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.

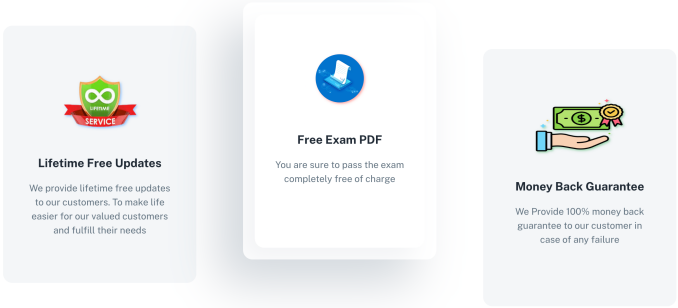
The misuse of the preparation system has left our team disillusioned. And for that reason, we decided it was time to make a difference. We had to make In this way, CertyIQ was created to provide quality materials without stealing from everyday people who are trying to make a living.

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: **370 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
```

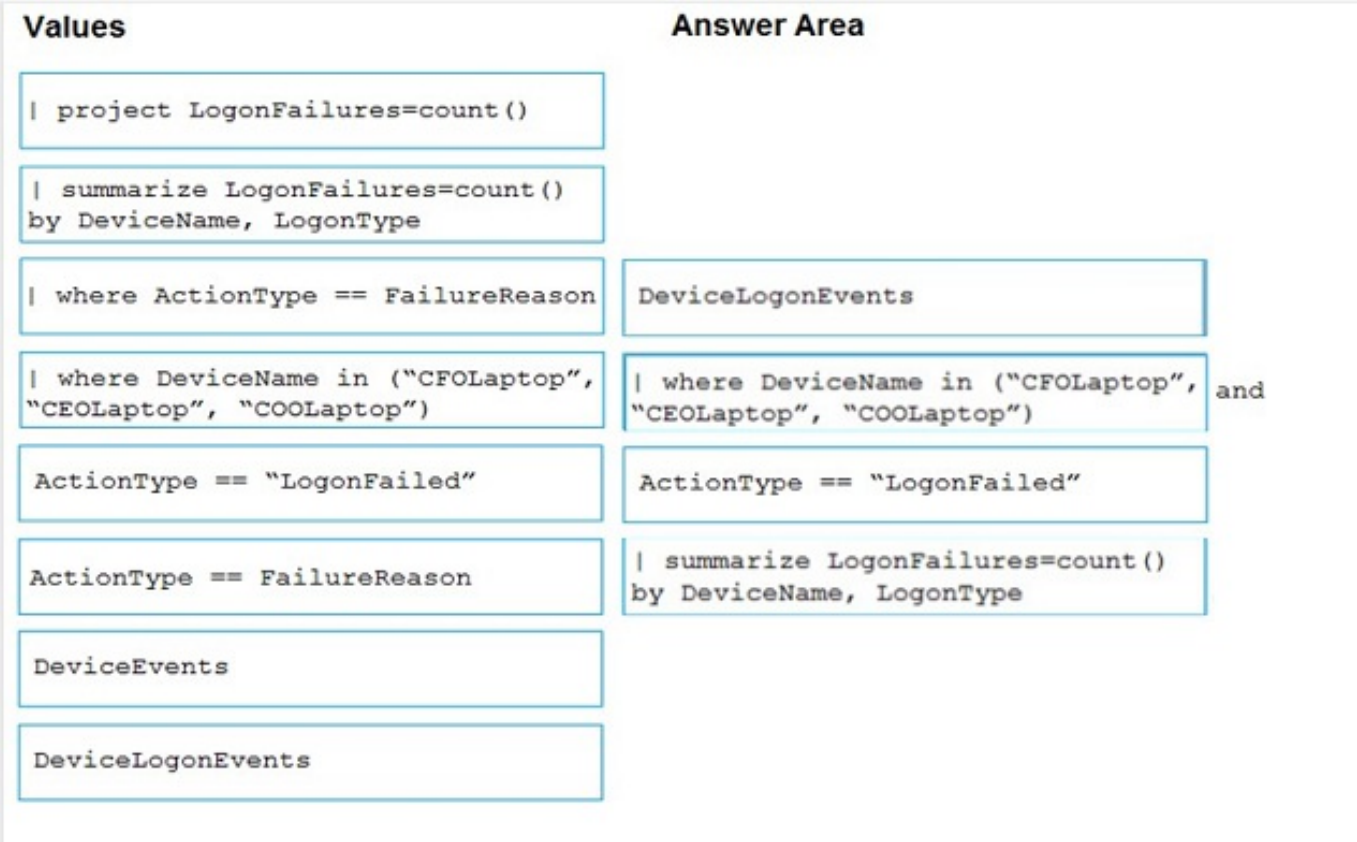
Answer Area

[ ] 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.

