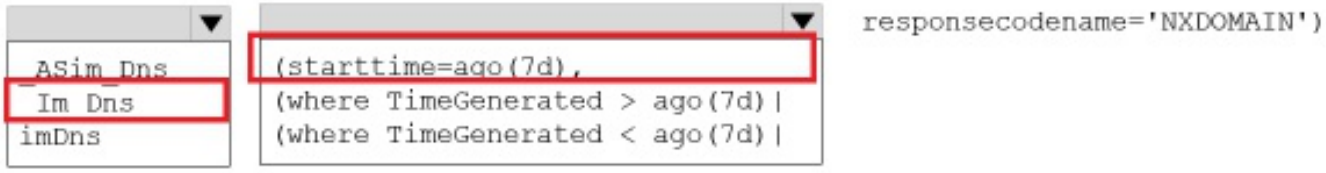
Answer Area




```
| summarize count() by SrcIpAddr, bin(TimeGenerated,15m)
```

Answer:

Answer Area




```
| summarize count() by SrcIpAddr, bin(TimeGenerated,15m)
```

Explanation:

Box1: _Im_DnsBox2: (starttime=ago)(7d),

Question: 196 CertyIQ

HOTSPOT
-

Case study
-

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 conta`in 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
-

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.

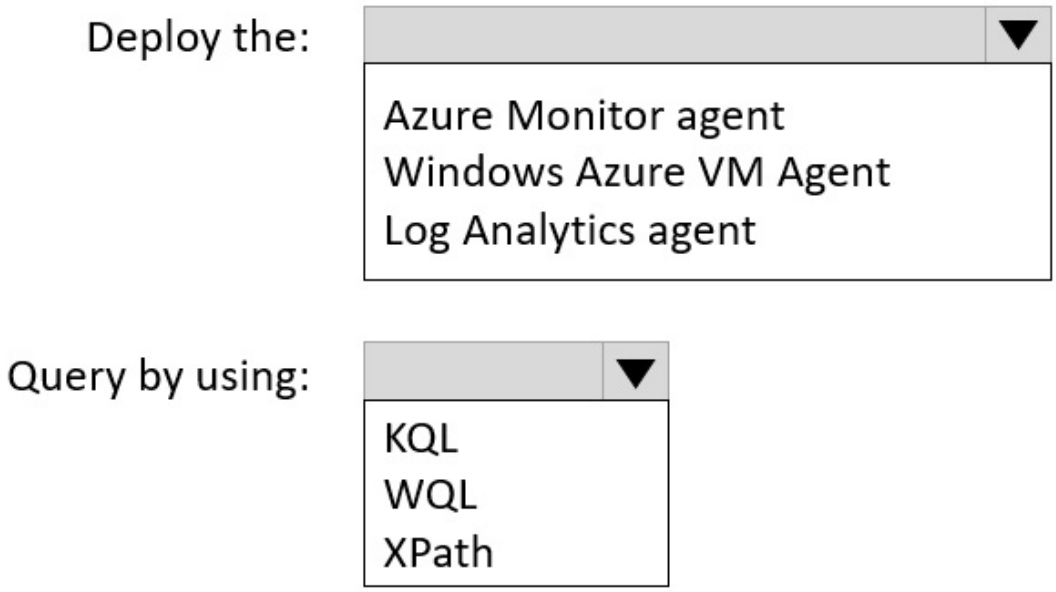
•Identify the mean time to triage for incidents generated during the last 30 days.
•Identify the mean time to close incidents generated during the last 30 days.
•Ensure that the members of Group1 can create and run playbooks.
•Ensure that the members of Group1 can manage analytics rules.
•Run hunting 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 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.

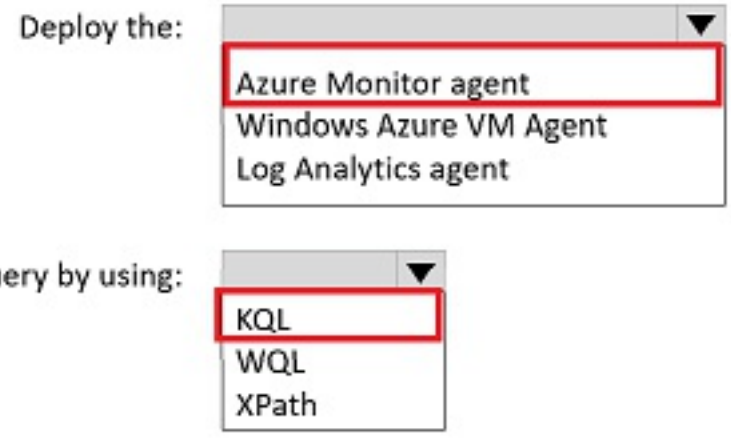
NOTE: Each correct selection is worth one point.

Answer Area



Answer:

Answer Area



Explanation:

Azure Monitoring Agent and KQL.

Question: 197 CertyIQ

HOTSPOT
-

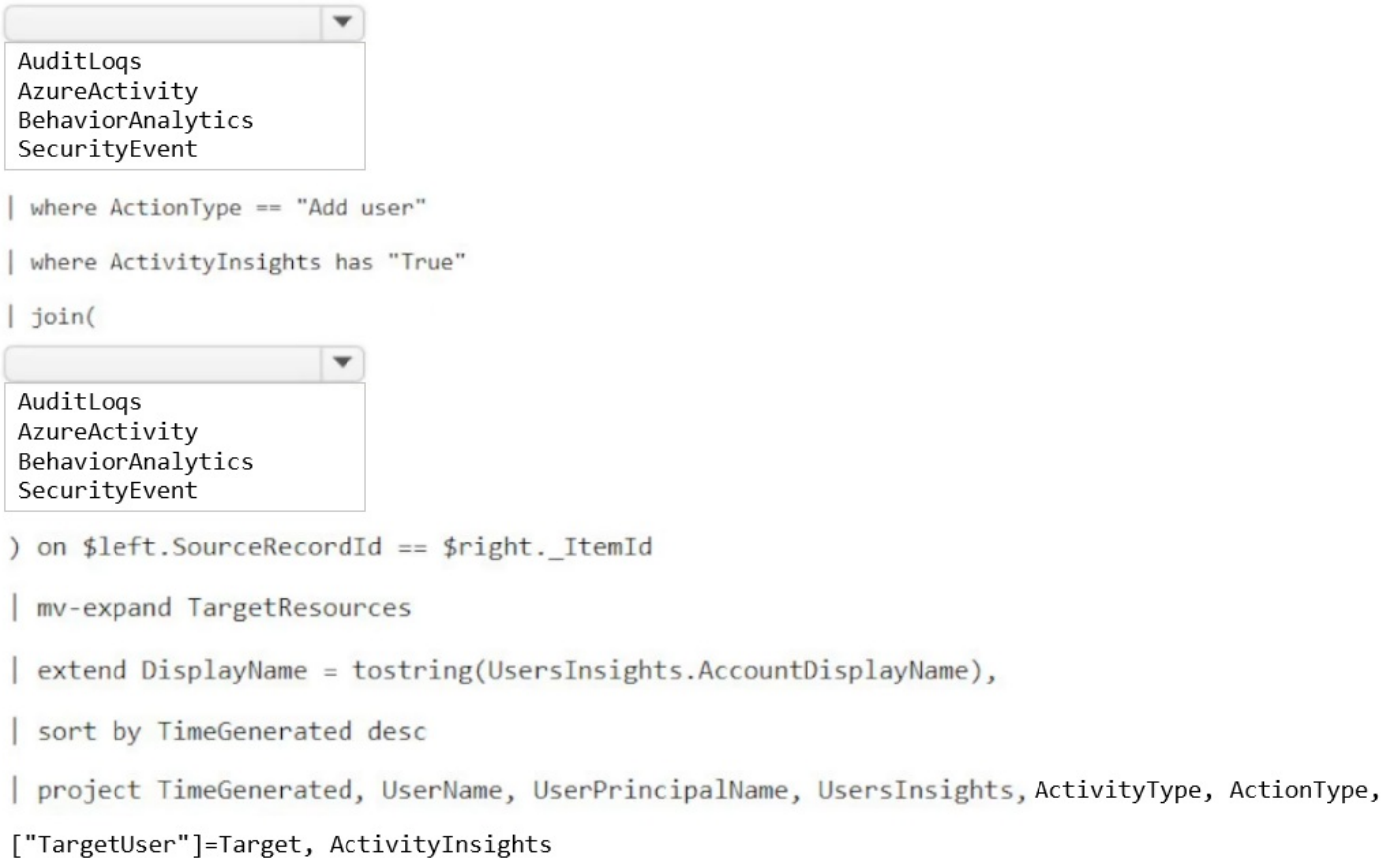
You have a Microsoft Sentinel workspace named sws1.

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

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

NOTE: Each correct selection is worth one point.

Answer Area



Answer:

Explanation:

AuditLogs BehaviorAnalytics

Question: 198 CertyIQ

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

You need to create a new near-real-time (NRT) analytics rule that will use the playbook.

What should you configure for the rule?

A.the incident automation settings
B.the query rule
C.entity mapping
D.the Alert automation settings

Answer: B

Explanation:
1. the answer is B. the query rule.To create an NRT rule, you need to follow these steps:From the Microsoft Sentinel navigation menu, select Analytics.Select Create from the button bar, then NRT query rule (preview) from the drop-down list.Follow the instructions of the analytics rule wizard.

Question: 199 CertyIQ

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

Explanation:

A. notebooks in Microsoft Sentinel. 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.

Question: 200 CertyIQ

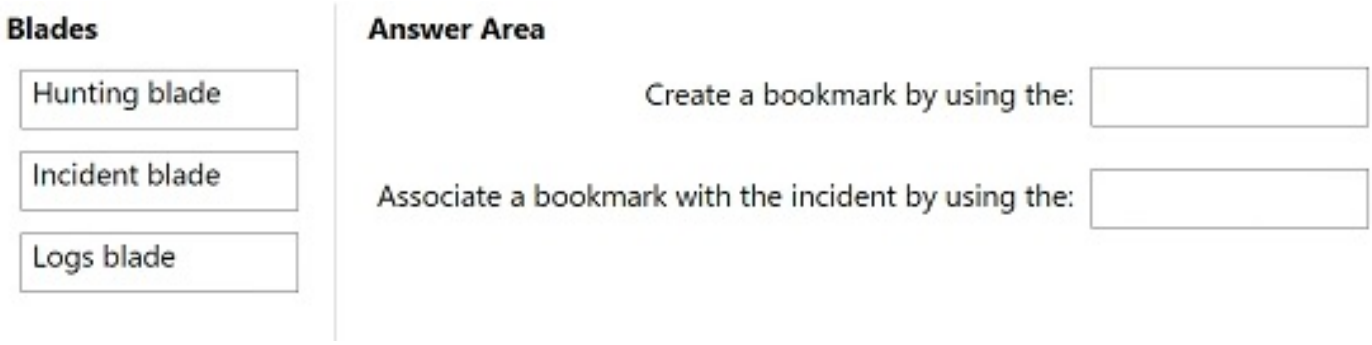
DRAG DROP
-

You have a Microsoft Sentinel workspace that contains an Azure AD data connector.

You need to associate a bookmark with an Azure AD-related incident.

What should you do? To answer, drag the appropriate blades to the correct tasks. Each blade 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:

Creating a bookmark by using the = hunting blade

Associate a bookmark with incident by using the = hunting blade

Question: 201 CertyIQ

HOTSPOT
-

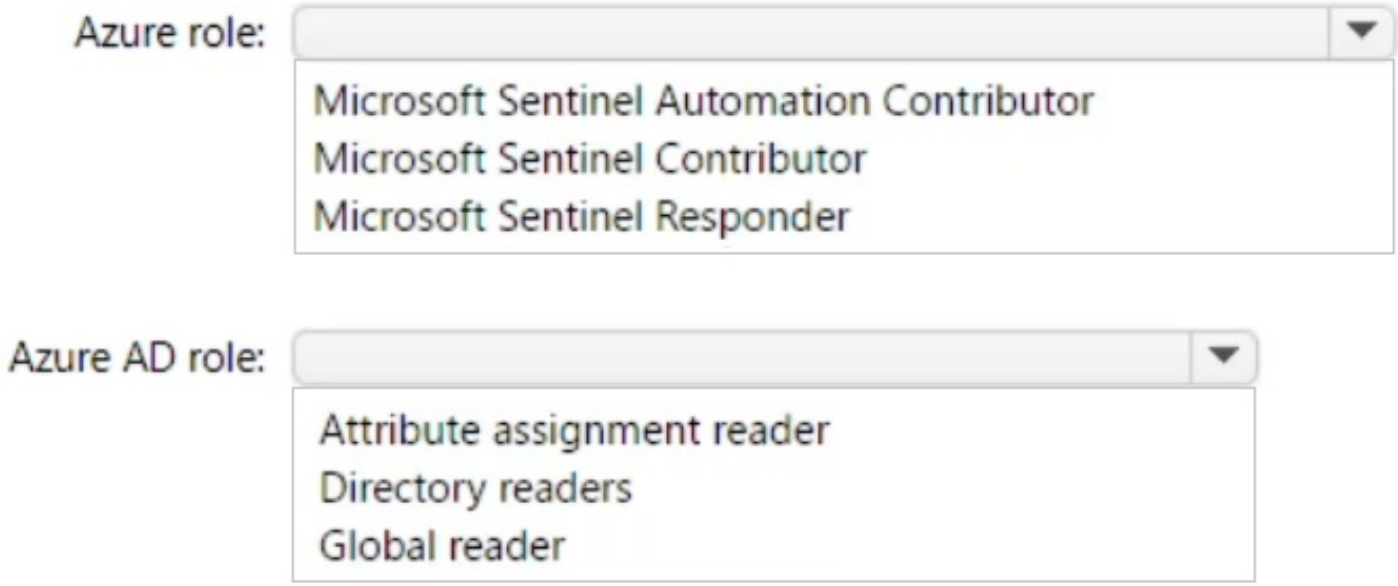
You have an Azure subscription that contains a guest user named User1 and a Microsoft Sentinel workspace named workspace1.

You need to ensure that User1 can triage Microsoft Sentinel incidents in workspace1. The solution must use the principle of least privilege.

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

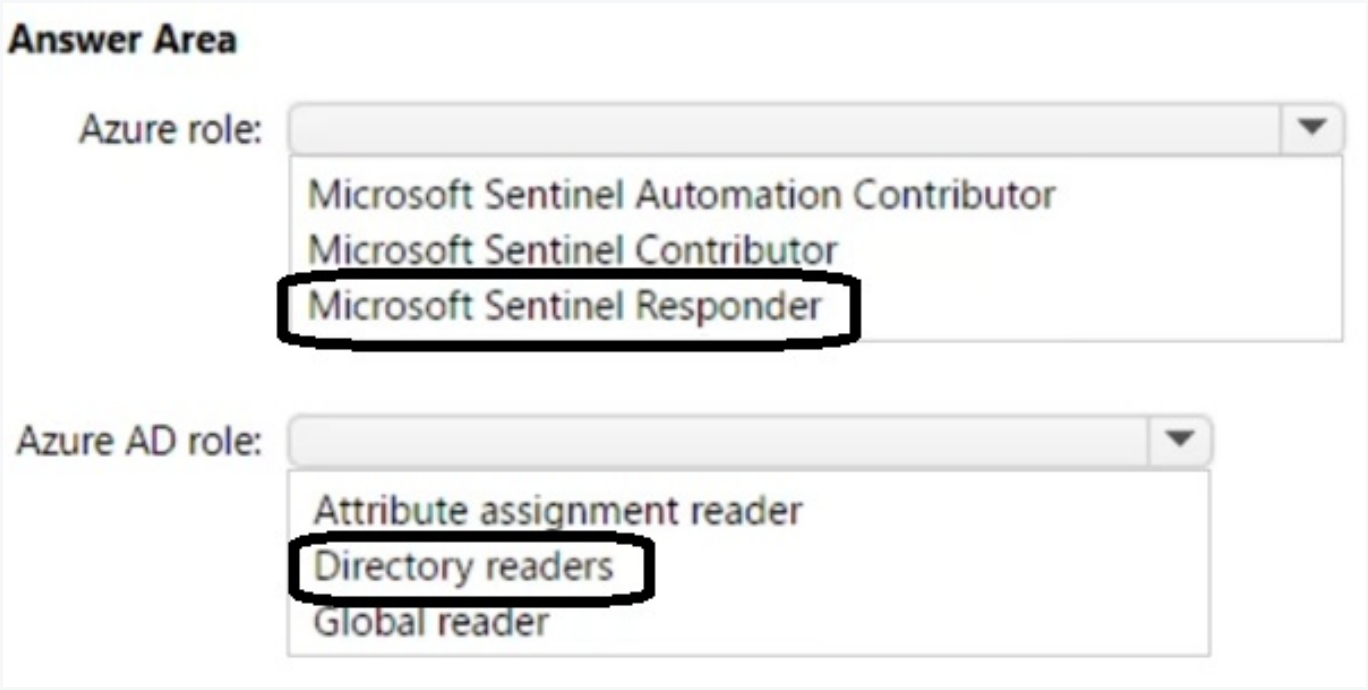
NOTE: Each correct selection is worth one point.

Answer Area



Answer:

Answer Area



Question: 202

CertyIQ

HOTSPOT

-

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

Question: 203

CertyIQ

HOTSPOT
-

You have an Azure subscription that contains the following resources:

•A virtual machine named VM1 that runs Windows Server
•A Microsoft Sentinel workspace named Sentinel1 that has User and Entity Behavior Analytics (UEBA) enabled

You have a scheduled query rule named Rule1 that tracks sign-in attempts to VM1.

You need to update Rule1 to detect when a user from outside the IT department of your company signs in to VM1. The solution must meet the following requirements:

•Utilize UEBA results.
•Maximize query performance.
•Minimize the number of false positives.

How should you complete the rule definition? 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", "4625")
| where Computer == "VM1"
| join kind = [ ▼ ] (
```

anti
fullouter
inner

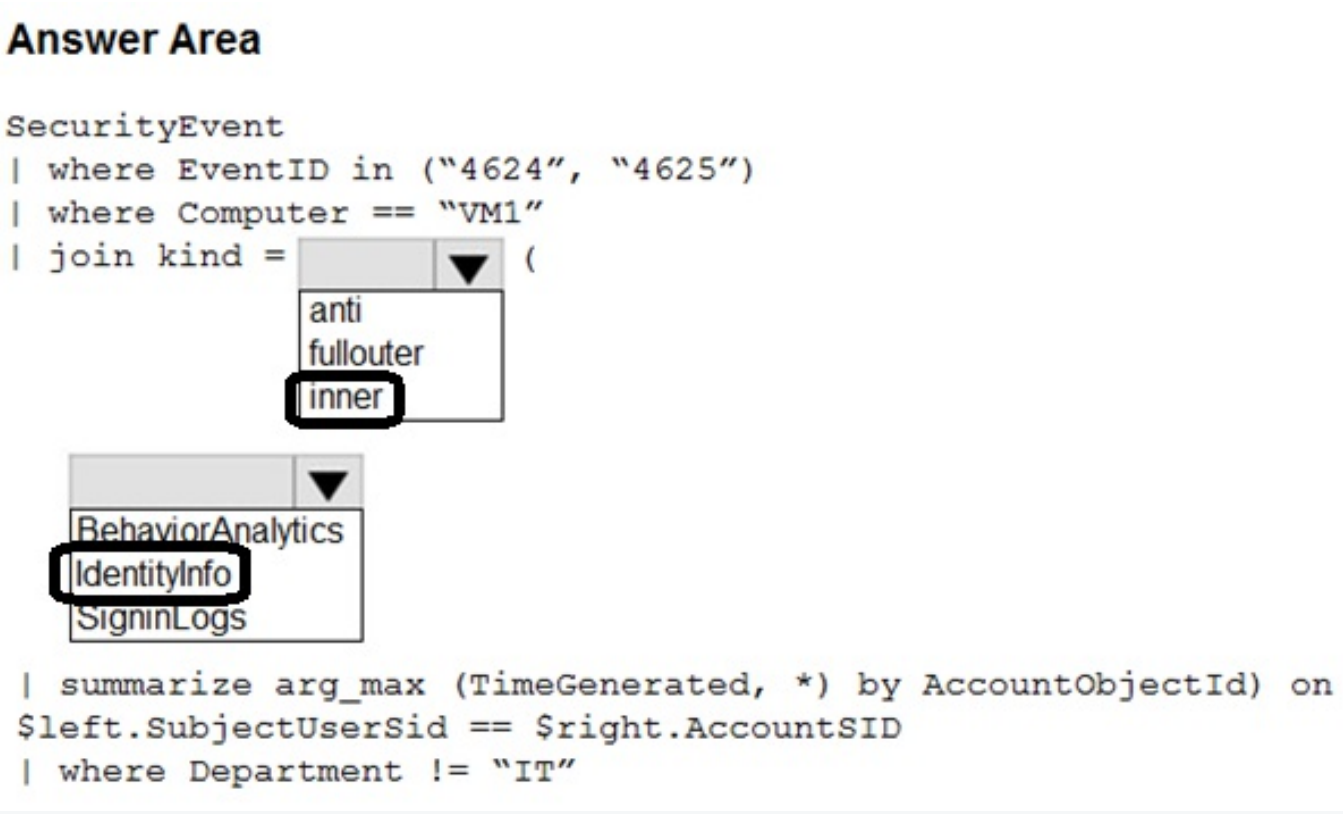
[▼]

BehaviorAnalytics
IdentityInfo
SigninLogs

```
| summarize arg_max (TimeGenerated, *) by AccountObjectId) on
$left.SubjectUserSid == $right.AccountSID
| where Department != "IT"
```

Answer:

Answer Area



Explanation:

SecurityEvent| where EventID in ("4624","4672")| where Computer == "My.High.Value.Asset"| join kind=inner (IdentityInfo| summarize arg_max(TimeGenerated, *) by AccountObjectId) on $left.SubjectUserSid == $right.AccountSID| where Department != "IT"https://learn.microsoft.com/en-us/azure/sentinel/investigate-with-ueba#embed-identityinfo-data-in-your-analytics-rules-public-preview

Question: 204 CertyIQ

DRAG DROP
-

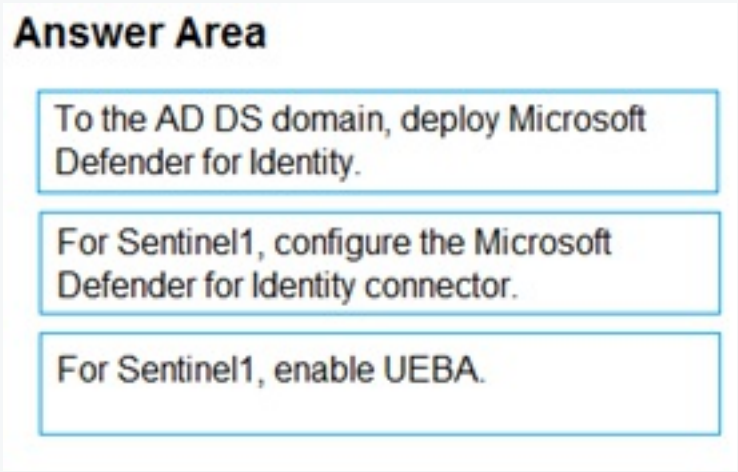
Your network contains an on-premises Active Directory Domain Services (AD DS) domain that syncs with an Azure AD tenant.

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:



Question: 205

CertyIQ

You have a Microsoft Sentinel workspace.

You enable User and Entity Behavior Analytics (UEBA) 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:
•Sign-in URL: https://www.company.com

Which entities can be investigated by using UEBA?

A.IP address and email address only

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

C.IP address only

D.used client app and app name only

Answer: B

Explanation:

B. app name, computer name, IP address, email address, and used client app only. These are all entities that can be investigated by using UEBA in Microsoft Sentinel.

Question: 206 CertyIQ

HOTSPOT
-

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

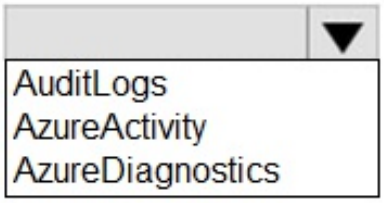
You need to create a hunting query using Kusto Query Language (KQL) that meets the following requirements:

•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.

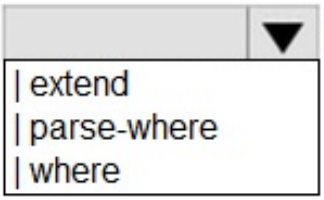
How should you complete the query? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area



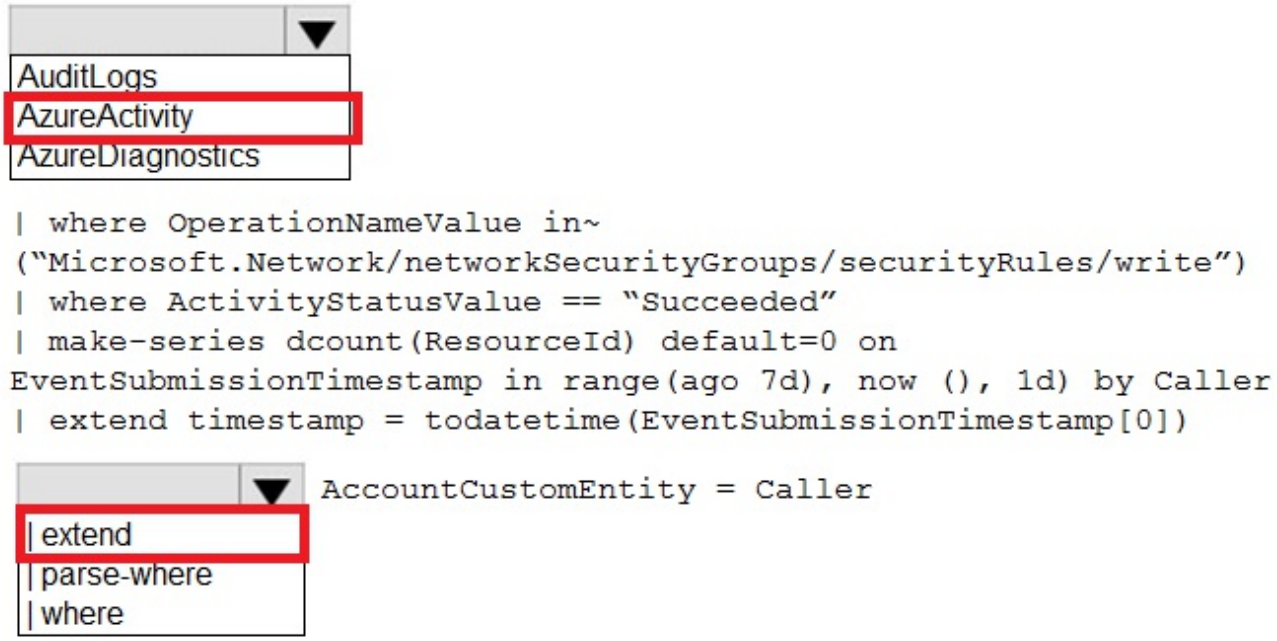

```
| where OperationNameValue in~
("Microsoft.Network/networkSecurityGroups/securityRules/write")
| where ActivityStatusValue == "Succeeded"
| make-series dcount(ResourceId) default=0 on
EventSubmissionTimestamp in range(ago 7d), now (), 1d) by Caller
| extend timestamp = todatetime(EventSubmissionTimestamp[0])
```




```
AccountCustomEntity = Caller
```

Answer:

Answer Area



Explanation:

Azure Activity

extend

Question: 207 CertyIQ

HOTSPOT
-

You have a Microsoft Sentinel workspace.

You need to configure a report visual for a custom workbook. The solution must meet the following requirements:
•The count and usage trend of AppDisplayName must be included.
•The TrendList column must be useable in a sparkline visual.

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

```
SigninLogs
| where ResultType == 0 and AppDisplayName != ""
| summarize count() by AppDisplayName
| [ ▼ ] (
    join
    let
    lookup
    mv-expand
SigninLogs
| [ ▼ ] TrendList = count() on TimeGenerated in range
    make_bag()                ({TimeRange:start}, {TimeRange:end}, 4h) by
    make-series               AppDisplayName
    mv-expand
    render
) on AppDisplayName
| top 10 by count_desc
```

Answer:

Answer Area

```
SigninLogs
| where ResultType == 0 and AppDisplayName != ""
| summarize count() by AppDisplayName
| [ ▼ ] (
    join
    let
    lookup
    mv-expand
SigninLogs
| [ ▼ ] TrendList = count() on TimeGenerated in range
    make_bag()                ({TimeRange:start}, {TimeRange:end}, 4h) by
    make-series               AppDisplayName
    mv-expand
    render
) on AppDisplayName
| top 10 by count_desc
```


Question: 208

CertyIQ

DRAG DROP

-

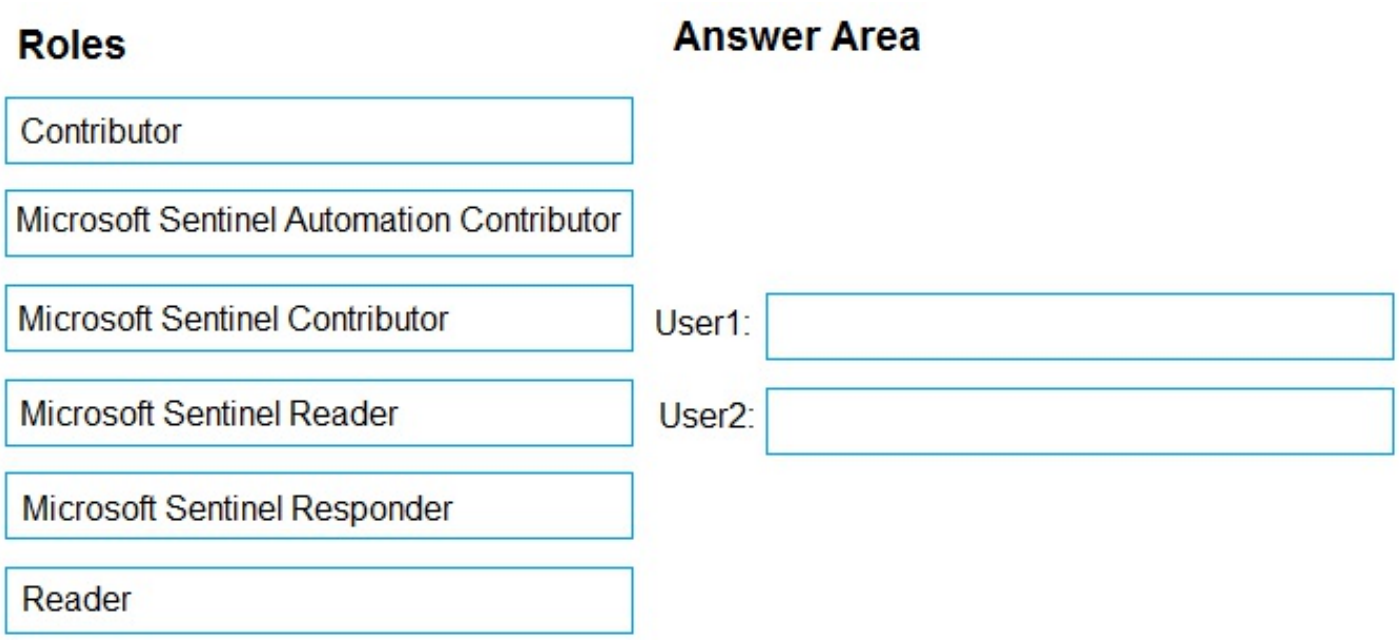
You have an Azure subscription that contains two users named User1 and User2 and a Microsoft Sentinel workspace named workspace1.

You need to ensure that the users can perform the following tasks in workspace1:
•User1 must be able to dismiss incidents and assign incidents to users.
•User2 must be able to modify analytics rules.

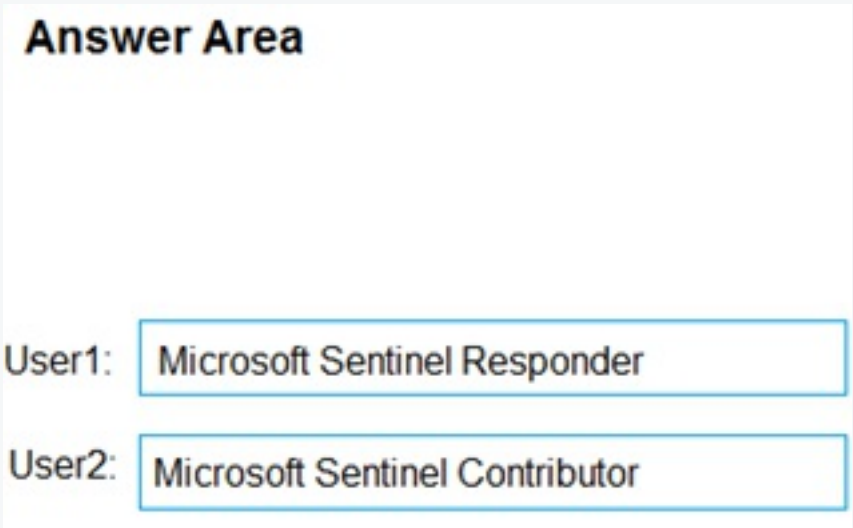
The solution must use the principle of least privilege.

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.

NOTE: Each correct selection is worth one point.



Answer:



Explanation:

user1=MS responder; user2=MS contributor

https://learn.microsoft.com/en-us/azure/sentinel/roles

Question: 209 CertyIQ

You have a Microsoft Sentinel workspace that uses the Microsoft 365 Defender data connector.

From Microsoft Sentinel, you investigate a Microsoft 365 incident.

You need to update the incident to include an alert generated by Microsoft Defender for Cloud Apps.

What should you use?

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

Answer: D

Explanation:
1. D. the Alerts page in the Microsoft 365 Defender portal.Open the Microsoft 365 Defender portal and select Alerts.Find the alert that you want to add to the incident and select it.In the alert details page, select Add to existing incident.In the Add alert to incident pane, select the incident that you want to update and then select Add.This will add the alert to the incident in both Microsoft 365 Defender and Microsoft Sentinel portals. Any changes you make to the incident in Microsoft 365 Defender will be synchronized to the same incident in Microsoft Sentinel

Question: 210 CertyIQ

You have a Microsoft Sentinel workspace.

You investigate an incident that has the following entities:
•A user account named User1
•An IP address of 192.168.10.200
•An Azure virtual machine named VM1
•An on-premises server named Server1

You need to label an entity as an indicator of compromise (IoC) directly by using the incidents page.

Which entity can you label?

A.192.168.10.200
B.VM1
C.Server1
D.User1

Answer: A

Explanation:

you can label an entity as an indicator of compromise (IoC) directly by using the incidents page in Microsoft Sentinel if the entity is one of the following types: domain name, IP address, URL, or file. Therefore, the correct answer is A. 192.168.10.200, since it is an IP address and the other entities are not of the supported types.

Question: 211 CertyIQ

You have a Microsoft Sentinel workspace that has User and Entity Behavior Analytics (UEBA) enabled for Signin Logs.

You need to ensure that failed interactive sign-ins are detected. The solution must minimize administrative effort.

What should you use?

A.a scheduled alert query
B.the Activity Log data connector
C.a UEBA activity template
D.a hunting query

Answer: C

Explanation:

Correct answer is C:a UEBA activity template.

Question: 212 CertyIQ

HOTSPOT
-

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 and configure UEBA to use data collected from Active Directory Domain Services (AD DS).

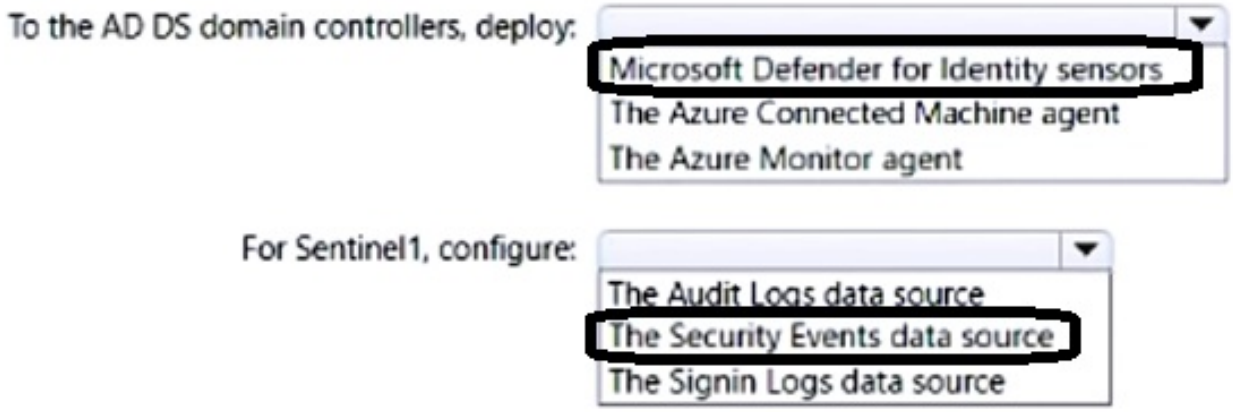
What should you do? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Answer:

Answer Area



Question: 213 CertyIQ

HOTSPOT
-

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

You need to query the number of daily security alerts. The solution must meet the following requirements:

•Identify alerts that occurred during the last 30 days.
•Display the results in a timechart.

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

NOTE: Each correct selection is worth one point.

Answer Area

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

Answer:

Answer Area