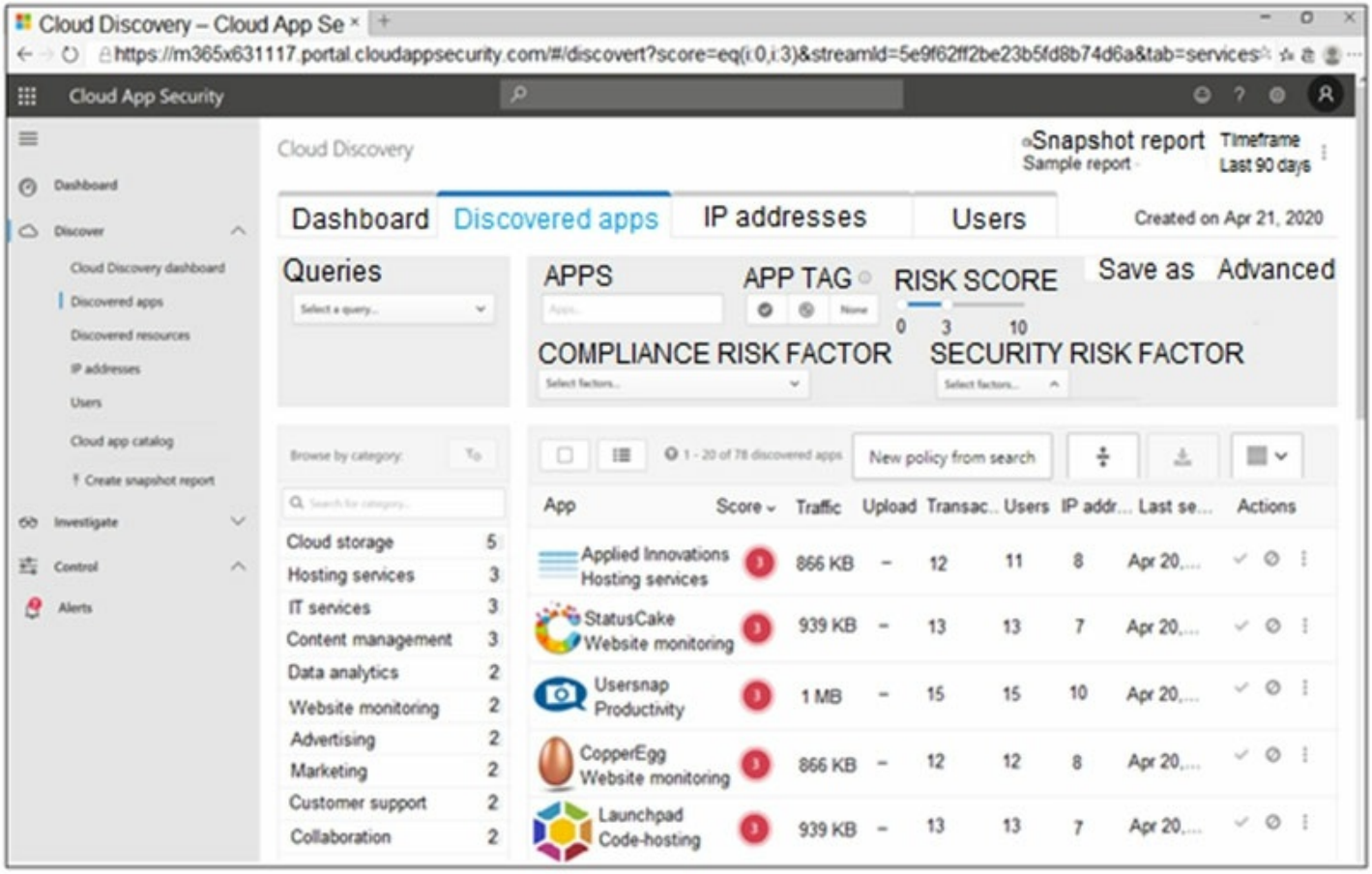
D. Create a suppression rule scoped to a device group: You can also create a suppression rule scoped to a specific device group if you want to only apply it to a specific group of devices. This helps you maintain the existing security posture.

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.