```
SecurityAlert
| where TimeGenerated >= ago(30d)
|  count() by ProviderName,  (TimeGenerated, 1d)
| render timechart
```

lookup / project / summarize

bin / make series / range

Question: 214 CertyIQ

HOTSPOT
-

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.

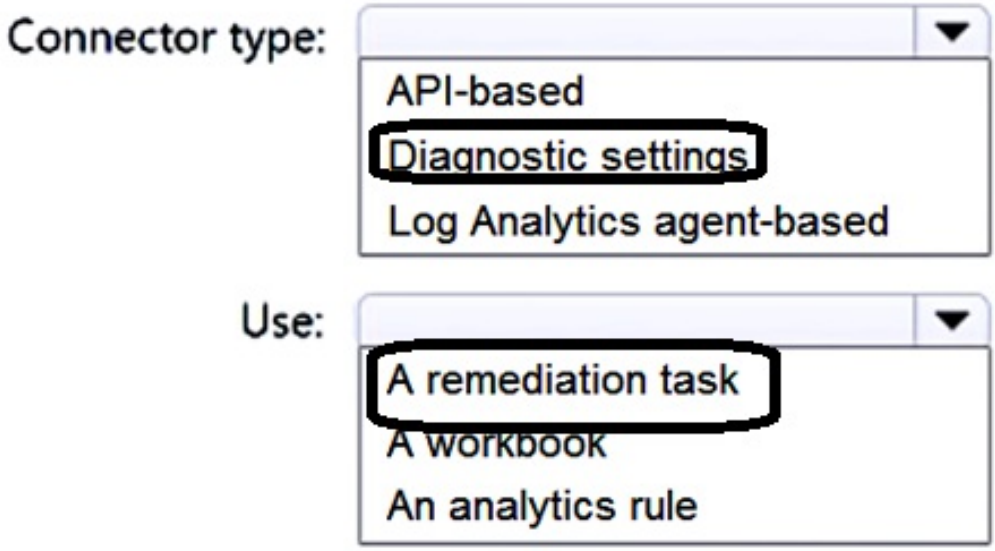
Answer Area

Connector type:
- API-based
- Diagnostic settings
- Log Analytics agent-based

Use:
- A remediation task
- A workbook
- An analytics rule

Answer:

Answer Area



Explanation:

https://learn.microsoft.com/en-us/azure/sentinel/connect-services-diagnostic-setting-based

Question: 215 CertyIQ

You have 50 Microsoft Sentinel workspaces.

You need to view all the incidents from all the workspaces on a single page in the Azure portal. The solution must minimize administrative effort.

Which page should you use in the Azure portal?

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

Answer: A

Explanation:

Correct answer is A) Microsoft Sentinel | Incidents, which allows you to view all incidents from all LA workspaces.

Question: 216 CertyIQ

Case study -

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 -

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 scheduled rule for incident generation based on rulequery1.

What should you configure first?

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

Answer: B

Explanation:

From Microsoft documentation after completing query: Alert enrichmentUse the Entity mapping configuration section to map parameters from your query results to Microsoft Sentinel-recognized entities. Entities enrich the rules' output (alerts and incidents) with essential information that serves as the building blocks of any investigative processes and remedial actions that follow. They are also the criteria by which you can group alerts together into incidents in the Incident settings tab.

Question: 217

CertyIQ

Case study -

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 -

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 ensure that the processing of incidents generated by rulequery1 meets the Microsoft Sentinel requirements.

What should you create first?

A.a playbook with an incident trigger

B.a playbook with an alert trigger

C.an Azure Automation rule

D.a playbook with an entity trigger

Answer: B

Explanation:

Correct answer is B:a playbook with an alert trigger.

Question: 218

CertyIQ

HOTSPOT
-

Case study
-

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
-

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:

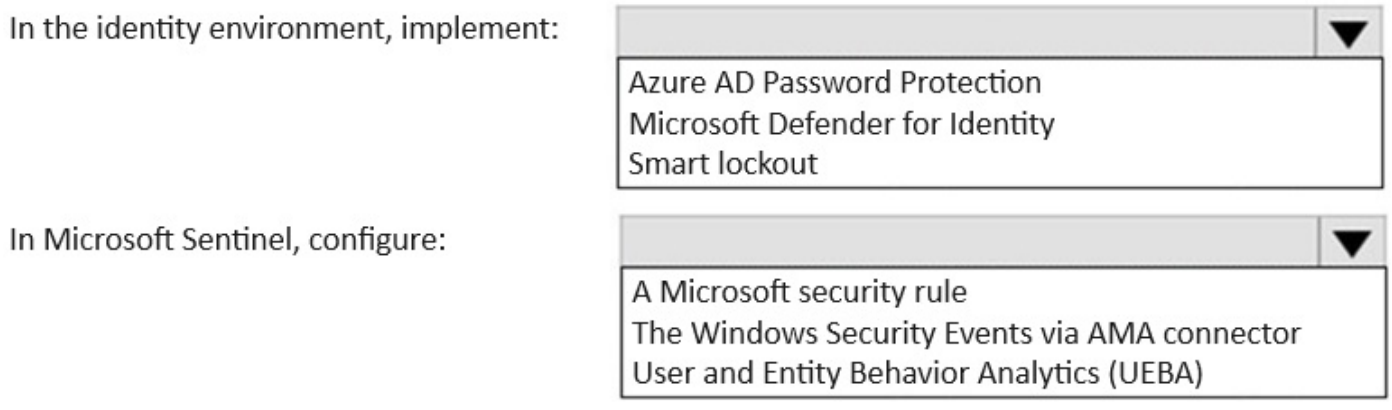
•Follow the principle of least privilege whenever possible.
•Minimize administrative effort whenever possible.

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

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

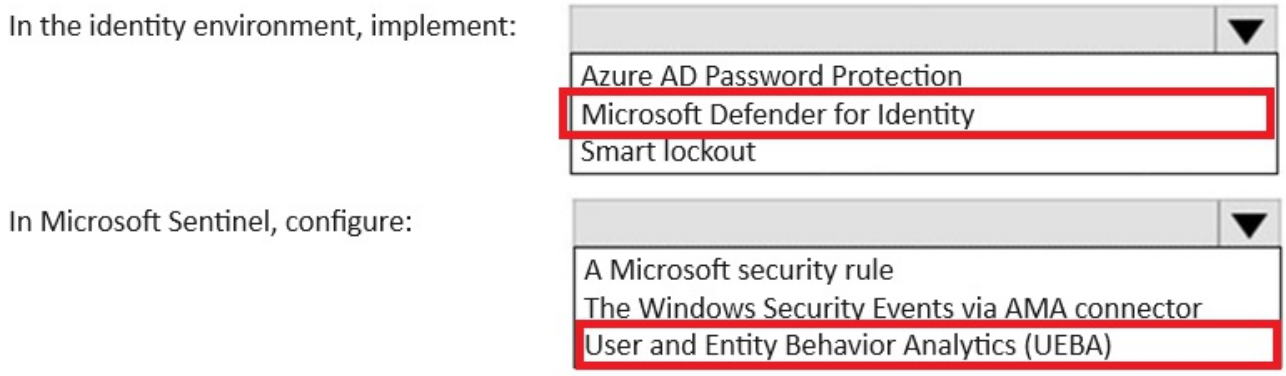
NOTE: Each correct selection is worth one point.

Answer Area



Answer:

Answer Area



Explanation:

Microsoft Defender for Identity and UEBA.

Defender for Identity: Monitor onpremises Domain logon activity or AD object changes

UEBA: Check for unusual patterns based on User Behaviour Analytics

Question: 219 CertyIQ

HOTSPOT
-

Case study
-

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
-

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:

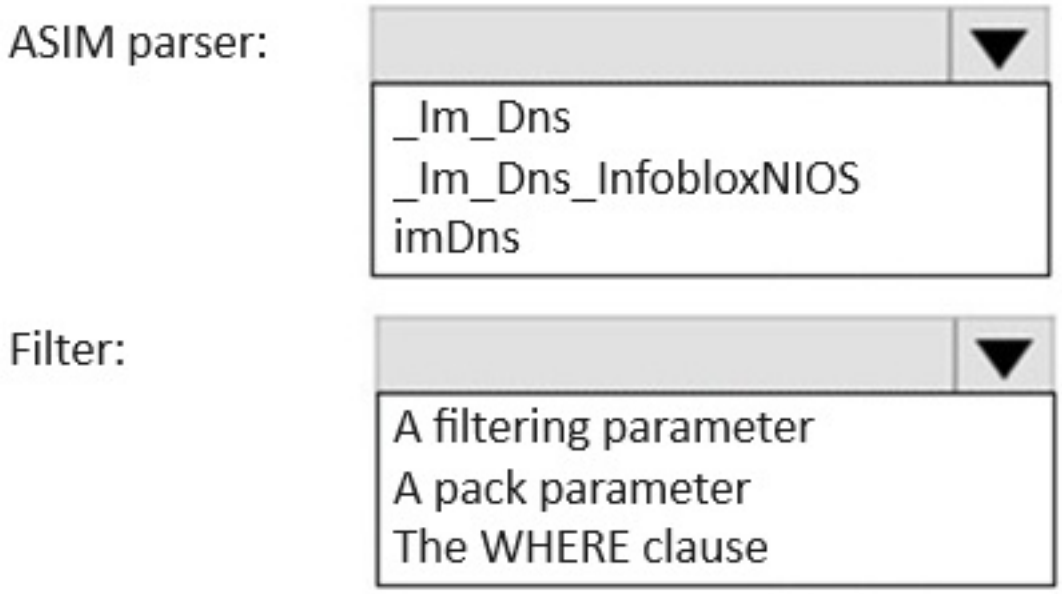
•Follow the principle of least privilege whenever possible.
•Minimize administrative effort whenever possible.

You need to implement the 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.

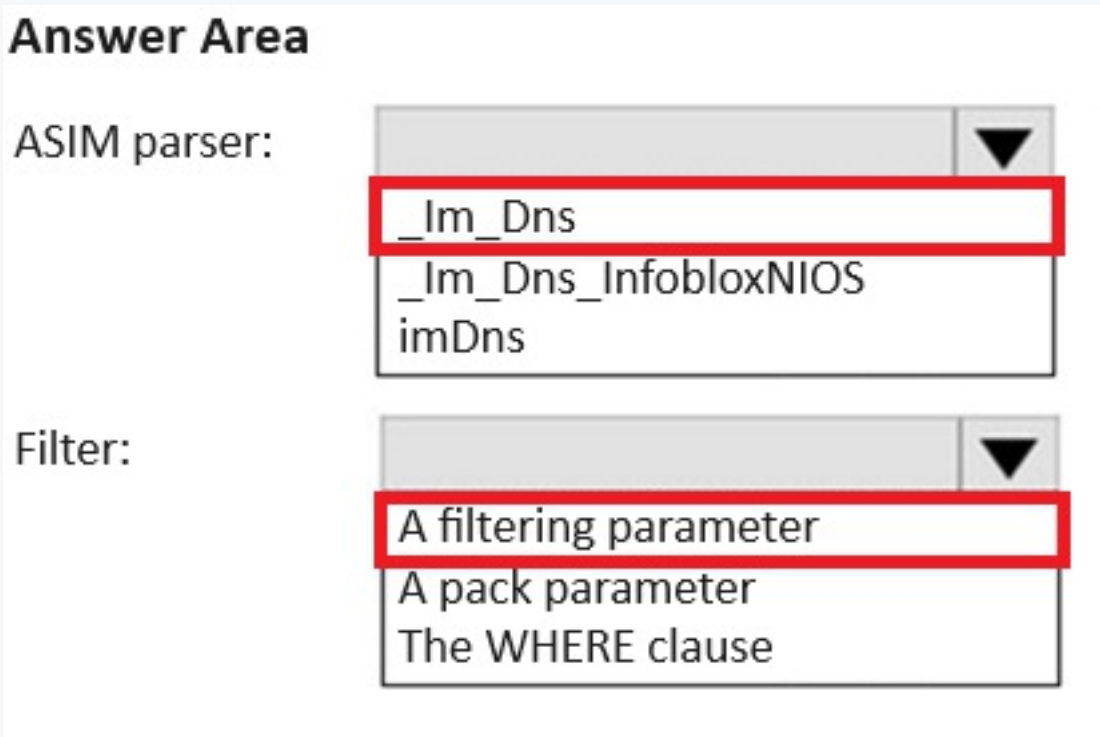
NOTE: Each correct selection is worth one point.

Answer Area



Answer:

Answer Area



Explanation:

_I m_ Dns

A filtering parameter

Reference:

https://learn.microsoft.com/en-us/azure/sentinel/normalization-about-parsers

Question: 220

CertyIQ

Case study -

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 -

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 configure event monitoring for Server1. The solution must meet the Microsoft Sentinel requirements.

What should you create first?

A.a Microsoft Sentinel automation rule
B.an Azure Event Grid topic
C.a Microsoft Sentinel scheduled query rule
D.a Data Collection Rule (DCR)

Answer: D

Explanation:

Correct answer is D:a Data Collection Rule (DCR).

Question: 221 CertyIQ

HOTSPOT
-

Case study
-

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
-

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.

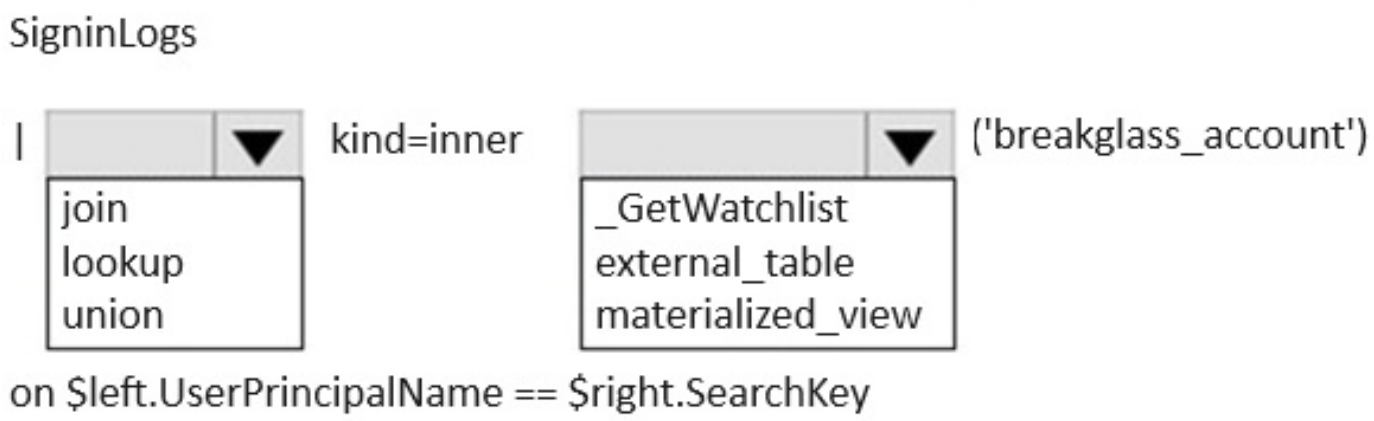
You need to implement the Microsoft Sentinel NRT rule for monitoring the designated break glass account. The

solution must meet the Microsoft Sentinel requirements.

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

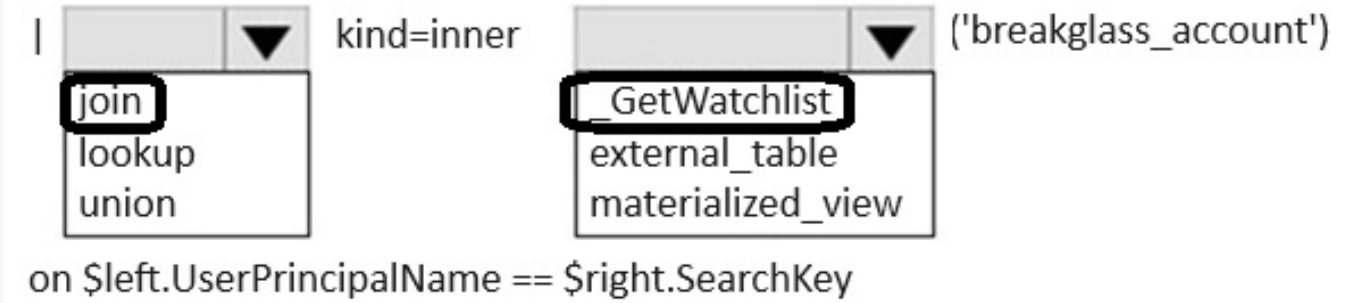
NOTE: Each correct selection is worth one point.

Answer Area



Answer:

Answer Area



Explanation:

JOIN

Get Watch List

Question: 222 CertyIQ

Case study -

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 -

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 ensure that the Group1 members can meet the Microsoft Sentinel requirements.

Which role should you assign to Group1?

A.Microsoft Sentinel Playbook Operator

B.Logic App Contributor

C.Automation Operator

D.Microsoft Sentinel Automation Contributor

Answer: B

Explanation:

Correct answer is B:Logic App Contributor.

Question: 223 CertyIQ

Case study -

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 -

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 ensure that the configuration of HuntingQuery1 meets the Microsoft Sentinel requirements.

What should you do?

A.Add HuntingQuery1 to a livestream.

B.Create a watchlist.

C.Create an Azure Automation rule.

D.Add HuntingQuery1 to favorites.

Answer: D

Explanation:

Correct answer: D. Favorites are automatically run when opening hunting page Ensure that HuntingQuery1 runs automatically when the Hunting page of Microsoft Sentinel in the Azure portal is accessed.

Question: 224 CertyIQ

HOTSPOT
-

Case study
-

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
-

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:

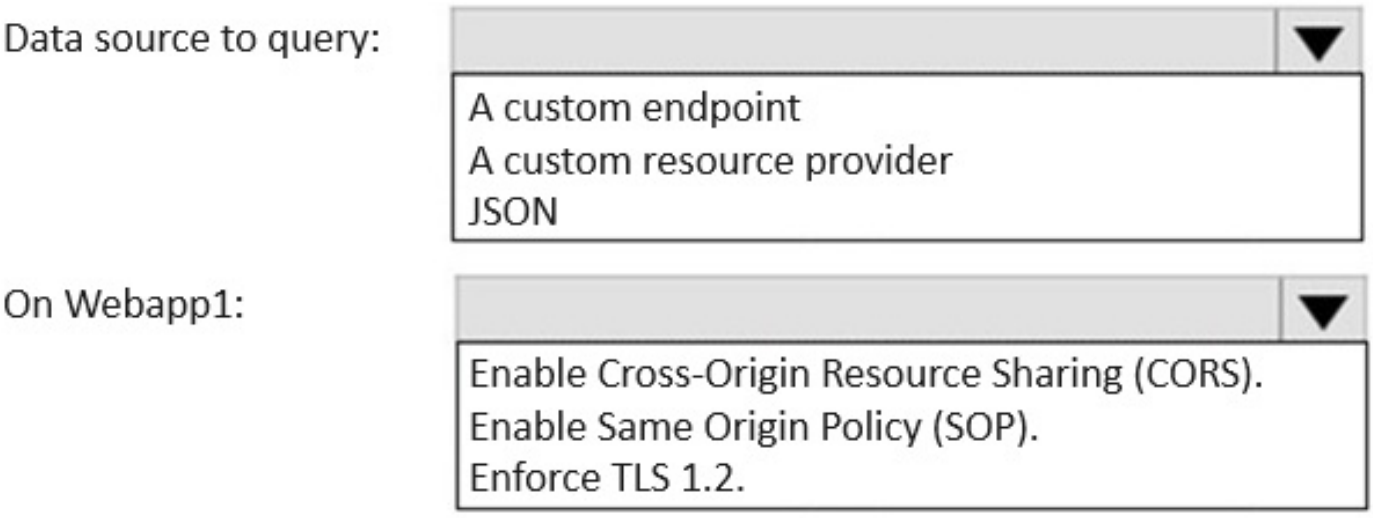
•Follow the principle of least privilege whenever possible.
•Minimize administrative effort whenever possible.

You need to implement the query for Workbook1 and Webapp1. The solution must meet the Microsoft Sentinel requirements.

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

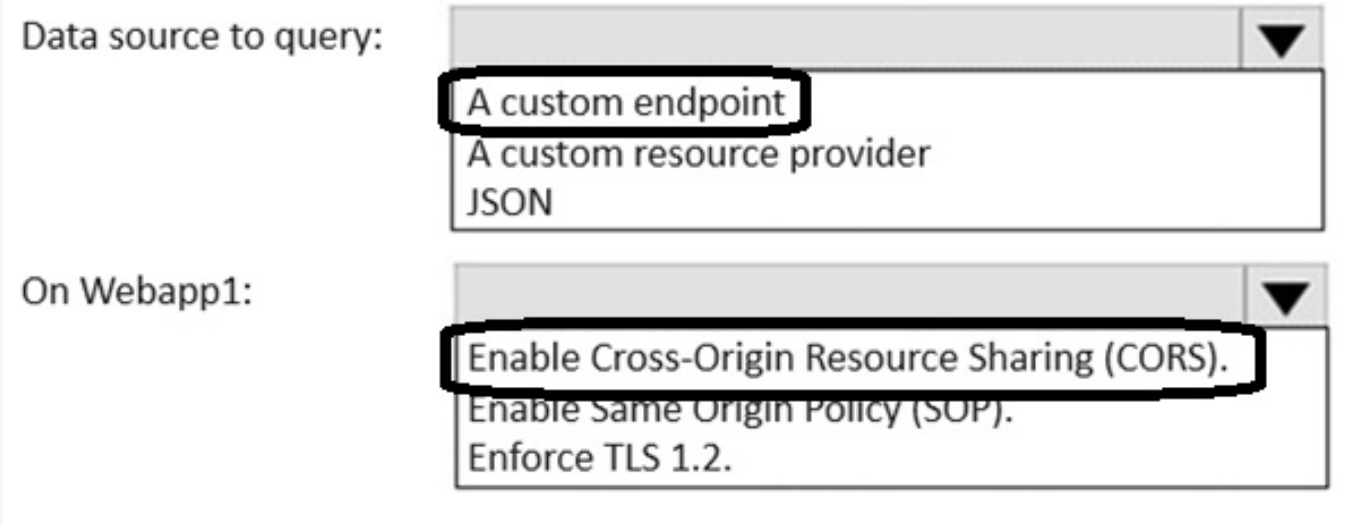
NOTE: Each correct selection is worth one point.

Answer Area



Answer:

Answer Area



Explanation:

A Custom endpoint and "CORS"

https://learn.microsoft.com/en-us/azure/azure-monitor/visualize/workbooks-data-sources#custom-endpoint

Question: 225

CertyIQ

The issue for which team can be resolved by using Microsoft Defender for Endpoint?

A.executive
B.sales
C.marketing

Answer: B

Explanation:

Correct - Sales need iOS EndPoint Protection from DfE

Reference:

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

Question: 226 CertyIQ

The issue for which team can be resolved by using Microsoft Defender for Office 365?

A.executive
B.marketing
C.security
D.sales

Answer: B

Explanation:

If the marketing team at Contoso has experienced incidents in which vendors uploaded files that contain malware to SharePoint Online sites, Microsoft Defender for Office 365 could potentially be useful for helping to protect against these types of threats.

Reference:

https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/atp-for-spo-odb-and-teams?view=o365-worldwide

Question: 227 CertyIQ

HOTSPOT
-

You have a Microsoft Sentinel workspace that has a default data retention period of 30 days. The workspace contains two custom tables as shown in the following table.

Name	Table plan	Interactive retention	Total retention period
Table1	Basic	Default	Default
Table2	Analytics	Default	365

Each table ingested two records per day during the past 365 days.

You build KQL statements for use in analytic rules as shown in the following table.

Name	KQL statement
Query1	Table1 | where TimeGenerated >= ago(15) | summarize count()
Query2	Table2 | where TimeGenerated >= ago(120) | summarize count()
Query3	Table1 | where TimeGenerated >= ago(45)

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
For Query1 to return a value of 30, you must change Table plan to **Analytics**.	○	○
For Query2 to return a value of 240, you must change Total retention period to **120 days**.	○	○
For Query3 to return 90 rows, you must change Total retention period to **45 days**.	○	○

Answer:

Answer Area

Statements	Yes	No
For Query1 to return a value of 30, you must change Table plan to **Analytics**.	○	○
For Query2 to return a value of 240, you must change Total retention period to **120 days**.	○	○
For Query3 to return 90 rows, you must change Total retention period to **45 days**.	○	○

Explanation:

No

No

Yes

Question: 228

CertyIQ

HOTSPOT

-

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

You have the on-premises devices shown in the following table.

Name	Management state	Operating system
Device1	Onboarded to and managed by using Microsoft Defender for Endpoint	Windows Server 2022
Device2	Discovered by Microsoft Defender for Endpoint and unmanaged	Linux

You are preparing an incident response plan for devices infected by malware.

You need to recommend response actions that meet the following requirements:

•Block malware from communicating with and infecting managed devices.
•Do NOT affect the ability to control managed devices.

Which actions should you use for each device? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Device1:

- Isolate device only
- Initiate Automated Investigation only
- Contain device only
- Isolate device and Initiate Automated Investigation only
- Isolate device, Initiate Automated Investigation, and Contain device

Device2:

- Isolate device only
- Initiate Automated Investigation only
- Contain device only
- Isolate device and Initiate Automated Investigation only
- Isolate device, Initiate Automated Investigation, and Contain device

Answer:

Answer Area

Device1:

- Isolate device only
- Initiate Automated Investigation only
- Contain device only
- Isolate device and Initiate Automated Investigation only
- Isolate device, Initiate Automated Investigation, and Contain device

Device2:

- Isolate device only
- Initiate Automated Investigation only
- Contain device only
- Isolate device and Initiate Automated Investigation only
- Isolate device, Initiate Automated Investigation, and Contain device

Question: 229 CertyIQ

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

You need to ensure that User1 can manage Microsoft Defender XDR custom detection rules and Endpoint security policies. The solution must follow the principle of least privilege.

Which role should you assign to User1?

A.Security Administrator
B.Security Operator
C.Cloud Device Administrator
D.Desktop Analytics Administrator

Answer: A

Explanation:

Correct answer is A:Security Administrator.

Question: 230 CertyIQ

HOTSPOT
-

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 Area

VM1:
- An Azure virtual machine extension
- The Azure Monitor Agent and an Azure virtual machine extension
- The Log Analytics agent and an Azure virtual machine extension

Server1:
- An Azure virtual machine extension
- The Azure Monitor Agent and an Azure virtual machine extension
- The Log Analytics agent and an Azure virtual machine extension

Answer:

Answer Area

VM1:
- An Azure virtual machine extension
- The Azure Monitor Agent and an Azure virtual machine extension
- The Log Analytics agent and an Azure virtual machine extension

Server1:
- An Azure virtual machine extension
- The Azure Monitor Agent and an Azure virtual machine extension
- The Log Analytics agent and an Azure virtual machine extension

Question: 231

CertyIQ

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

You need to create a visual based on the SecurityEvent 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 metric
C.a group
D.links or tabs

Answer: A

Explanation:

A query allows you to retrieve specific data from the SecurityEvent table.You can write a query that filters events based on the past week's timestamp and aggregates the count of events by day.The timechart visualization will display this aggregated data over time, showing the event count trends.

Question: 232 CertyIQ

HOTSPOT
-

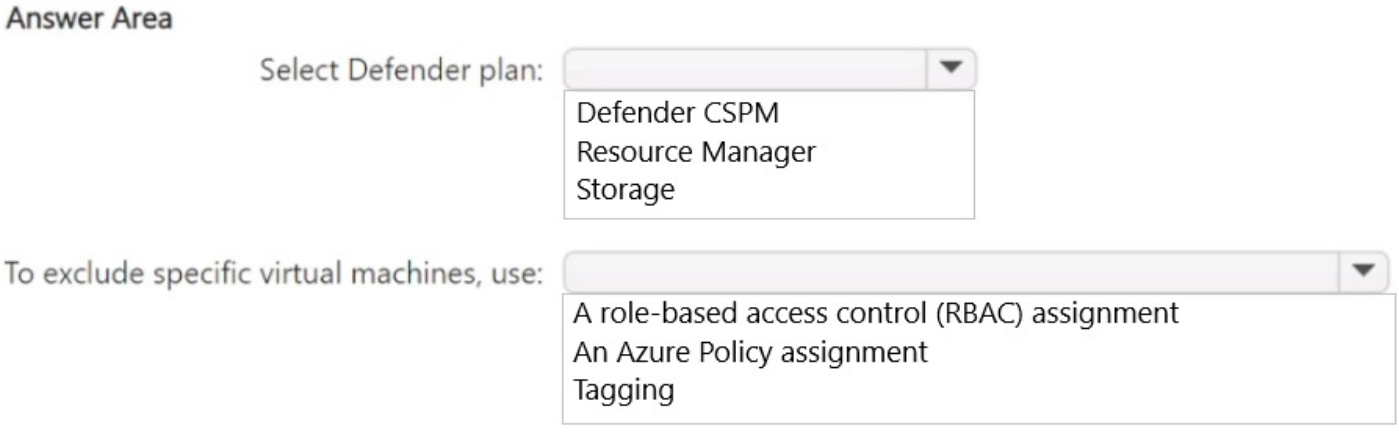
You have an Azure subscription that contains 50 virtual machines.

You plan to deploy Microsoft Defender for Cloud.

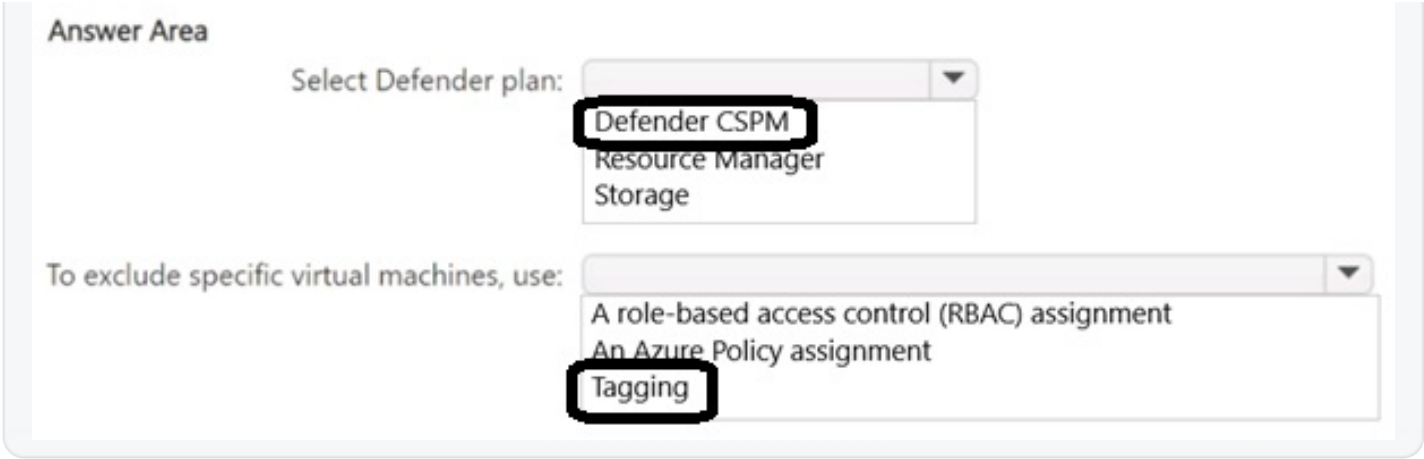
You need to enable agentless scanning for 40 virtual machines. The solution must create disk snapshots of the virtual machines and perform out-of-band analysis of the snapshots.

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

NOTE: Each correct selection is worth one point.



Answer:



Question: 233 CertyIQ

You have an Azure subscription.

You need to stream the Microsoft Graph activity logs to a third-party security information and event management (SIEM) tool. The solution must minimize administrative effort.

To where should you stream the logs?

A.an Azure Event Hubs namespace
B.an Azure Storage account
C.an Azure Event Grid namespace
D.a Log Analytics workspace

Answer: A

Question: 234 CertyIQ

HOTSPOT
-

You have a Microsoft 365 E5 subscription that uses Microsoft Defender XDR and contains two users named User1 and User2.

You need to ensure that the users can perform searches by using the Microsoft Purview portal. The solution must meet the following requirements:

•Ensure that User1 can search the Microsoft Purview Audit service logs and review the Microsoft Purview Audit service configuration.
•Ensure that User2 can search Microsoft Exchange Online mailboxes.
•Follow the principle of least privilege.

To which Microsoft Purview role group should you add each user? To answer, select the appropriate options in the answer area

NOTE: Each correct selection is worth one point.

Answer Area

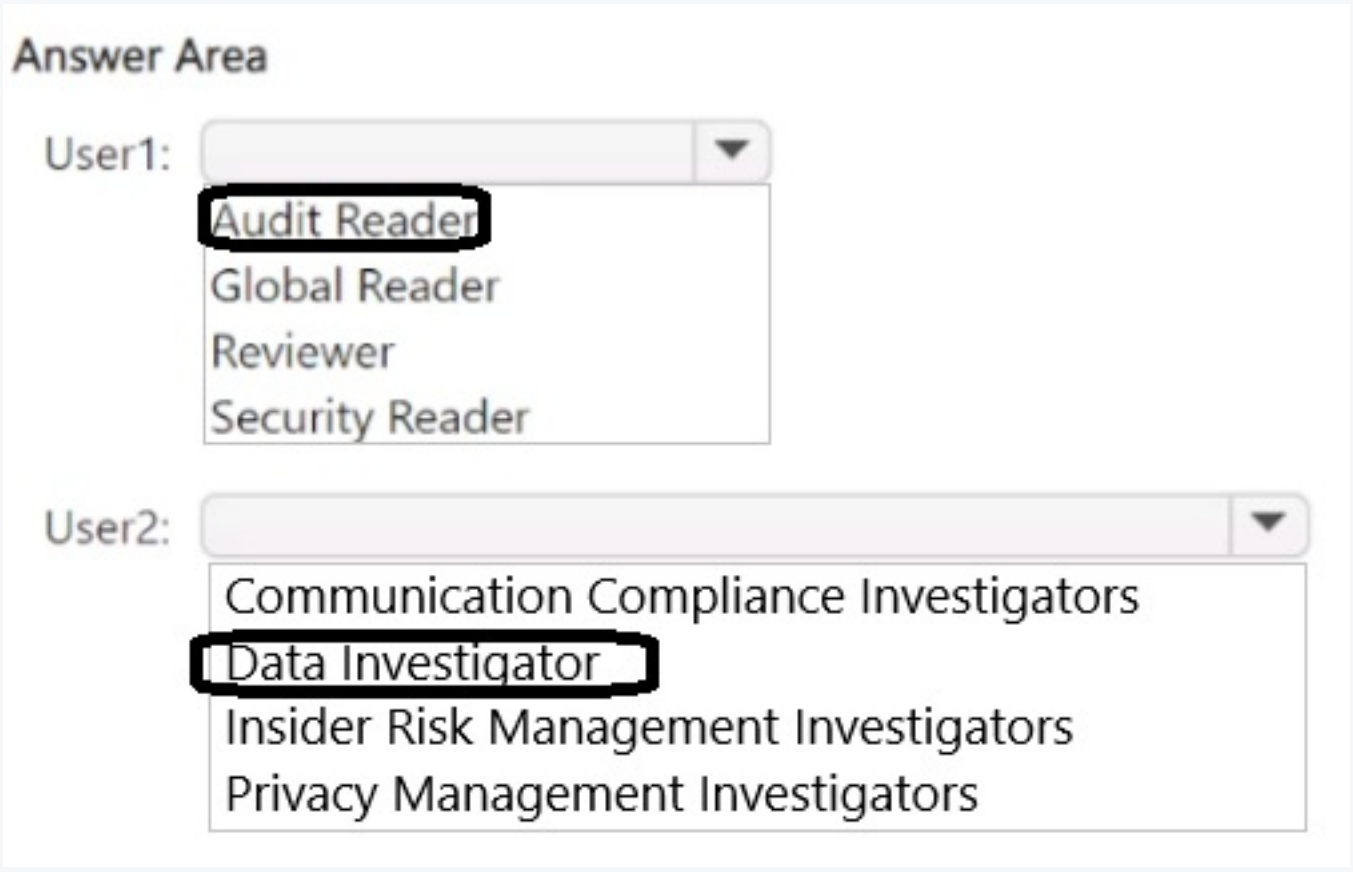
User1:

- Audit Reader
- Global Reader
- Reviewer
- Security Reader

User2:

- Communication Compliance Investigators
- Data Investigator
- Insider Risk Management Investigators
- Privacy Management Investigators

Answer:



Question: 235

CertyIQ

You have a Microsoft 365 subscription that uses Microsoft Defender for Endpoint Plan 2 and contains 500 Windows devices.

As part of an incident investigation, you identify the following suspected malware files:

•sys
•pdf
•docx
•xlsx

You need to create indicator hashes to block users from downloading the files to the devices.

Which files can you block by using the indicator hashes?

A.File1.sys only
B.File1.sys and File3.docx only
C.File1.sys, File3.docx, and File4.xlsx only
D.File2.pdf, File3.docx, and File4.xlsx only
E.File1.sys, File2.pdf, File3.docx, and File4.xlsx

Answer: E

Explanation:

File1.sys, File2.pdf, File3.docx, and File4.xlsx.

Question: 236 CertyIQ

You have a Microsoft 365 subscription that uses Microsoft Defender for Endpoint and contains a user named User1 and a Microsoft 365 group named Group1. All users are assigned a Defender for Endpoint Plan 1 license.

You enable Microsoft Defender XDR Unified role-based access control (RBAC) for Endpoints & Vulnerability Management.

You need to ensure that User1 can configure alerts that will send email notifications to Group1. The solution must follow the principle of least privilege.

Which permissions should you assign to User1?

A.Defender Vulnerability Management - Remediation handling
B.Alerts investigation
C.Live response capabilities: Basic
D.Manage security settings

Answer: B

Explanation:

Correct answer is B.Alerts Investigation"Alerts investigation - Security operations \ Security data \ Alerts (manage)

"https://learn.microsoft.com/en-us/defender-xdr/compare-rbac-roles

Question: 237 CertyIQ

HOTSPOT
-

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

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

Answer:

Answer Area

Question: 238 CertyIQ

You need to implement the Azure Information Protection requirements.
What should you configure first?

A.Device health and compliance reports settings in Microsoft Defender Security Center

B.scanner clusters in Azure Information Protection from the Azure portal

C.content scan jobs in Azure Information Protection from the Azure portal

D.Advanced features from Settings in Microsoft Defender Security Center

Answer: D

Explanation:

D is correct.As stated by the requirements below, this is on a Windows 10 endpoint, which would require Defender, not Azure Portal.Azure Information Protection RequirementsAll files that have security labels and are stored on the Windows 10 computers must be available from the Azure Information Protection " Data discovery dashboard.

Reference:

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

Question: 239 CertyIQ

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

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

Answer: C

Explanation:

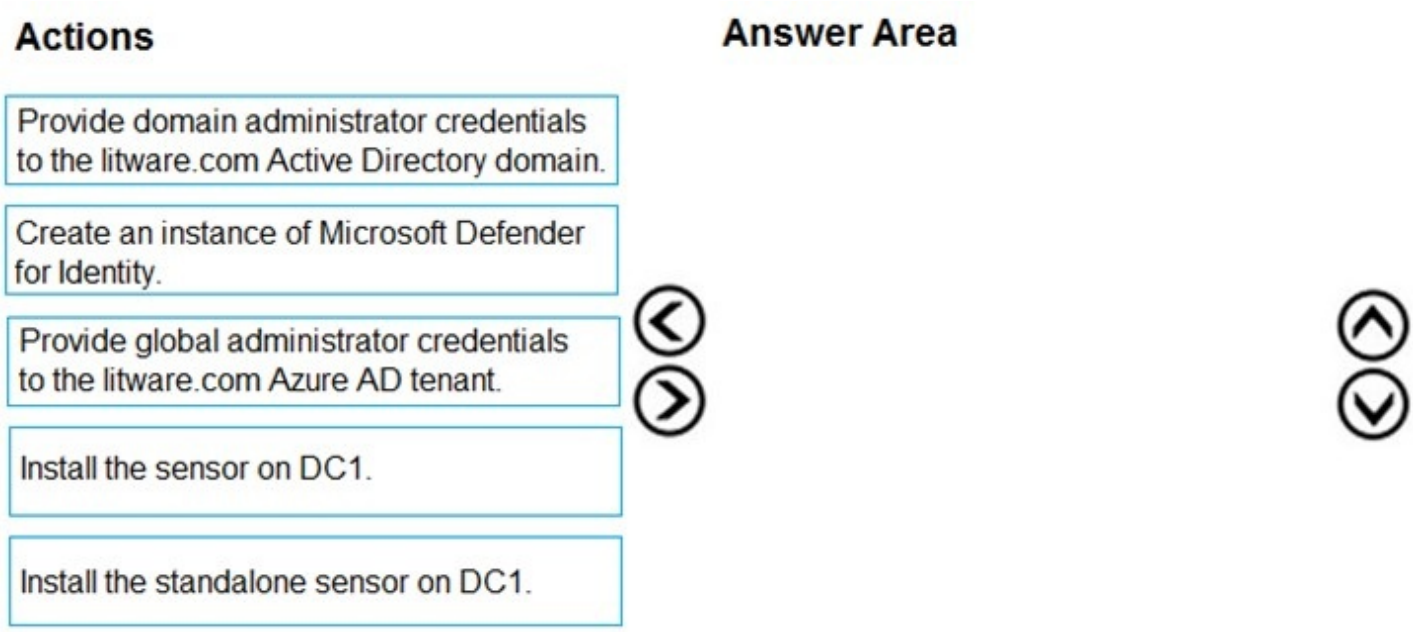
C. Users connecting to two geographically separate locations at the same time would trigger the impossible travel alert, however as these are legitimate then this setting needs to be altered to include both network addresses.

Reference:

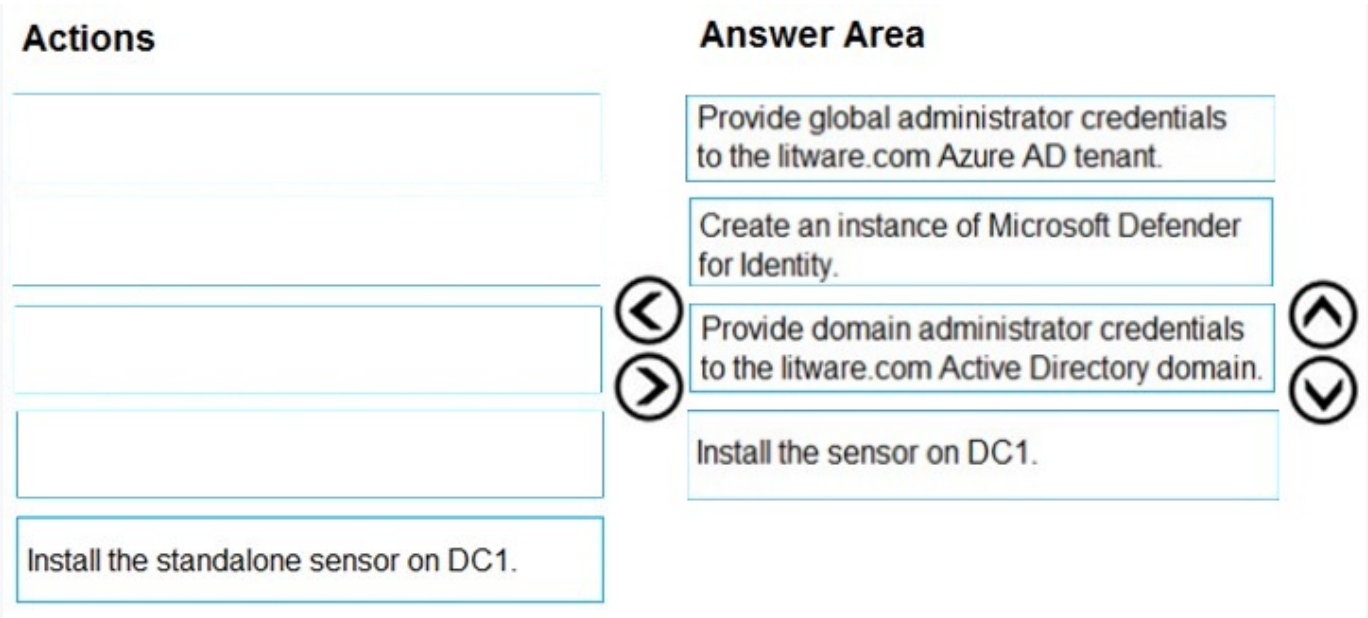
https://docs.microsoft.com/en-us/cloud-app-security/anomaly-detection-policy

Question: 240 CertyIQ

DRAG DROP -
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.
Select and Place:



Answer:



Explanation:
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

Question: 241 CertyIQ

HOTSPOT
-

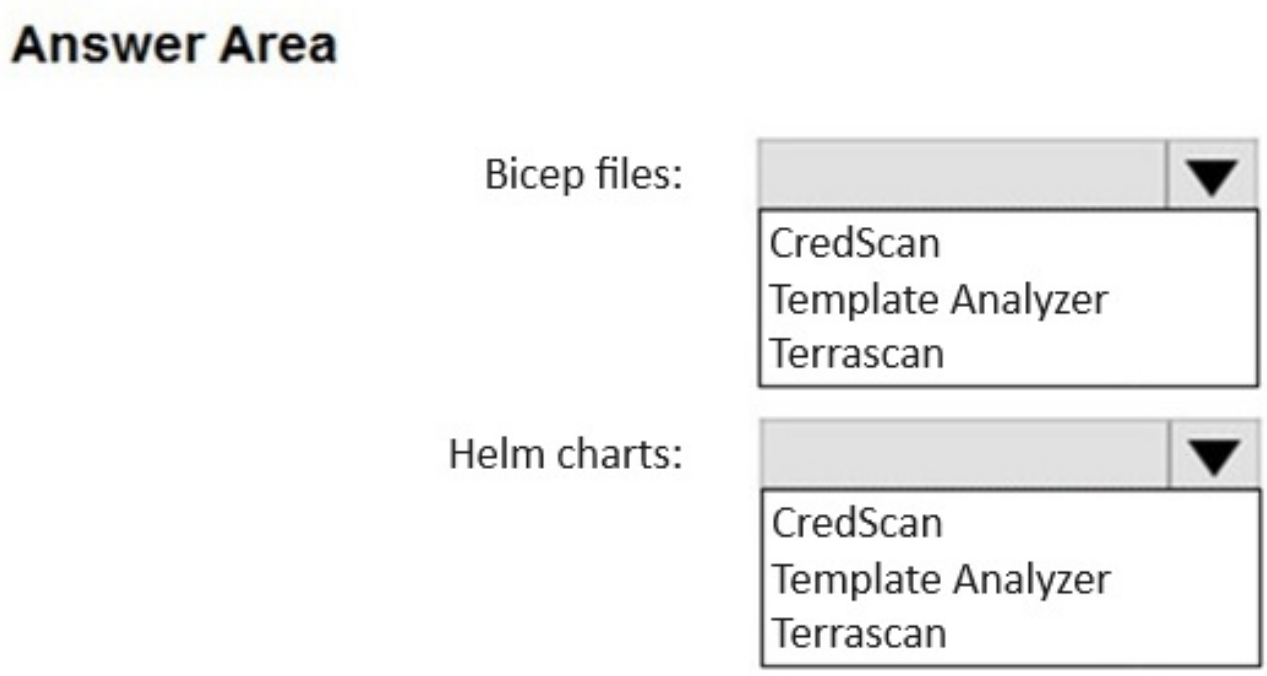
You have an Azure DevOps organization that contains an Azure Repos repository named Repo1 and is onboarded to Microsoft Defender for DevOps.

You create infrastructure as code (IaC) files and store them in Repo1. The IaC files are formatted as Bicep files and Helm charts.

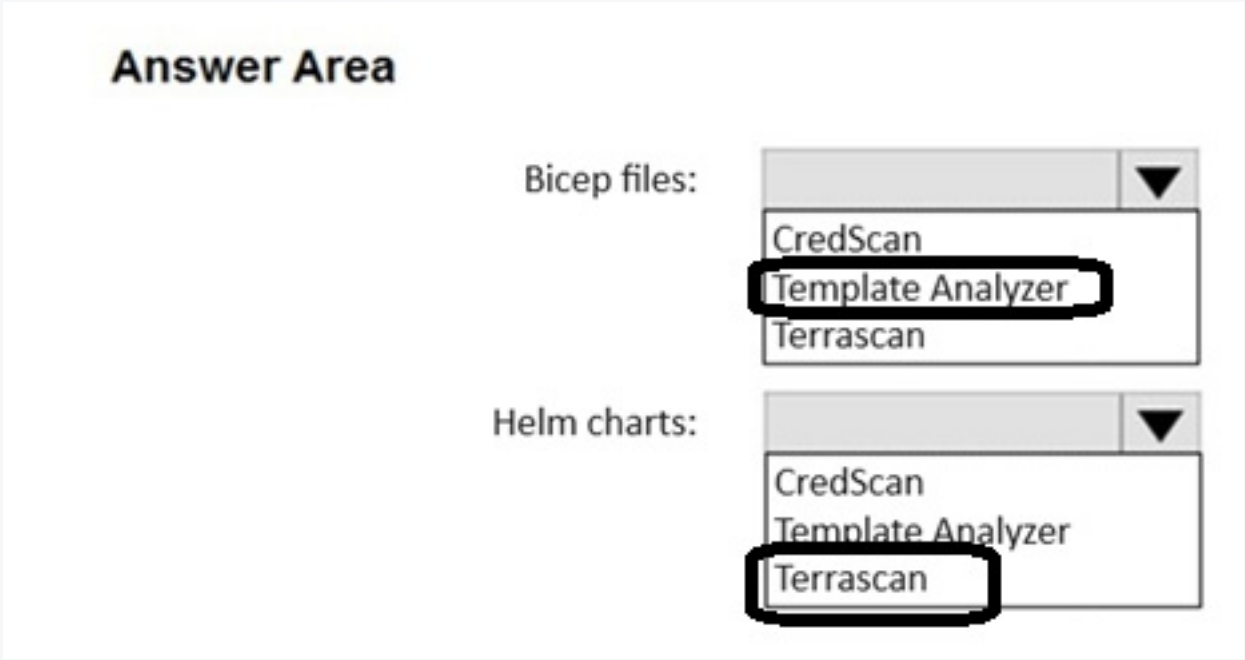
You need to configure Defender for DevOps to identify misconfigurations in the IaC files.

Which scanning tool should you use for each type of files? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.



Answer:



Explanation:

Template Analyzer.

Terrascan.

Question: 242 CertyIQ

HOTSPOT
-

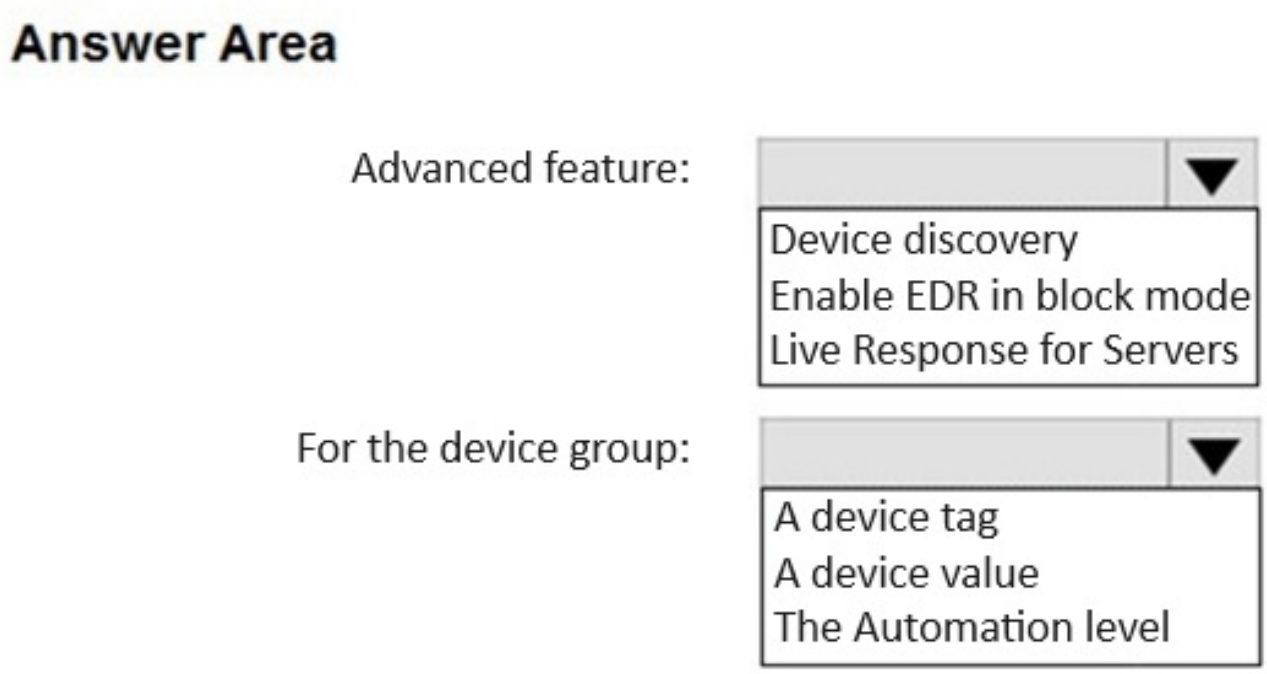
You have a Microsoft 365 E5 subscription that uses Microsoft 365 Defender for Endpoint.

You need to ensure that you can initiate remote shell connections to Windows servers by using the Microsoft 365

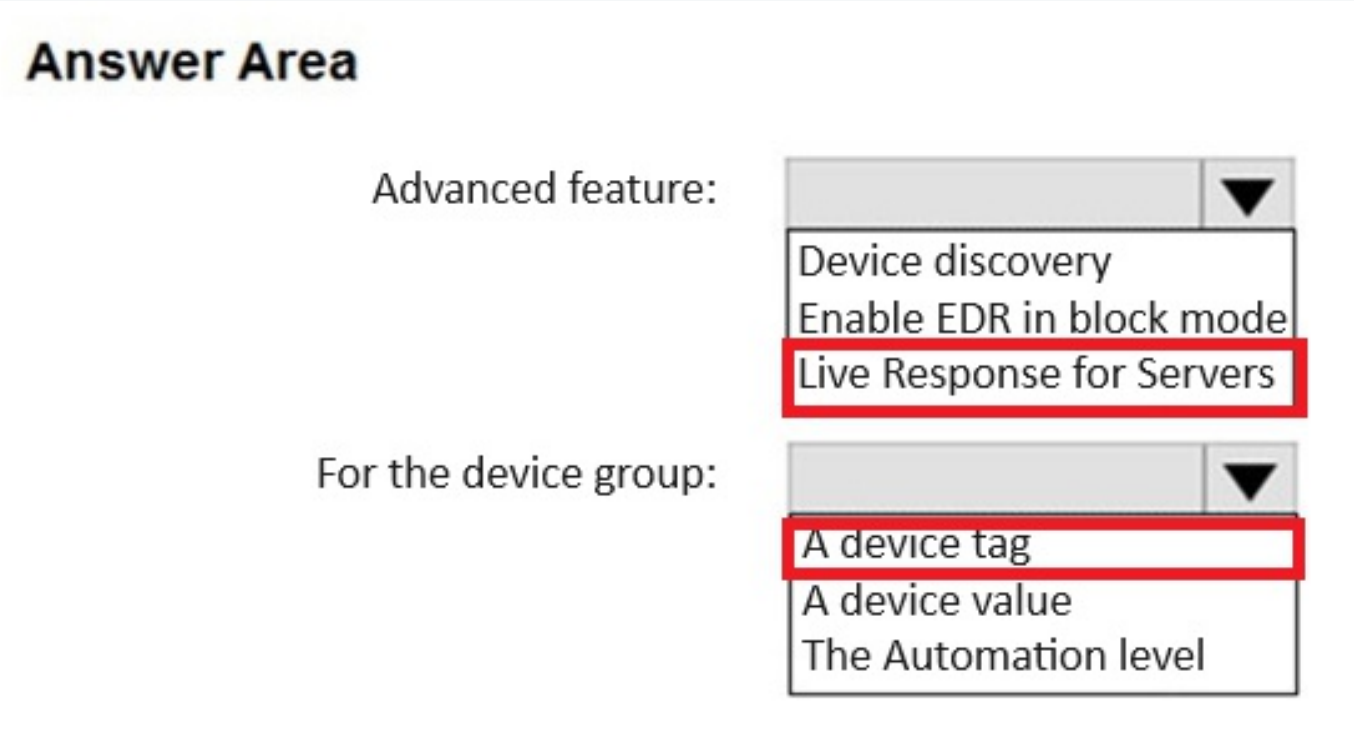
Defender portal.

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

NOTE: Each correct selection is worth one point.



Answer:



Explanation:

Live response for servers.

A device Tag.

Question: 243 CertyIQ

You have 500 on-premises devices.

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

You onboard 100 devices to Microsoft Defender 365.

You need to identify any unmanaged on-premises devices. The solution must ensure that only specific onboarded devices perform the discovery.

What should you do first?

A.Create a device group.
B.Create an exclusion.
C.Set Discovery mode to Basic.
D.Create a tag.

Answer: C

Explanation:

Set Discovery Mode to Basic:Configure the Discovery mode for your onboarded devices.Choose Basic discovery mode to passively collect events in your network and extract device information from them.Basic discovery uses the SenseNDR.exe binary for passive network data collection, and no network traffic is initiated. Endpoints extract data from all network traffic seen by an onboarded device.Note that with basic discovery, you gain limited visibility of unmanaged endpoints in your network.

Reference:

https://learn.microsoft.com/en-us/defender-endpoint/device-discovery?view=o365-worldwide

Question: 244 CertyIQ

You have a Microsoft 365 E5 subscription that contains a device named Device1. Device1 is enrolled in Microsoft Defender for Endpoint.

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.Autoruns
C.Security event log
D.Scheduled tasks
E.Prefetch files

Answer: E

Explanation:

Correct answer is E:Prefetch files.

Question: 245 CertyIQ

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

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

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

What should you install first on Server1?

A.the Microsoft Monitoring Agent
B.the Azure Monitor agent
C.the Azure Connected Machine agent
D.the Azure Pipelines agent

Answer: C

Explanation:

C. the Azure Connected Machine agent.

Question: 246 CertyIQ

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

You are investigating an attacker that is known to use the Microsoft Graph API as an attack vector. The attacker performs the tactics shown the following table.

Name	Tactic
Tactic1	Conditional Access policy reconnaissance
Tactic2	Mailbox reconnaissance
Tactic3	Invites guest users to the tenant

You need to search for malicious activities in your organization.

Which tactics can you analyze by using the MicrosoftGraphActivityLogs table?

A.Tactic2 only
B.Tactic1 and Tactic2 only
C.Tactic2 and Tactic3 only
D.Tactic1, Tactic2, and Tactic3

Answer: D

Explanation:

Correct answer is D:Tactic1, Tactic2, and Tactic3.

Question: 247 CertyIQ

DRAG DROP
-

You have a Microsoft Sentinel workspace that contains the following Advanced Security Information Model (ASIM) parsers:

•_Im_ProcessCreate
•imProcessCreate

You create a new source-specific parser named vimProcessCreate.

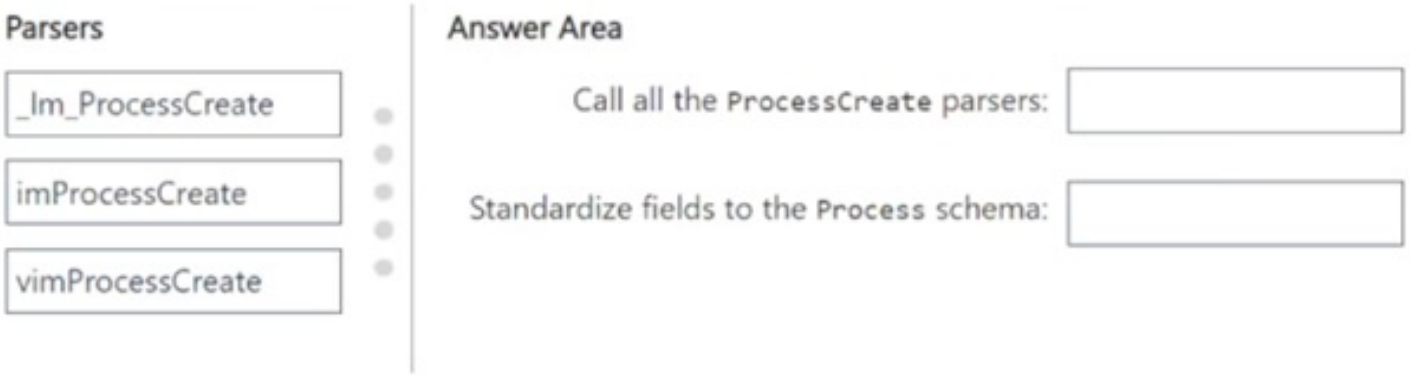
You need to modify the parsers to meet the following requirements:

•Call all the ProcessCreate parsers.
•Standardize fields to the Process schema.

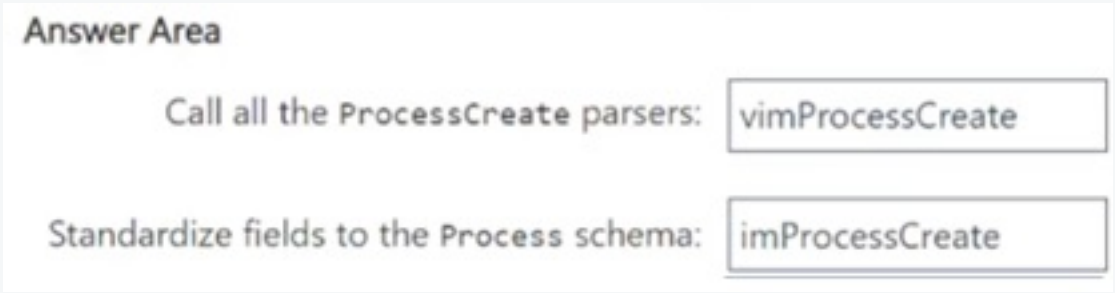
Which parser should you modify to meet each requirement? To answer, drag the appropriate parsers to the correct requirements.

Each 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:



Question: 248 CertyIQ

HOTSPOT
-

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 Area