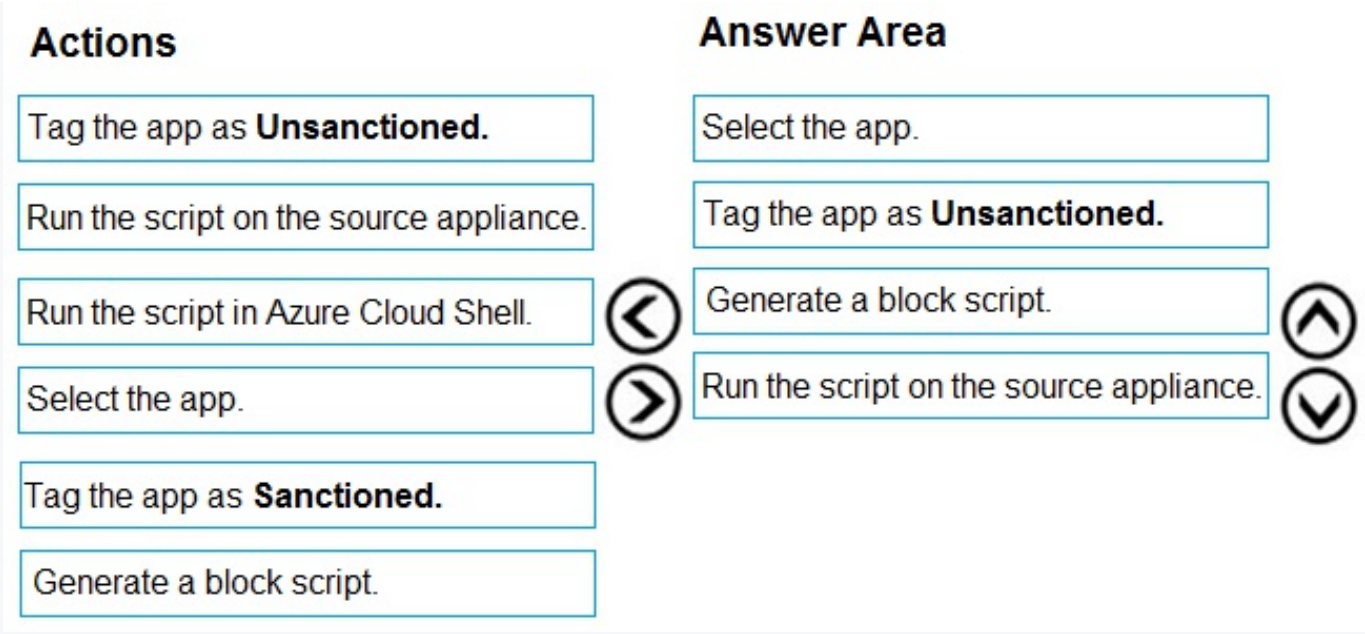
Your environment does NOT have Microsoft Defender for Endpoint enabled.
You need to remediate the risk for the Launchpad app.
Which four actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.
Select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

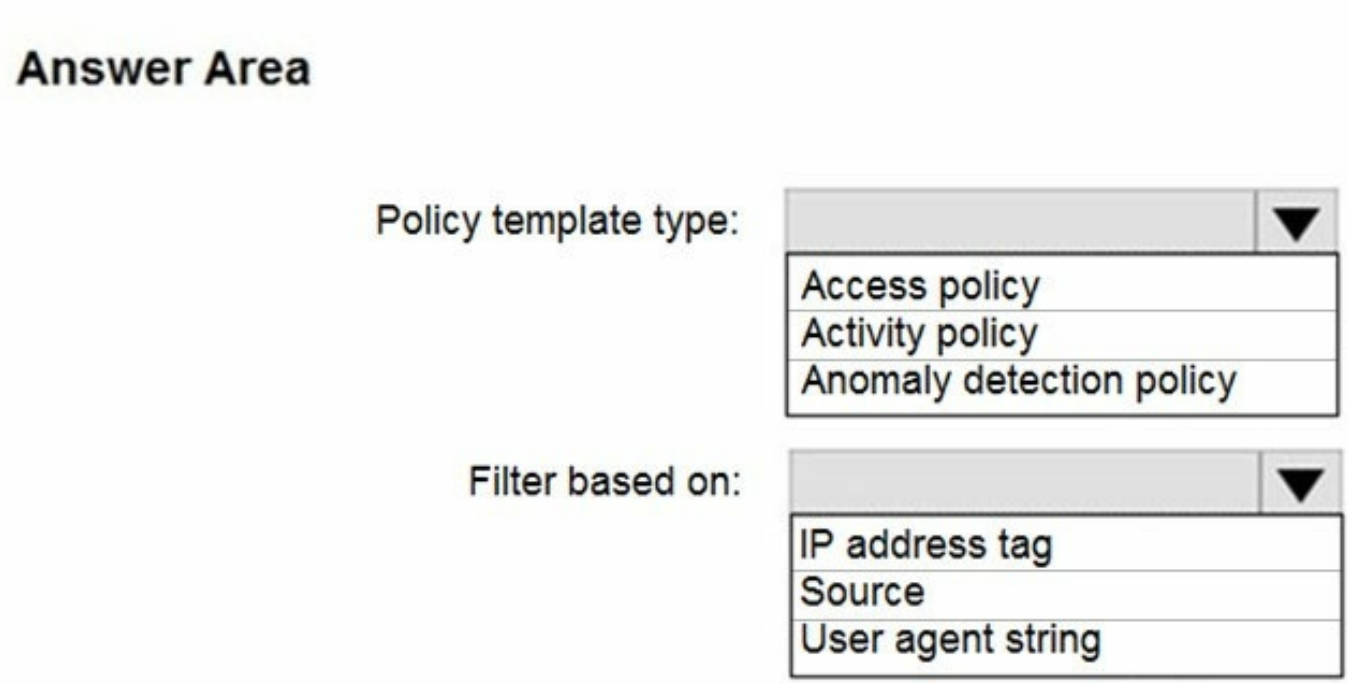
Explanation:

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.