```
$events = '
    @{Log="Security";EventType="System";EventID="4624";EventID="4625"
    <Security> <System> <EventID>4624</EventID> <EventID>4625</EventID> </System> </Security>
    Security!*[System[(EventID=4624 or EventID=4625)]]
'

Get-WinEvent -LogName 'Security'  $events
```

-FilterHashtable
-FilterXml
-FilterXPath

Answer:

Answer Area

```
$events = '
    @{Log="Security";EventType="System";EventID="4624";EventID="4625"
    <Security> <System> <EventID>4624</EventID> <EventID>4625</EventID> </System> </Security>
    Security!*[System[(EventID=4624 or EventID=4625)]]
'

Get-WinEvent -LogName 'Security'  $events
```

-FilterHashtable
-FilterXml
-FilterXPath

Question: 249 CertyIQ

You have a Microsoft 365 subscription that uses Microsoft Defender for Endpoint Plan 2 and contains 500 Windows devices.

You plan to create a Microsoft Defender XDR custom deception rule.

You need to ensure that the rule will be applied to only 10 specific devices.

What should you do first?

A. Add custom lures to the rule.
B. Add the IP address of each device to the list of decoy accounts and hosts of the rule.
C. Add the devices to a group.
D. Assign a tag to the devices.

Answer: A

Explanation:

Add custom lures to the rule"In the rule creation pane, add a rule name, description, and select what lure types to create.

"https://learn.microsoft.com/en-us/defender-xdr/configure-deception

Question: 250 CertyIQ

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 Log Analytics.
B.Enable the Cloud Security Posture Management (CSPM) plan for the subscription.
C.Configure the Continuous export settings for Azure Event Hubs.
D.Disable the Microsoft Cloud Security Benchmark (MCSB) assignment.

Answer: B

Explanation:

Enable the Cloud Security Posture Management (CSPM) plan for the subscription.

Question: 251 CertyIQ

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 Sentinel?

A.Content hub
B.Entity behavior
C.Analytics
D.Settings

Answer: C

Explanation:

C. Analytics You can now find anomaly rules displayed in a grid in the Anomalies tab in the Analytics page.

https://learn.microsoft.com/en-us/azure/sentinel/work-with-anomaly-rules

Question: 252 CertyIQ

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 hunting livestream session

B.a query bookmark

C.a scheduled query rule

D.a Fusion rule

Answer: C

Explanation:

C. a scheduled query rule:This is used to run queries on a schedule, and when a match is found, it can create an incident in Microsoft Sentinel. Given that you have a hunting query that detects a new attack vector, setting up a scheduled query rule will ensure that this query runs regularly and automatically generates an incident whenever the attack vector is detected.

Question: 253 CertyIQ

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

The security team at your company detects command and control (C2) agent traffic on the network. Agents communicate once every 50 hours.

You need to create a Microsoft Defender XDR custom detection rule that will identify compromised devices and establish a pattern of communication. The solution must meet the following requirements:

•Identify all the devices that have communicated during the past 14 days.
•Minimize how long it takes to identify the devices.

To what should you set the detection frequency for the rule?

A.Every 12 hours

B.Every 24 hours

C.Every three hours

D.Every hour

Answer: B

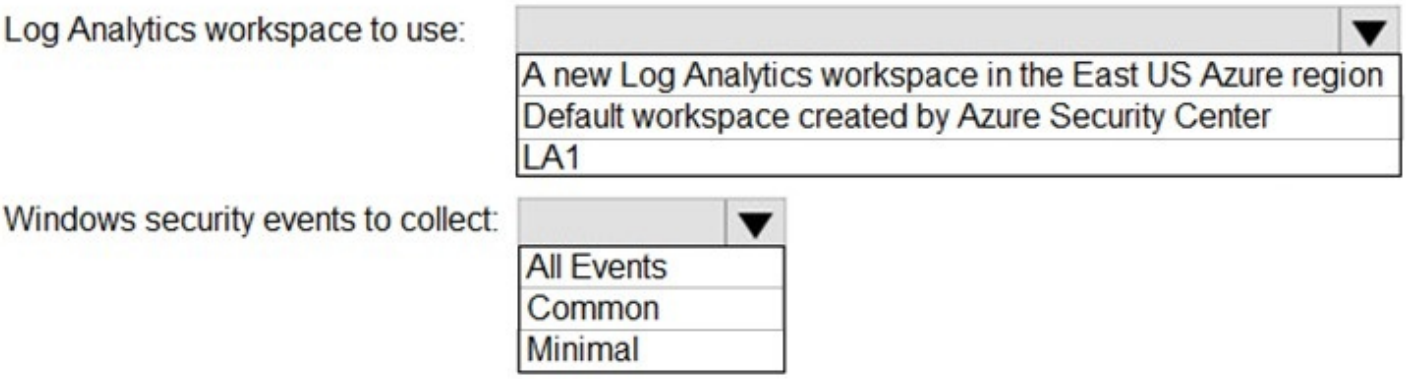
Explanation:

Correct answer is B:Every 24 hours.

Question: 254 CertyIQ

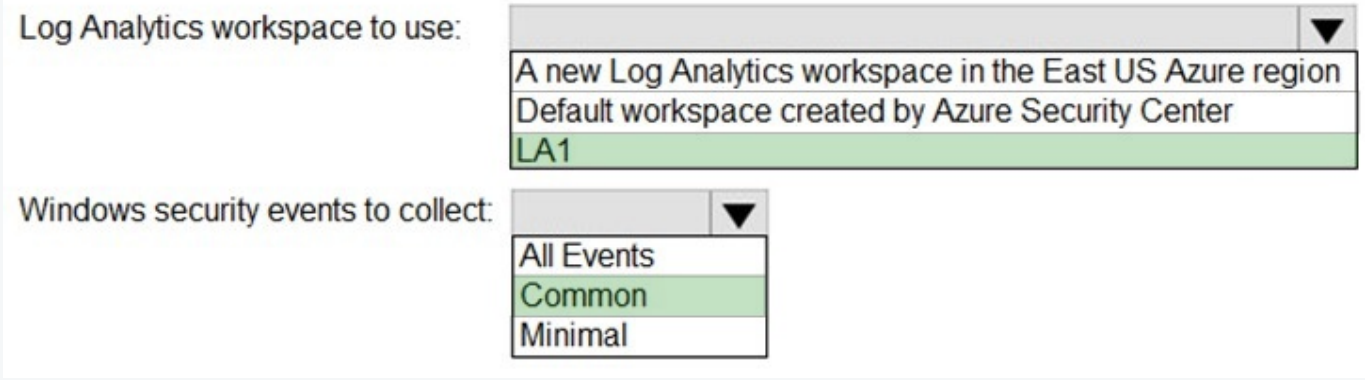
HOTSPOT -
You need to implement Azure Defender to meet the Azure Defender requirements and the business requirements.
What should you include in the solution? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.
Hot Area:

Answer Area



Answer:

Answer Area



Explanation:

Reference:

https://docs.microsoft.com/en-us/azure/sentinel/connect-windows-security-events?tabs=LAA

Question: 255

CertyIQ

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

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

Answer: B

Explanation:

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

Mitigate threats using Azure Defender

Question: 256 CertyIQ

You have an Azure subscription that uses Microsoft Sentinel.

You need to minimize the administrative effort required to respond to the incidents and remediate the security threats detected by Microsoft Sentinel.

Which two features should you use? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

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

Answer: CD

Question: 257 CertyIQ

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: D

Explanation:

Reference:

https://learn.microsoft.com/en-us/azure/defender-for-cloud/configure-email-notifications

Question: 258

CertyIQ

You have an on-premises network.

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

From the Microsoft Defender portal, you investigate an incident on a device named Device1 of a user named User1. The incident contains the following Defender for Identity alert.

Suspected identity theft (pass-the-ticket) (external ID 2018)

You need to contain the incident without affecting users and devices. The solution must minimize administrative effort.

What should you do?

A.Disable User1 only.

B.Quarantine Device1 only.

C.Reset the password for all the accounts that previously signed in to Device1.

D.Disable User1 and quarantine Device1.

E.Disable User1, quarantine Device1, and reset the password for all the accounts that previously signed in to Device1.

Answer: E

Explanation:

Disable User1, quarantine Device1, and reset the password for all the accounts that previously signed in to Device1.

Question: 259

CertyIQ

HOTSPOT
-

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:

MicrosoftGraphActivityLogs.

(parse_url(RequestUri).Path).

Question: 260

CertyIQ

HOTSPOT
-

You have a Microsoft 365 subscription that uses Microsoft Defender XDR and contains a Windows device named Device1.

You investigate a suspicious process named Prod on Device1 by using a live response session.

You need to perform the following actions:

•Stop Prod.
•Send Prod for further review.

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 Area

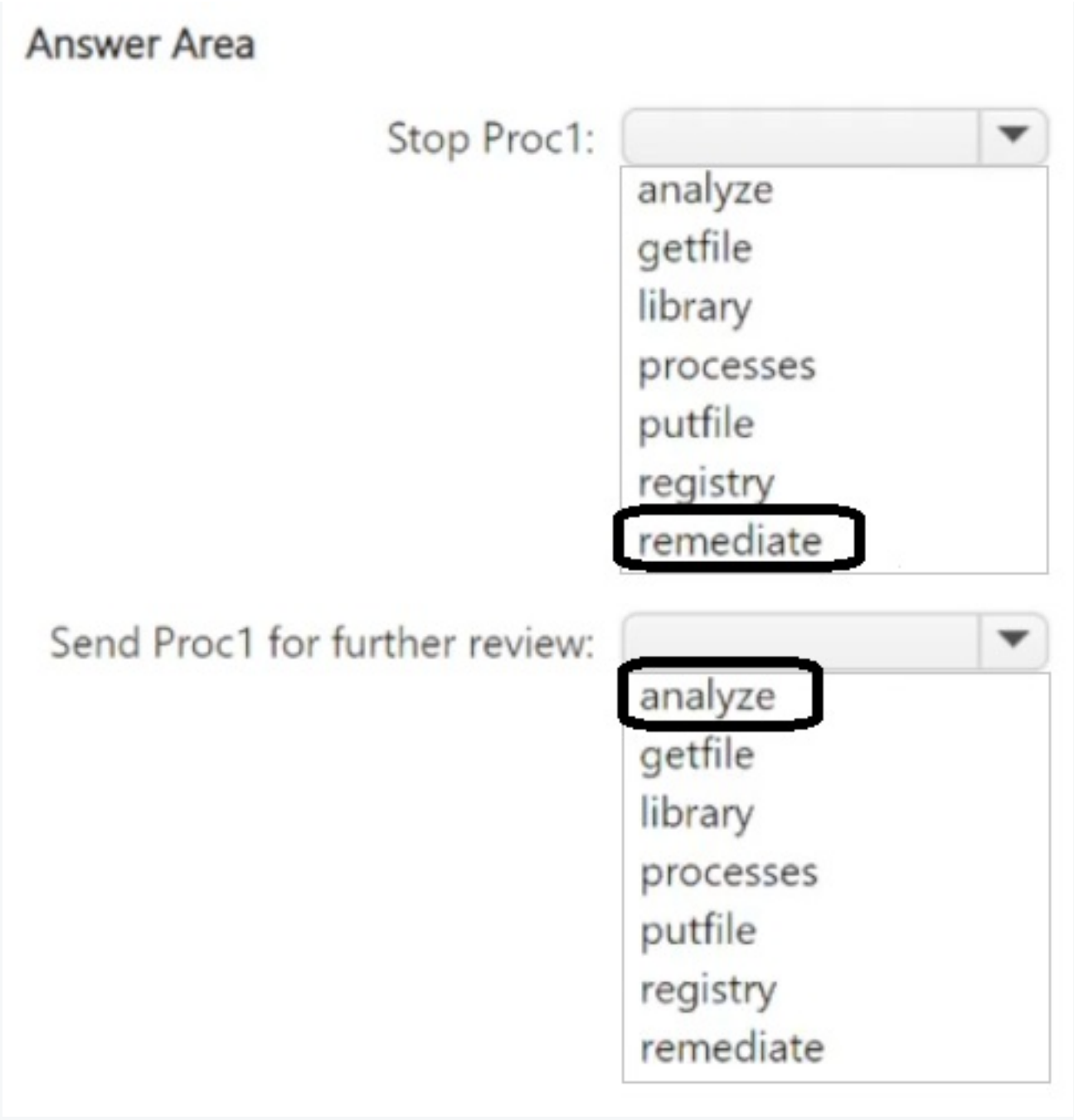
Stop Proc1:

- analyze
- getfile
- library
- processes
- putfile
- registry
- remediate

Send Proc1 for further review:

- analyze
- getfile
- library
- processes
- putfile
- registry
- remediate

Answer:



Explanation:

remediate.

analyze.

Question: 261 CertyIQ

HOTSPOT
-

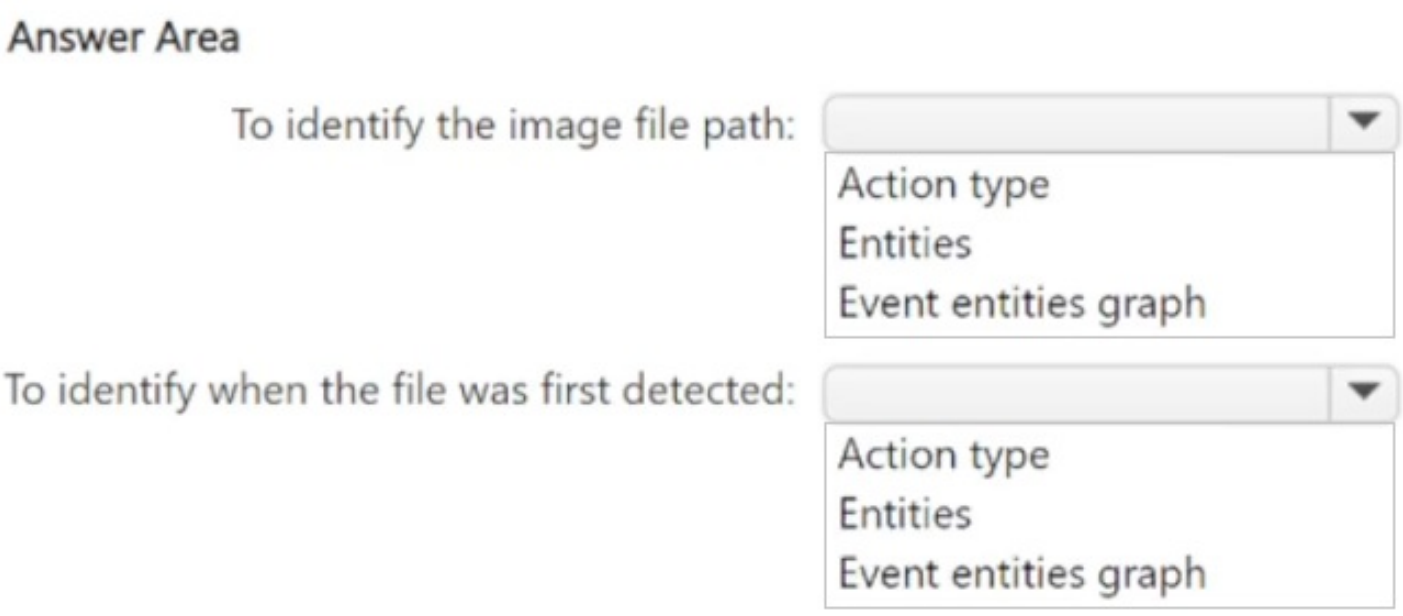
You have a Microsoft 365 E5 subscription that uses Microsoft Defender for Endpoint and contains a Windows device named Device1.

You need to investigate a suspicious executable file detected on Device1. The solution must meet the following requirements:

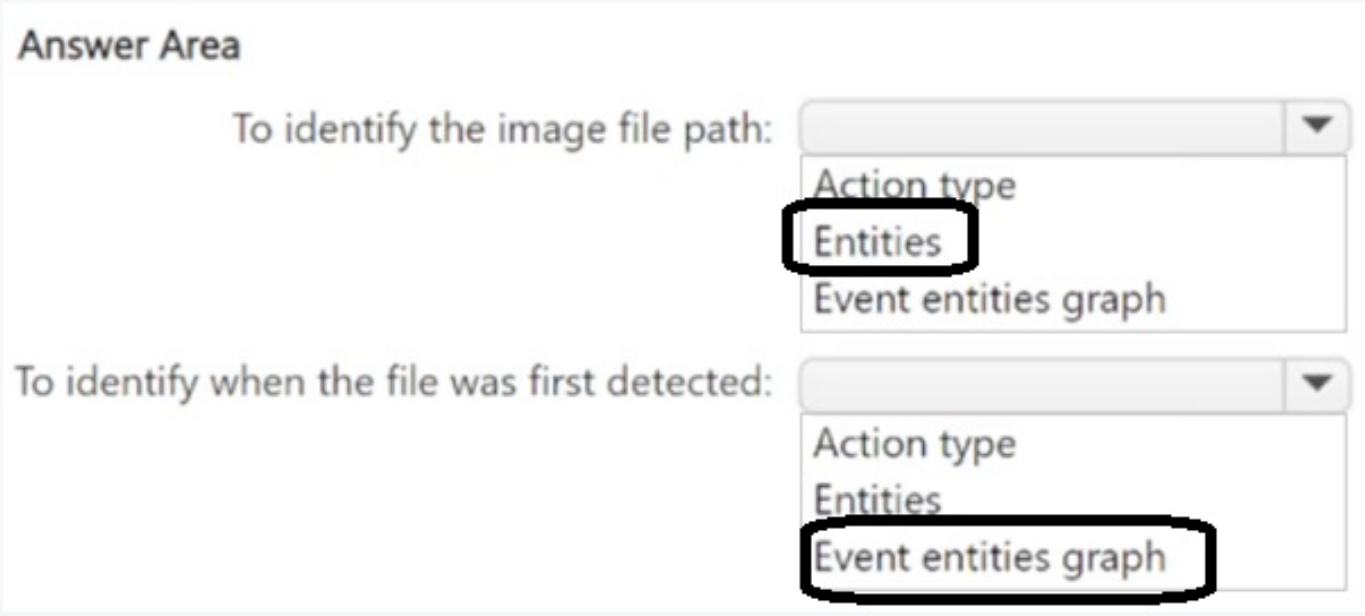
•Identify the image file path of the file.
•Identify when the file was first detected on Device1.

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:



Question: 262 CertyIQ

You have a Microsoft 365 subscription that uses Microsoft Defender for Endpoint Plan 2 and contains 1,000 Windows devices.

You have a PowerShell script named Script1.ps1 that is signed digitally.

You need to ensure that you can run Script1.ps1 in a live response session on one of the devices.

What should you do first from the live response session?

A.Run the library command.

B.Upload Script1.ps1 to the library.

C.Run the putfile command.

D.Modify the PowerShell execution policy of the device.

Answer: B

Explanation:

Upload Script1.ps1 to the library.

Question: 263 CertyIQ

HOTSPOT
-

You have a Microsoft 365 subscription that uses Microsoft Defender for Endpoint Plan 2 and contains a Windows device named Device1.

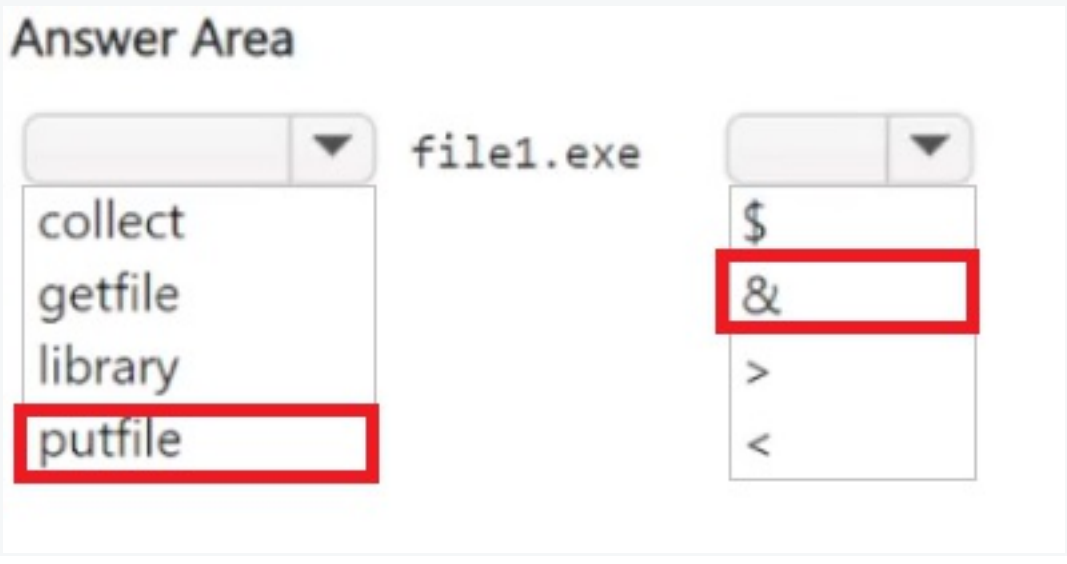
You initiated a live response session on Device1.

You need to run a command that will download a 250-MB file named File1.exe from the live response library to Device1. The solution must ensure that File1.exe is downloaded as a background process.

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

NOTE: Each correct selection is worth one point.

Answer:



Explanation:

1. Putfile - this command is used to download a file from the library to the device.

2. & to make this a background task.

Question: 264 CertyIQ

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 an Azure subscription that uses Microsoft Defender XDR.

From the Microsoft Defender portal, you perform an audit search and export the results as a file named File1.csv that contains 10,000 rows.

You use Microsoft Excel to perform Get & Transform Data operations to parse the AuditData column from File1.csv. The operations fail to generate columns for specific JSON properties.

You need to ensure that Excel generates columns for the specific JSON properties in the audit search results.

Solution: From Defender, you modify the search criteria of the audit search to increase the number of returned records, and then you export the results. From Excel, you perform the Get & Transform Data operations by using the new export.

Does this meet the requirement?

A.Yes

B.No

Answer: B

Explanation:

Reference:

https://learn.microsoft.com/en-us/purview/audit-log-export-records

Question: 265 CertyIQ

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 an Azure subscription that uses Microsoft Defender XDR.

From the Microsoft Defender portal, you perform an audit search and export the results as a file named File1.csv that contains 10,000 rows.

You use Microsoft Excel to perform Get & Transform Data operations to parse the AuditData column from File1.csv. The operations fail to generate columns for specific JSON properties.

You need to ensure that Excel generates columns for the specific JSON properties in the audit search results.

Solution: From Excel, you apply filters to the existing columns in File1.csv to reduce the number of rows, and then you perform the Get & Transform Data operations to parse the AuditData column.

Does this meet the requirement?

A.Yes
B.No

Answer: A

Explanation:

Yes Another workaround is to filter items in the Operations column to reduce the number of rows (before you perform step 5 above) before transforming the JSON object in the AuditData column.

Question: 266 CertyIQ

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 an Azure subscription that uses Microsoft Defender XDR.

From the Microsoft Defender portal, you perform an audit search and export the results as a file named File1.csv that contains 10,000 rows.

You use Microsoft Excel to perform Get & Transform Data operations to parse the AuditData column from File1.csv. The operations fail to generate columns for specific JSON properties.

You need to ensure that Excel generates columns for the specific JSON properties in the audit search results.

Solution: From Defender, you modify the search criteria of the audit search to reduce the number of returned records, and then you export the results. From Excel, you perform the Get & Transform Data operations by using the new export.

Does this meet the requirement?

A.Yes
B.No

Answer: A

Explanation:

you have to reduce the records

https://learn.microsoft.com/en-us/purview/audit-log-export-records

Question: 267 CertyIQ

HOTSPOT

-

You have a Microsoft 365 E5 subscription that uses Microsoft Defender XDR and contains a Windows device named Device1.

You investigate Device1 for malicious activity and discover a suspicious file named File1.exe. You collect an investigation package from Device1.

You need to review the following forensic data points:

•Is an attacker currently accessing Device1 remotely?
•When was File1.exe first executed?

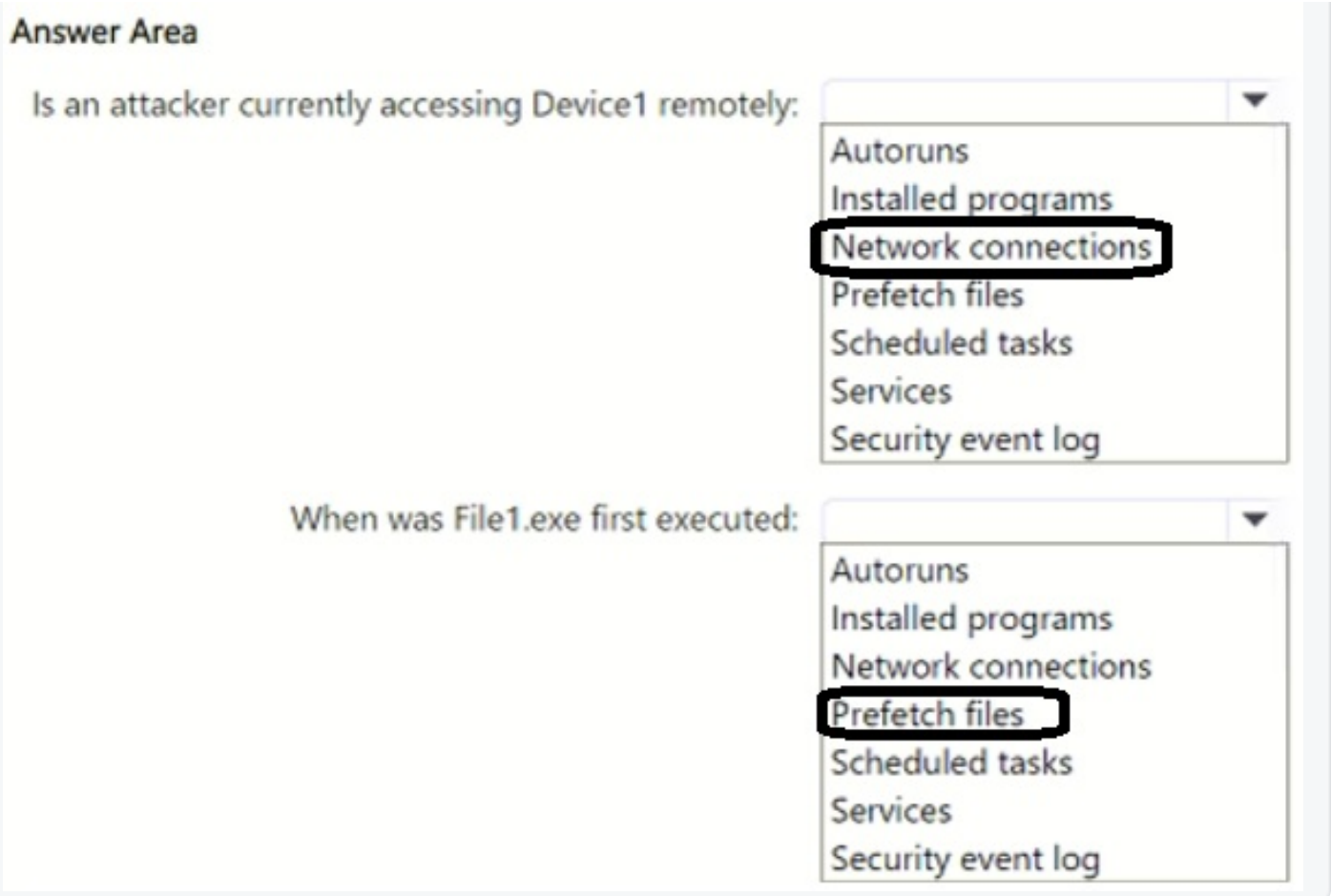
Which folder in the investigation package should you review for each data point? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Answer:

Answer Area



Question: 268

CertyIQ

HOTSPOT
-

You have a Microsoft 365 subscription that uses Microsoft Defender for Endpoint Plan 2 and contains a Windows device named Device1.

Twenty files on Device1 are quarantined by custom indicators as part of an investigation.

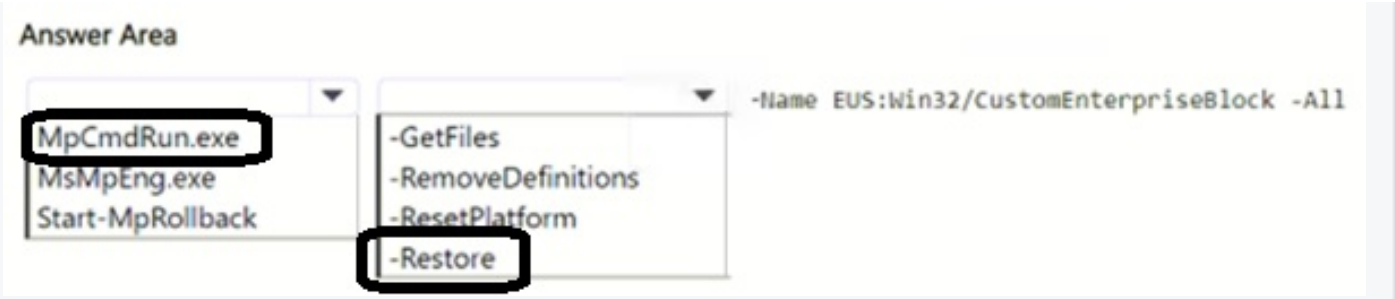
You need to release the 20 files from quarantine.

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

NOTE: Each correct selection is worth one point.

Answer Area

Answer:



Question: 269 CertyIQ

You have a Microsoft 365 E5 subscription.

Automated investigation and response (AIR) is enabled in Microsoft Defender for Office 365 and devices use full automation in Microsoft Defender for Endpoint.

You have an incident involving a user that received malware-infected email messages on a managed device.

Which action requires manual remediation of the incident?

A.soft deleting the email message
B.hard deleting the email message
C.isolating the device
D.containing the device

Answer: B

Explanation:

hard deleting the email message.

Question: 270 CertyIQ

You have a Microsoft 365 subscription that uses Microsoft Defender XDR and contains a Windows device named Device1.

The timeline of Device1 includes three files named File1.ps1, File2.exe, and File3.dll.

You need to submit files for deep analysis in Microsoft Defender XDR.

Which files can you submit?

A.File1.ps1 only
B.File2.exe only
C.File3.dll only
D.File2.exe and File3.dll only
E.File1.ps1 and File2.exe only
F.File1.ps1, File2.exe, and File3.dll

Answer: D

Explanation:

File2.exe and File3.dll only.

Question: 271 CertyIQ

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

You need to identify all the entities affected by an incident.

Which tab should you use in the Microsoft Defender portal?

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

Answer: C

Explanation:

Evidence and Response: This tab provides a detailed view of all the evidence collected during the investigation, including affected entities such as files, processes, users, and devices. It also shows the response actions taken for the incident.

Question: 272 CertyIQ

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

You are investigating an attacker that is known to use the Microsoft Graph API as an attack vector. The attacker performs the tactics shown the following table.

Name	Tactic
Tactic1	Discovers misconfigured mailboxes
Tactic2	Searches Microsoft Teams chats and exports full conversations
Tactic3	Deletes Azure virtual machines

You need to search for malicious activities in your organization.

Which tactics can you analyze by using the MicrosoftGraphActivityLogs table?

A.Tactic1 only
B.Tactic2 only
C.Tactic1 and Tactic3 only
D.Tactic2 and Tactic3 only
E.Tactic1, Tactic2, and Tactic3

Answer: E

Explanation:

Tactic1, Tactic2, and Tactic3.

Question: 273 CertyIQ

HOTSPOT
-

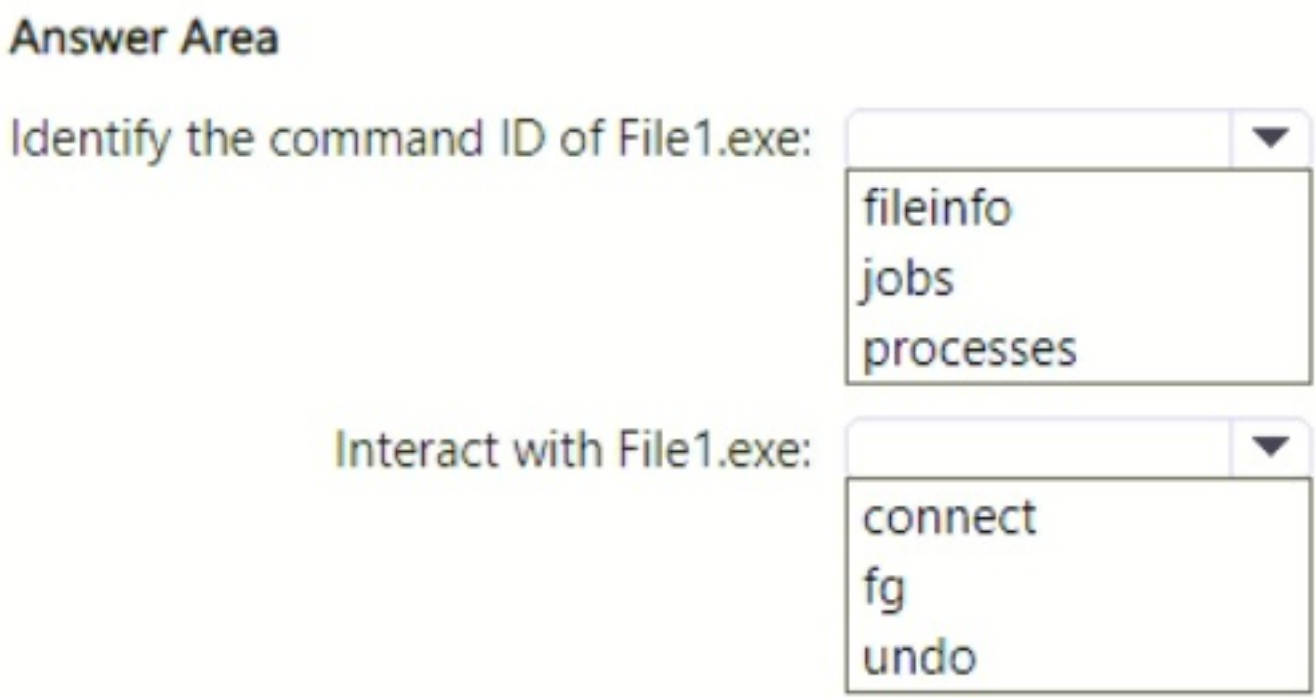
You have a Microsoft 365 subscription that uses Microsoft Defender for Endpoint Plan 2 and contains a Windows device named Device1.
You initiate a live response session on Device1 and launch an executable file named File1.exe in the background.

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:

Answer Area

Identify the command ID of File1.exe:

- fileinfo
- jobs
- processes

Interact with File1.exe:

- connect
- fg
- undo

Question: 274 CertyIQ

HOTSPOT
-

You have a Microsoft 365 subscription that uses Microsoft Purview and contains a Microsoft SharePoint Online site named Site1.

Site1 contains the files shown in the following table.

Name	Author
File1.docx	User1
File2.docx	User2
File3.xlsx	User3

From Microsoft Purview, you create the content search queries shown in the following table.

Name	Query
Search1	`Author:"User1" FileExtension:xlsx`
Search2	`Author:"User*" and FileExtension:*`
Search3	`Author:("User1..3")`

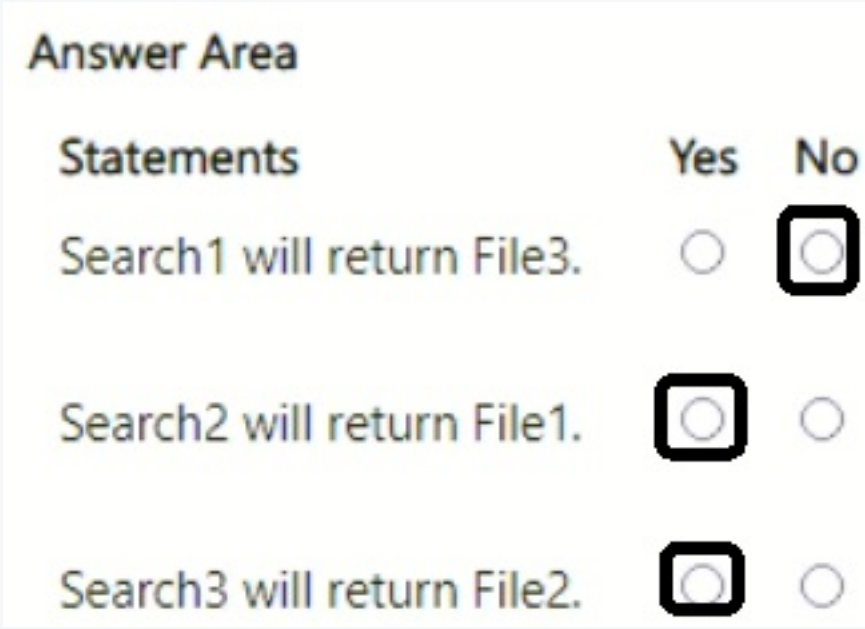
For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
Search1 will return File3.	○	○
Search2 will return File1.	○	○
Search3 will return File2.	○	○

Answer:



Explanation:

No

Yes

Yes

Question: 275 CertyIQ

You have a Microsoft Sentinel workspace named SW1.

In SW1, you investigate an incident that is associated with the following entities:

•Host
•IP address
•User account
•Malware name

Which entity can be labeled as an indicator of compromise (IoC) directly from the incident's page?

A.malware name
B.host
C.user account
D.IP address

Answer: D

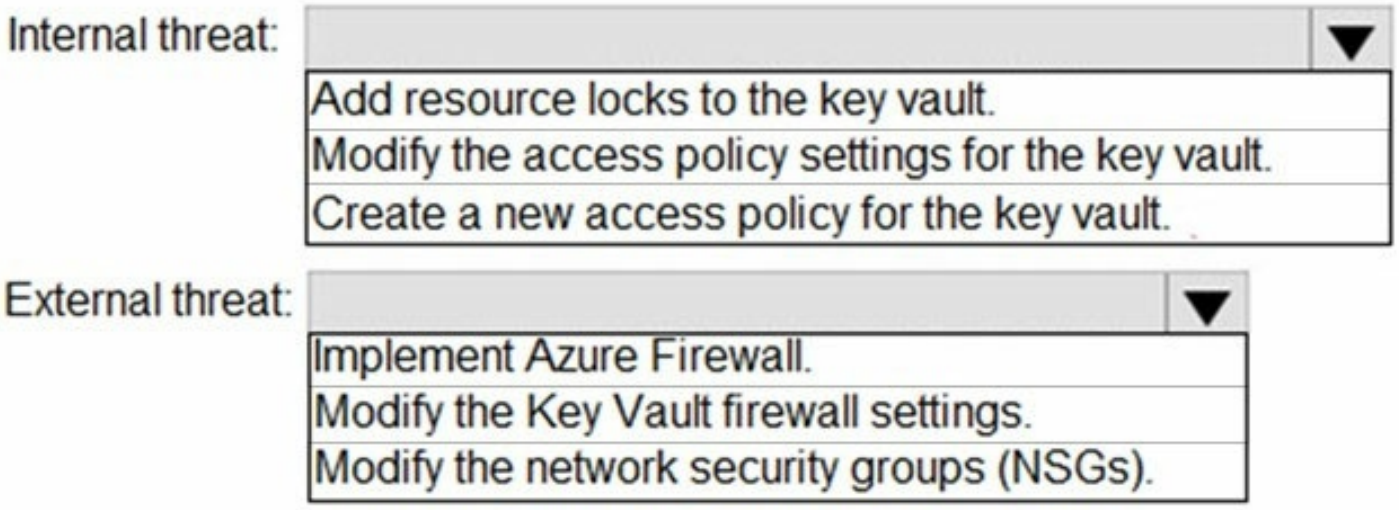
Explanation:

Correct answer is D:IP address.

Question: 276 CertyIQ

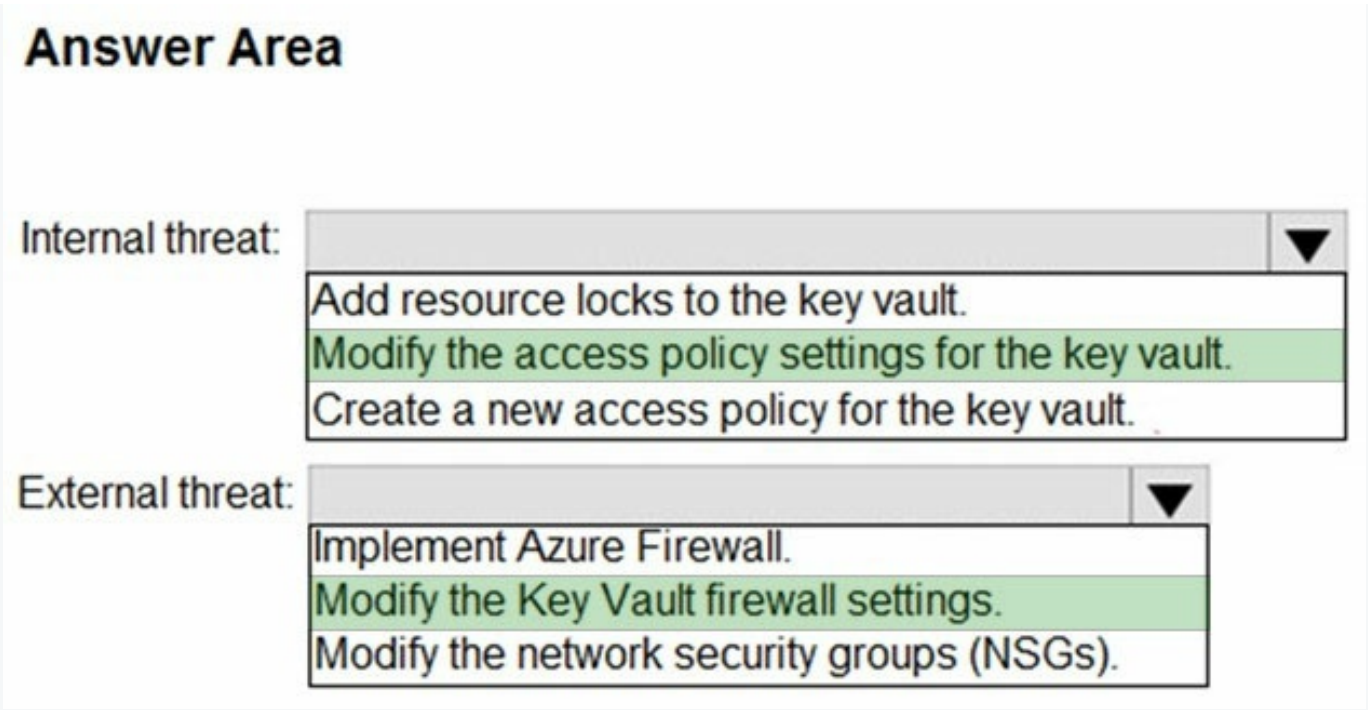
HOTSPOT -
You need to recommend remediation actions for the Azure Defender alerts for Fabrikam.
What should you recommend for each threat? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.
Hot Area:

Answer Area



Answer:

Answer Area



Explanation:

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

Question: 277 CertyIQ

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

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

Answer: B

Explanation:

"Defender for Cloud helps you limit exposure to brute force attacks."

Reference:

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

Question: 278 CertyIQ

DRAG DROP
-

You have a Microsoft Sentinel workspace named SW1.

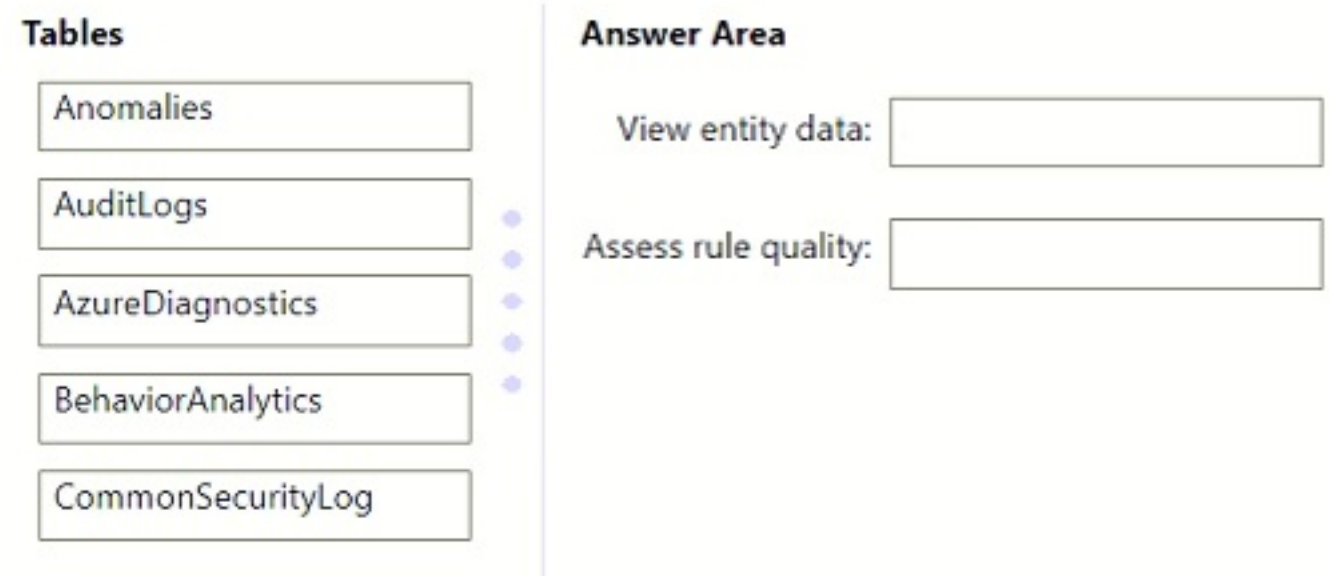
In SW1, you enable User and Entity Behavior Analytics (UEBA).

You need to use KQL to perform the following tasks:

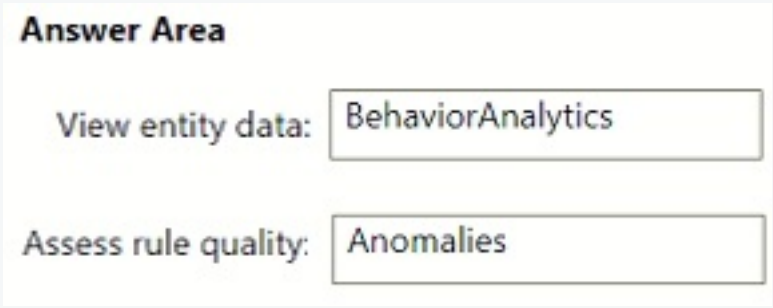
•View the entity data that has fields for each type of entity.
•Assess the quality of rules by analyzing how well a rule performs.

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:



Question: 279 CertyIQ

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.AADServicePrincipalRiskEvents
B.AADDomainServicesAccountLogon
C.SigninLogs
D.IdentityLogonEvents

Answer: D

Explanation:

Reference:

https://learn.microsoft.com/en-us/azure/azure-monitor/reference/queries/identitylogonevents

Question: 280 CertyIQ

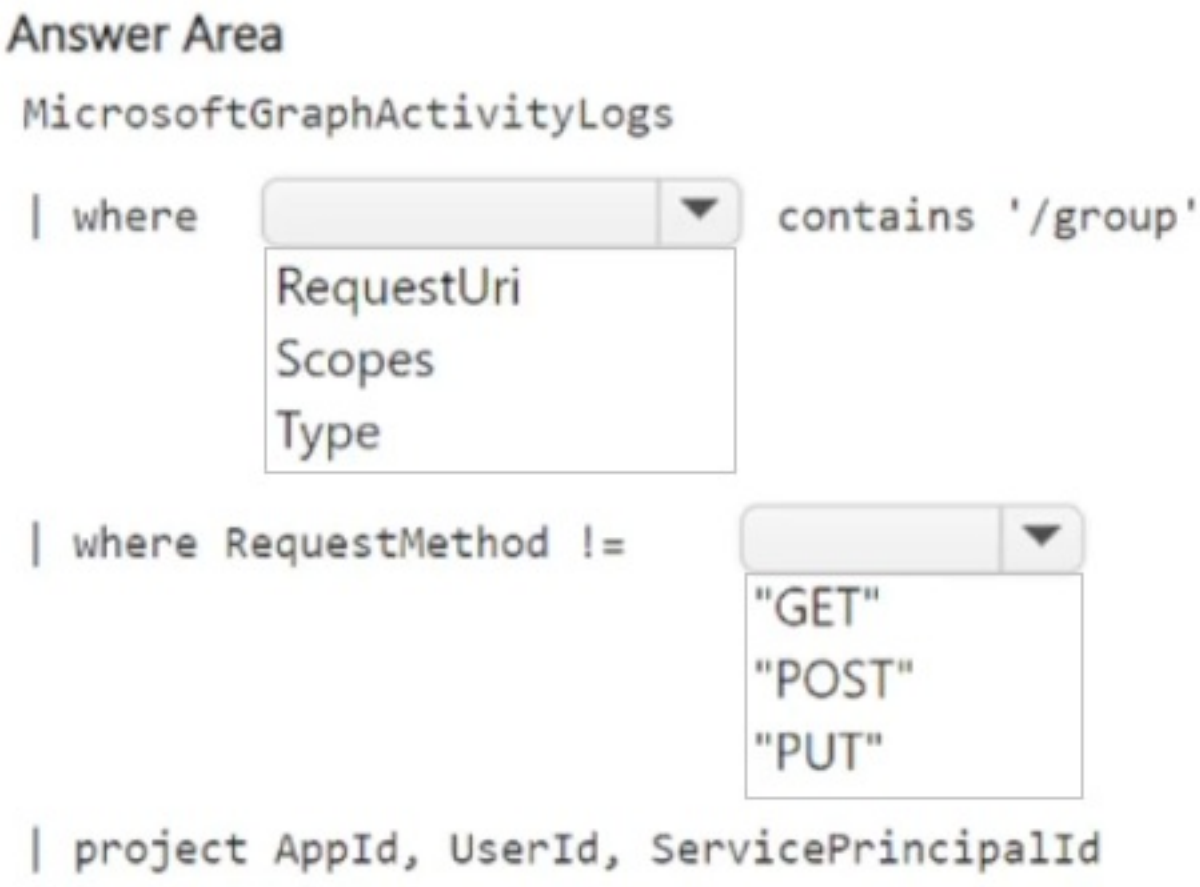
HOTSPOT
-

You have a Microsoft 365 subscription.

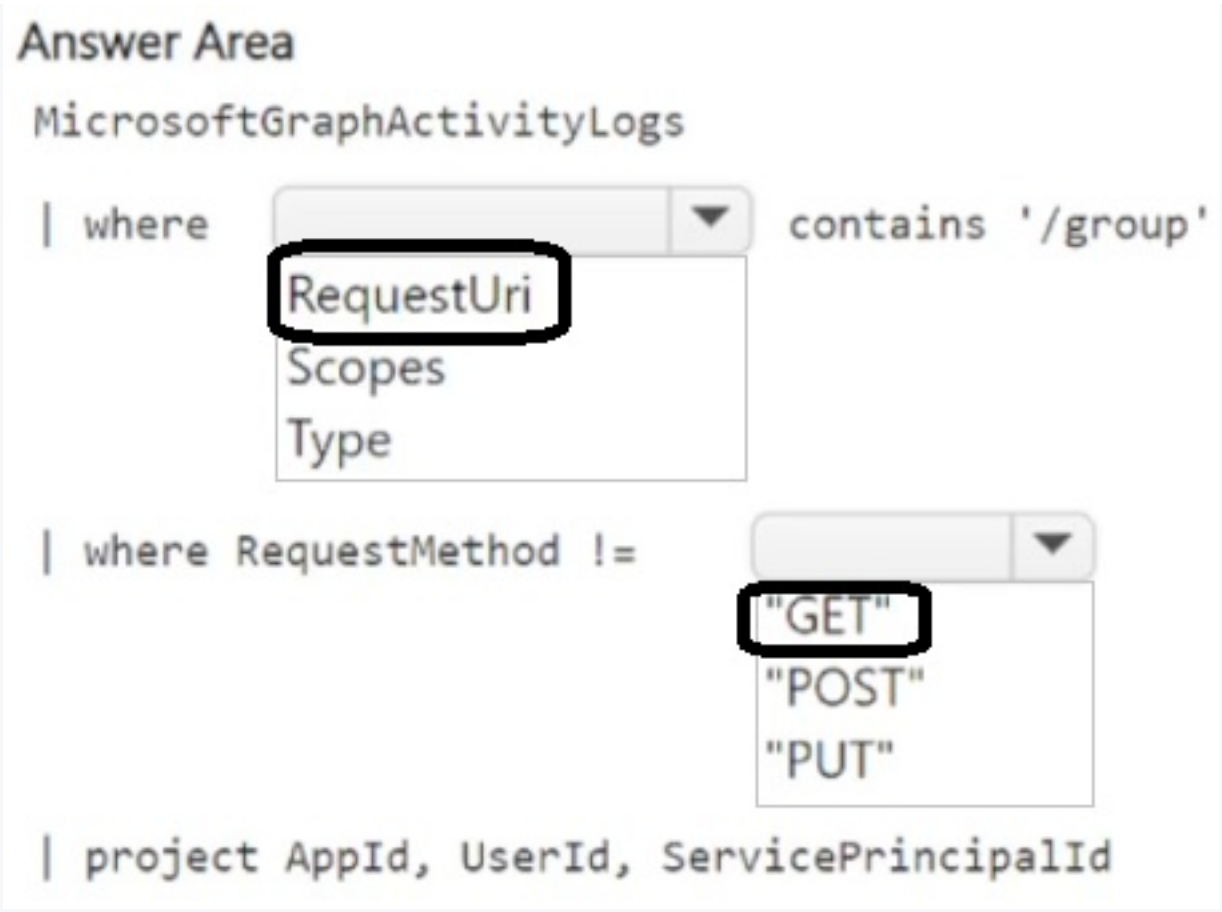
You need to identify all the security principals that submitted requests to change or delete groups.

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:

Request Uri

"GET"

Question: 281 CertyIQ

You have a Microsoft 365 subscription that uses Microsoft Defender for Endpoint Plan 2 and contains a macOS device named Device1.

You need to investigate a Defender for Endpoint agent alert on Device1. The solution must meet the following requirements:

•Identify all the active network connections on Device1.
•Identify all the running processes on Device1.
•Retrieve the login history of Device1.
•Minimize administrative effort.

What should you do first from the Microsoft Defender portal?

A.From Devices, click Collect investigation package for Device1.
B.From Advanced features in Endpoints, enable Live Response unsigned script execution.
C.From Devices, initiate a live response session on Device1.
D.From Advanced features in Endpoints, disable Authenticated telemetry.

Answer: A

Explanation:

From Devices, click Collect investigation package for Device1.

Question: 282 CertyIQ

HOTSPOT
-

You have a Microsoft Sentinel workspace.

You plan to visualize data from Microsoft SharePoint Online and OneDrive sites.

You need to create a KQL query for the visual. The solution must meet the following requirements:

•Select all workloads as a single operation.
•Include two parameters named Operations and Users.
•In the results, exclude empty values for the site URLs.

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

```
OfficeActivity
[ ▼ ]
| where Operation in ((Operations))
| where Operation in ({Operations})
| where ("{Operations}"=="AH" or {Operations})
| where "{Operations:lable}" = = "AH" or Operation in ({Operations})

| where OfficeWorkload in ('OneDrive', 'SharePoint')
[ ▼ ]
| project Site_Url
| where Operation != ''
| where SiteUrl != ''
| where SiteUrl =~ ''

| summarize Number = count() by Site_Url, UserId, Operation, TimeGenerated
```

Answer:

Answer Area

```
OfficeActivity
[ ▼ ]
| where Operation in ((Operations))
| where Operation in ({Operations})
| where ("{Operations}"=="AH" or {Operations})
| where "{Operations:lable}" = = "AH" or Operation in ({Operations})

| where OfficeWorkload in ('OneDrive', 'SharePoint')
[ ▼ ]
| project Site_Url
| where Operation != ''
| where SiteUrl != ''
| where SiteUrl =~ ''
| summarize Number = count() by Site_Url, UserId, Operation, TimeGenerated
```

Question: 283 CertyIQ

HOTSPOT
-

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 Area

```
SecurityEvent
| summarize count() by [ ▼ ] ( [ ▼ ] , 7d)
| render timechart
```

bin
coalesce
extract
max_of

Account
EventID
ProcessId
TimeGenerated

Answer:

Answer Area

```
SecurityEvent
| summarize count() by [ bin ▼ ] ( [ TimeGenerated ▼ ] , 7d)
| render timechart
```

bin, coalesce, extract, max_of

Account, EventID, ProcessId, TimeGenerated

Question: 284 CertyIQ

HOTSPOT
-

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

You need to create a visual in Workbook1 that will display the logon count for accounts that have logon event IDs of 4624 and 4634.

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 == "4624"
| summarize LogOnCount=count() by EventID, Account
| project LogOnCount, Account
|  [ ]  kind = [ ] (
```

[ ] options: join, project, summarize, union

[ ] options: full, inner, left, right

```
  SecurityEvent
  | where EventID == "4634"
  | summarize LogOffCount=count() by EventID, Account
  | project LogOffCount, Account
) on Account
```

Answer:

Answer Area

Question: 285 CertyIQ

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.SeenBy()
B.DeviceFromIP()
C.next()
D.current_cluster_endpoint()

Answer: A

Explanation:

By invoking the SeenBy function, in your advanced hunting query, you can get detail on which onboarded device a discovered device was seen by. This information can help determine the network location of each discovered device and subsequently, help to identify it in the network.

https://learn.microsoft.com/en-us/defender-endpoint/device-discovery

Question: 286 CertyIQ

You have an Azure subscription that contains a resource group named RG1. RG1 contains a Microsoft Sentinel workspace. The subscription is linked to a Microsoft Entra tenant that contains a user named User1.

You need to ensure that User1 can deploy and customize Microsoft Sentinel workbook templates. The solution must follow the principle of least privilege.

Which role should you assign to User1 for RG1?

A.Microsoft Sentinel Contributor
B.Workbook Contributor
C.Microsoft Sentinel Automation Contributor
D.Contributor

Answer: B

Explanation:

Correct answer is B:Workbook Contributor.

Question: 287 CertyIQ

HOTSPOT
-

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:

Answer Area

```
DeviceEvents
| where ingestion_time() > ago(1d)
| where ActionType == "AntivirusDetection"
| summarize (Timestamp, [ ])=arg_max(Timestamp, [ ]), count(
| where count_ > 5
```

DeviceId	DeviceId
InitiatingProcessAccountObjectId	InitiatingProcessAccountObjectId
ReportId	ReportId
TimeGenerated	TimeGenerated

Question: 288

CertyIQ

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

A.Security alerts in Azure Security Center

B.Activity log in Azure

C.Azure Advisor

D.the query windows of the Log Analytics workspace

Answer: D

Explanation:

D is correct. By increasing the time window, we would know if the failed sign ins are common or suspecious. The corrected code would be something like:BehaviorAnalytics| where ActivityType == "FailedLogOn"| extend ActivityInsightsArray=parse_json(ActivityInsights)| extend UnusualFailedSignIns = tostring(parse_json(ActivityInsightsArray).UnusualNumberOfFailedSignInOfThisUser)| where UnusualFailedSignIns == True| summarize count() by SourceIPLocation, UserName| order by count_ desc

Question: 289

CertyIQ

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

D.Azure Sentinel livestreams

Answer: B

Explanation:

Logic Apss = Playbooks which provide automated workflows to run based on triggers.

Reference:

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

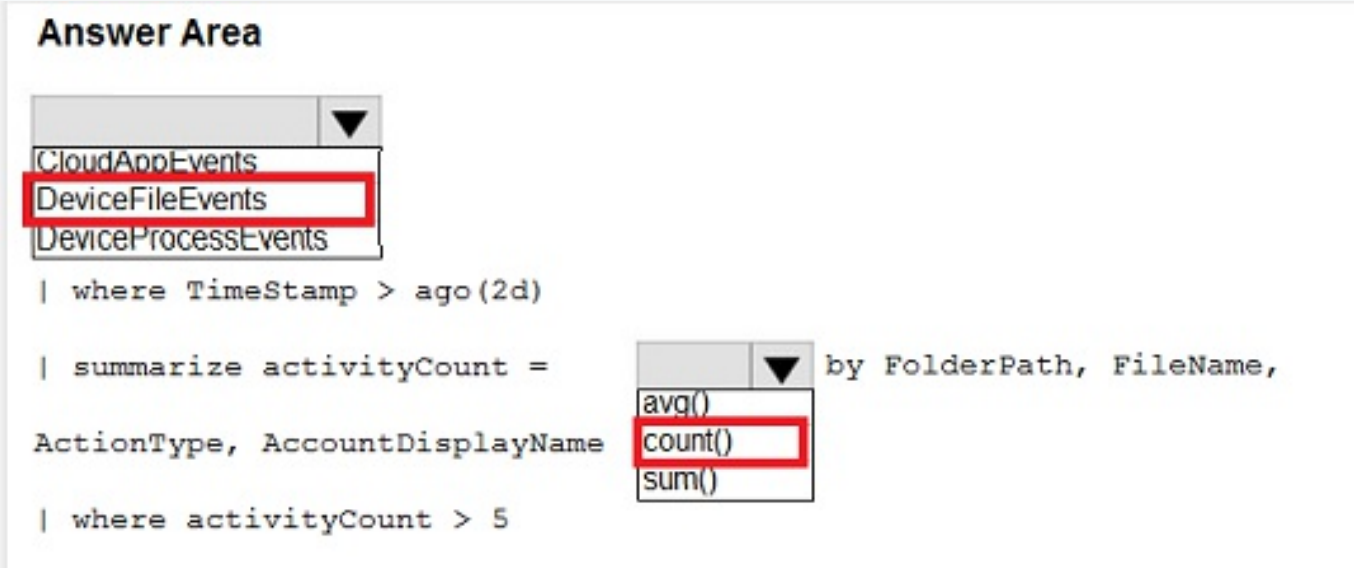
Question: 290 CertyIQ

HOTSPOT -
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.
Hot Area:

Answer Area

```
[ CloudAppEvents | DeviceFileEvents | DeviceProcessEvents ]
| where TimeStamp > ago(2d)
| summarize activityCount = [ avg() | count() | sum() ] by FolderPath, FileName,
ActionType, AccountDisplayName
| where activityCount > 5
```

Answer:



Explanation:

CloudAppEvents doesn't have the FolderPath column, so it's probably DeviceFileEvents:
https://docs.microsoft.com/en-us/microsoft-365/security/defender/advanced-hunting-devicefileevents-table?view=o365-worldwide

Question: 291 CertyIQ

HOTSPOT -
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.
Hot Area:

Answer Area

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

- 0
- 1
- 2
- 3

Query element required to correlate data between tenants:

- extend
- project
- workspace

Answer:

Answer Area

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

- 0
- 1
- 2
- 3

Query element required to correlate data between tenants:

- extend
- project
- workspace

Explanation:

1 workspace (every sentinel requires a workspace)

Reference:

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

Question: 292 CertyIQ

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

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

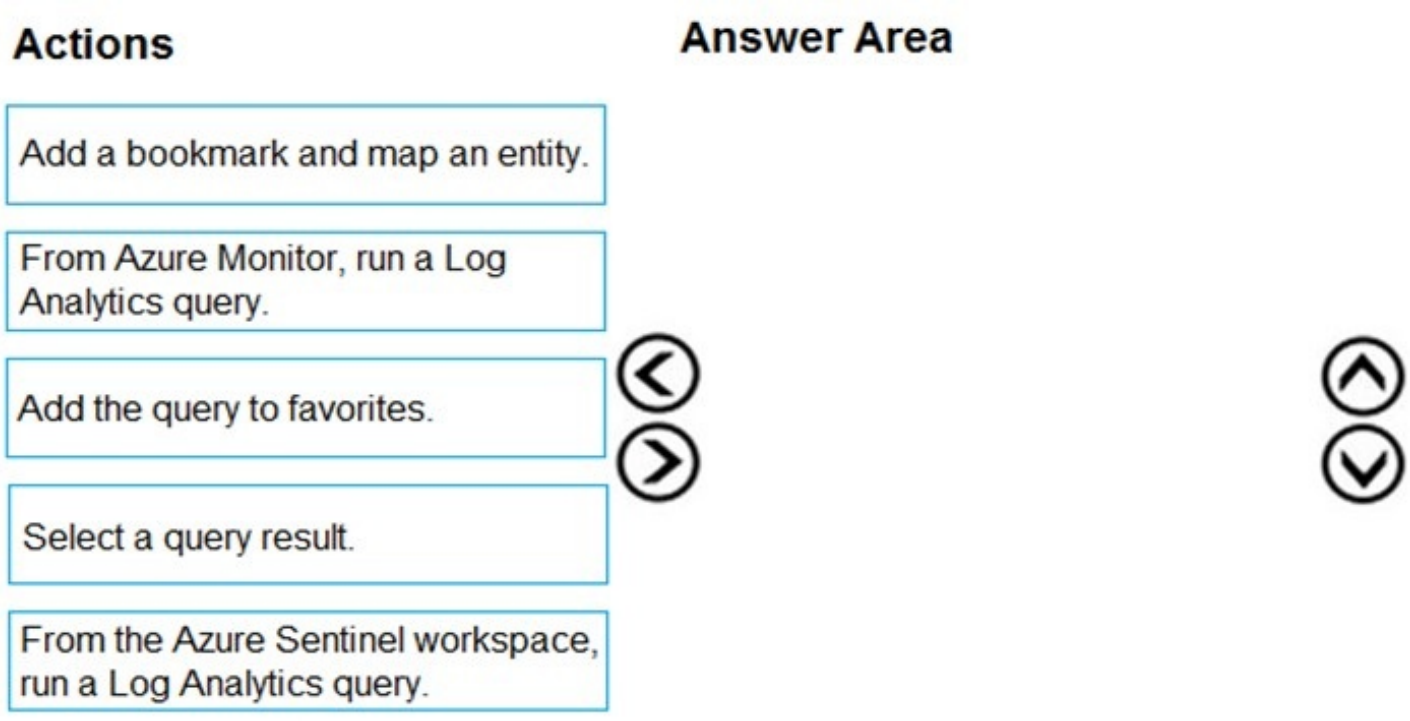
Answer: CD

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

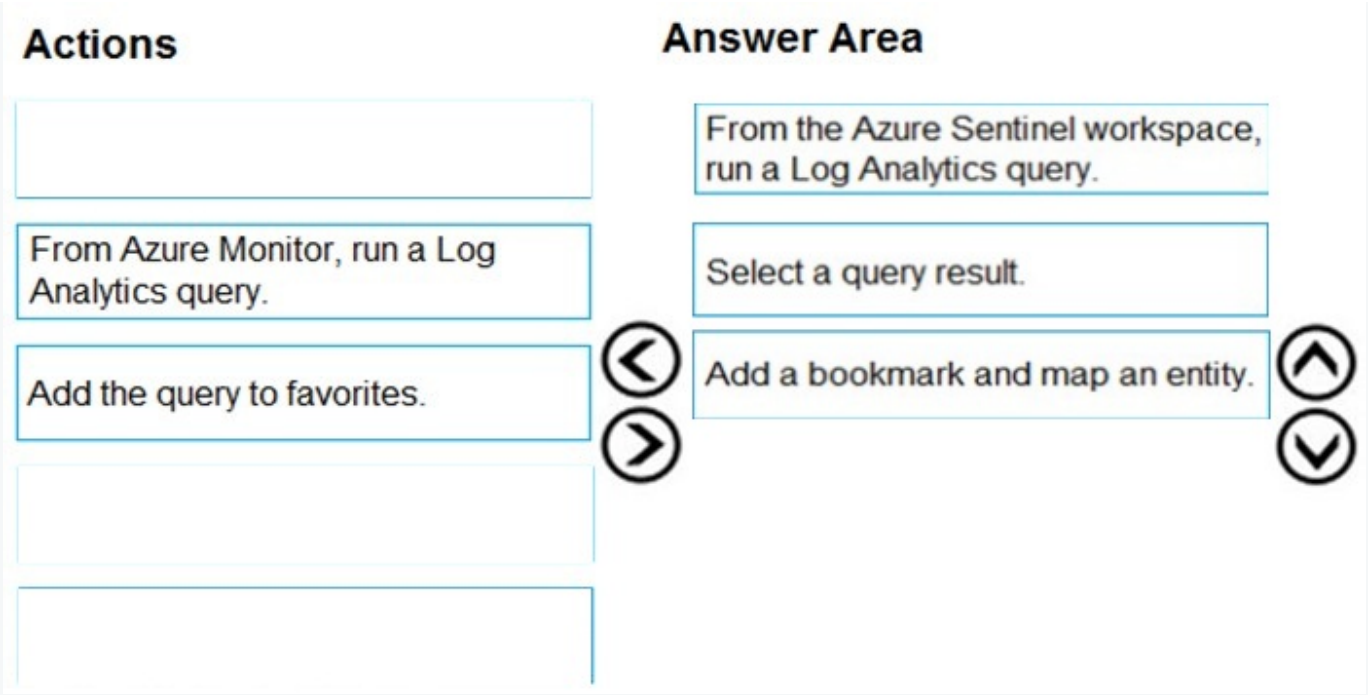
Reference:
https://docs.microsoft.com/en-us/cloud-app-security/mde-govern

Question: 293 CertyIQ

DRAG DROP -
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.
Select and Place:



Answer:

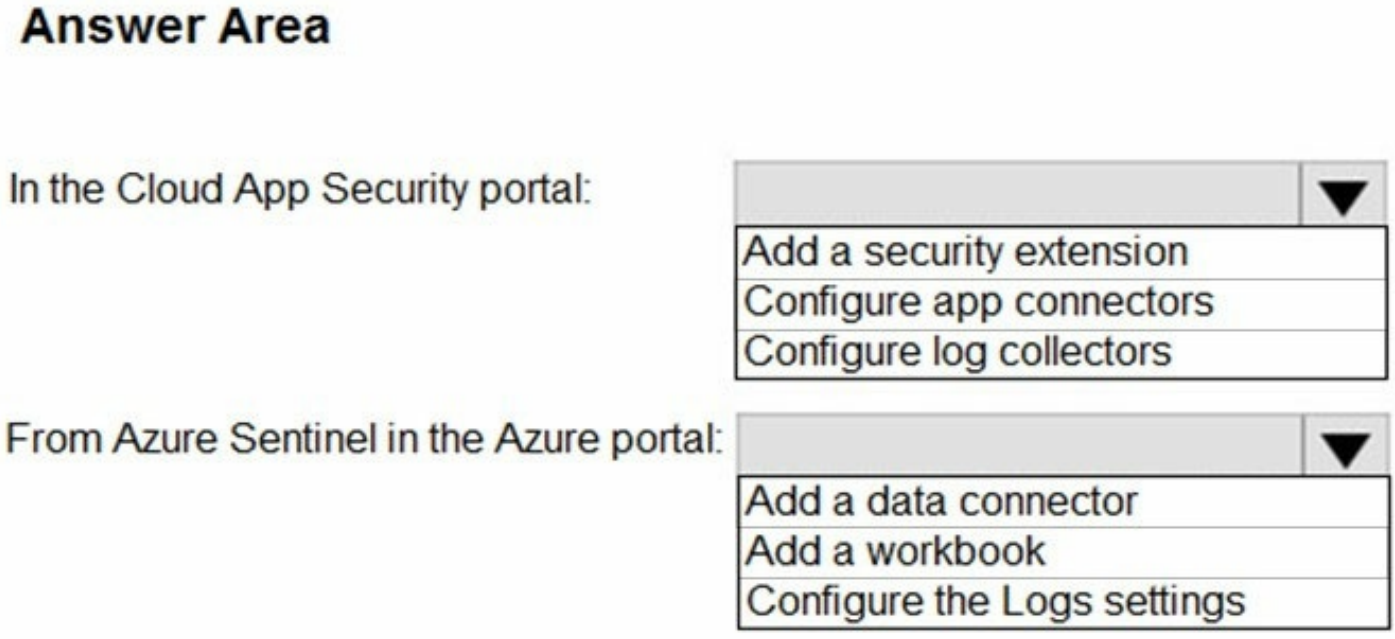


Explanation:

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

Question: 294 CertyIQ

HOTSPOT -
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.
Hot Area:



Answer:

Answer Area

In the Cloud App Security portal:

- Add a security extension
- Configure app connectors
- Configure log collectors

From Azure Sentinel in the Azure portal:

- Add a data connector
- Add a workbook
- Configure the Logs settings

Explanation:

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

Question: 295 CertyIQ

You need to assign a role-based access control (RBAC) role to admin1 to meet the Azure Sentinel requirements and the business requirements.
Which role should you assign?

A.Automation Operator
B.Automation Runbook Operator
C.Azure Sentinel Contributor
D.Azure Sentinel Responder

Answer: C

Explanation:
Litware must meet the following requirements:
➩ Ensure that a user named admin1 can configure Azure Sentinel playbooks.
➩ The principle of least privilege must be used whenever possible.
Azure Sentinel Contributor can view data, incidents, workbooks, and other Azure Sentinel resources, manage incidents (assign, dismiss, etc.), create and edit workbooks, analytics rules, and other Azure Sentinel resources.

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

Question: 296 CertyIQ

Which rule setting should you configure to meet the Azure Sentinel requirements?

A.From Set rule logic, turn off suppression.
B.From Analytics rule details, configure the tactics.

C.From Set rule logic, map the entities.

D.From Analytics rule details, configure the severity.

Answer: C

Explanation:

Correct answer. Check any analytics rules, after you map the entities under the "Set rule logic" tab, then you can enable the "Alert grouping" under "Incident settings" by selecting "Enabled", then select "Grouping alerts into a single incident if the selected entity types and details match:" and select the entities from the drop down menu.If you don't map entities, you can't group alerts under "Incident settings" becuase the drop down menu will show "no available items".

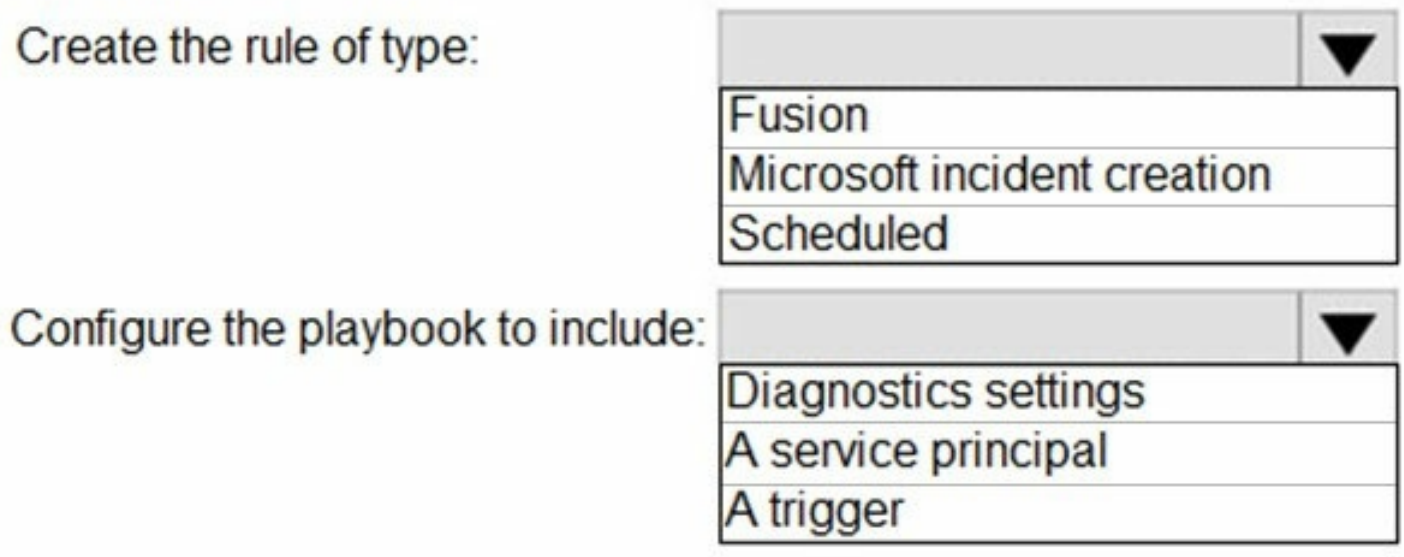
Reference:

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

Question: 297 CertyIQ

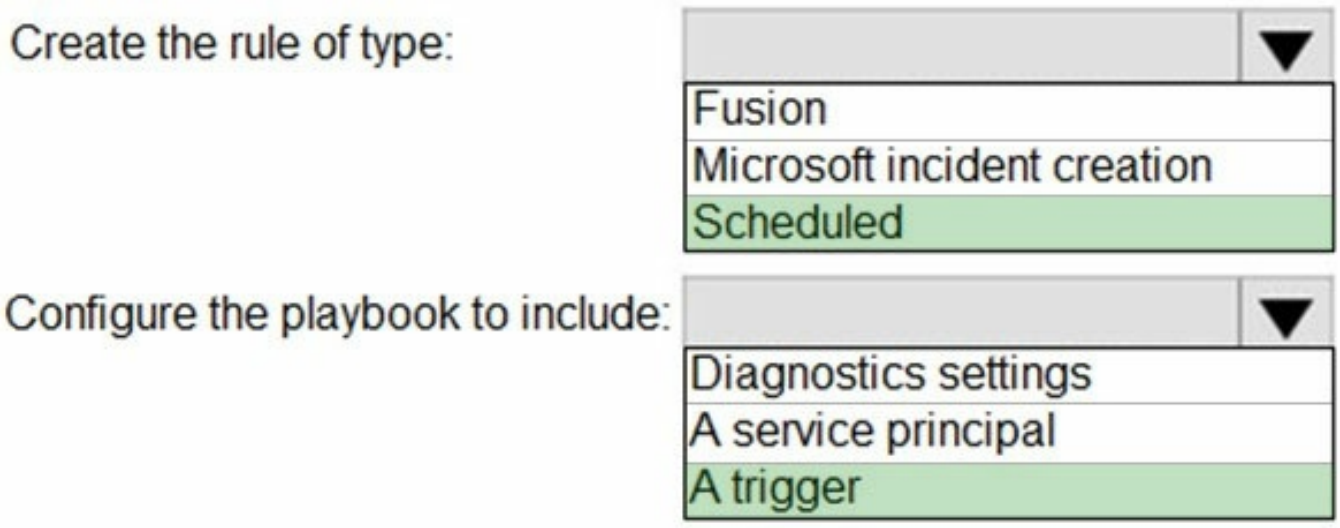
HOTSPOT -
You need to create the analytics rule to meet the Azure Sentinel requirements.
What should you do? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.
Hot Area:

Answer Area



Answer:

Answer Area



Explanation:

Reference:
https://docs.microsoft.com/en-us/azure/sentinel/tutorial-detect-threats-custom#set-automated-responses-and-create-the-rule https://docs.microsoft.com/en-us/azure/sentinel/tutorial-respond-threats-playbook

Thank you

Thank you for being so interested in the premium exam material.
I'm glad to hear that you found it informative and helpful.

If you have any feedback or thoughts on the bumps, I would love to hear them.
Your insights can help me improve our writing and better understand our readers.

Best of Luck

You have worked hard to get to this point, and you are well-prepared for the exam
Keep your head up, stay positive, and go show that exam what you're made of!

Feedback

More Papers

Future is Secured

100% Pass Guarantee

24/7 Customer Support

Mail us - certyiqofficial@gmail.com

Free Updates

Lifetime Free Updates!

Total: **297 Questions**

Link: https://certyiq.com/papers/microsoft/sc-200