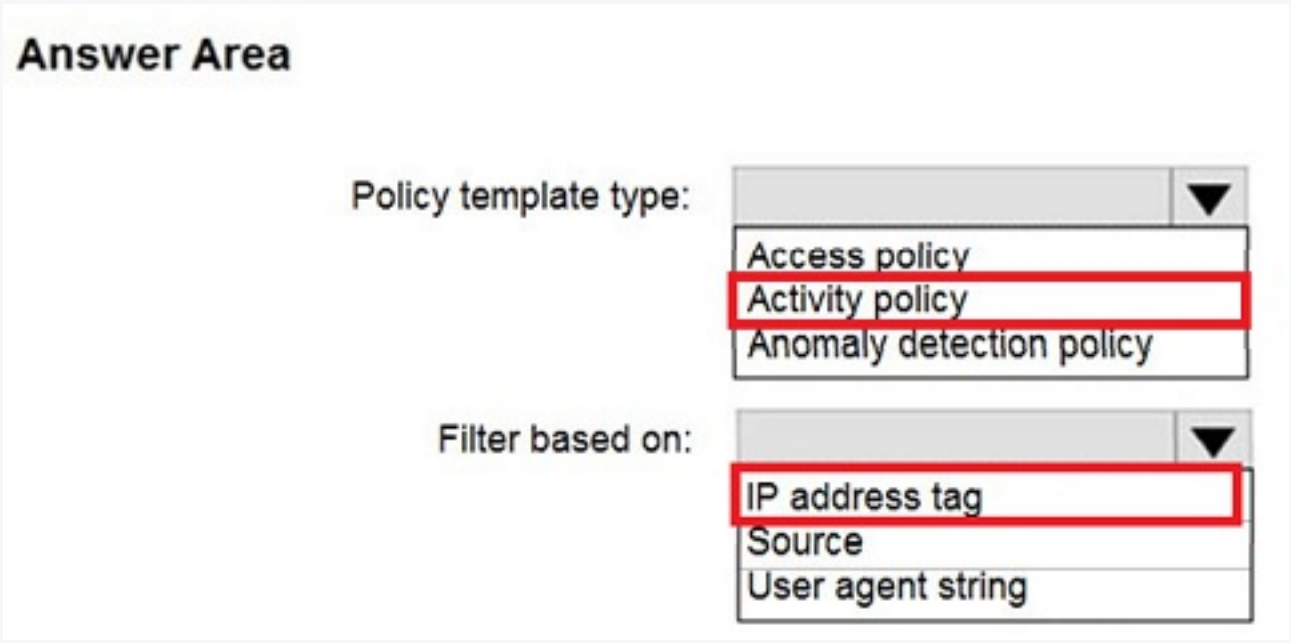
E. From Settings, select Information Protection, select Files, and then enable file monitoring. This will enable Cloud App Security to monitor files for external sharing and other activities, and to generate alerts and trigger remediation actions in response to potential threats or policy violations.

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: AD

Explanation:

A. **Configure automatic data enrichment:** Automatic data enrichment in Microsoft Cloud App Security helps to enhance the context of alerts and logs by adding relevant information. This can include details such as user profiles, IP addresses, and locations. By enabling data enrichment, legitimate sign-ins from known IP addresses can be recognized more effectively, reducing false positives from alerts.

D. **Add the IP addresses to the other address range category and add a tag:** By adding the IP addresses of your corporate offices to the "other address range" category and tagging them appropriately, you can help Microsoft Cloud App Security recognize these IP addresses as trusted. This means that sign-ins from these locations will be less likely to trigger alerts for impossible travel or risky IP addresses, as the system will know these are legitimate sources.

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

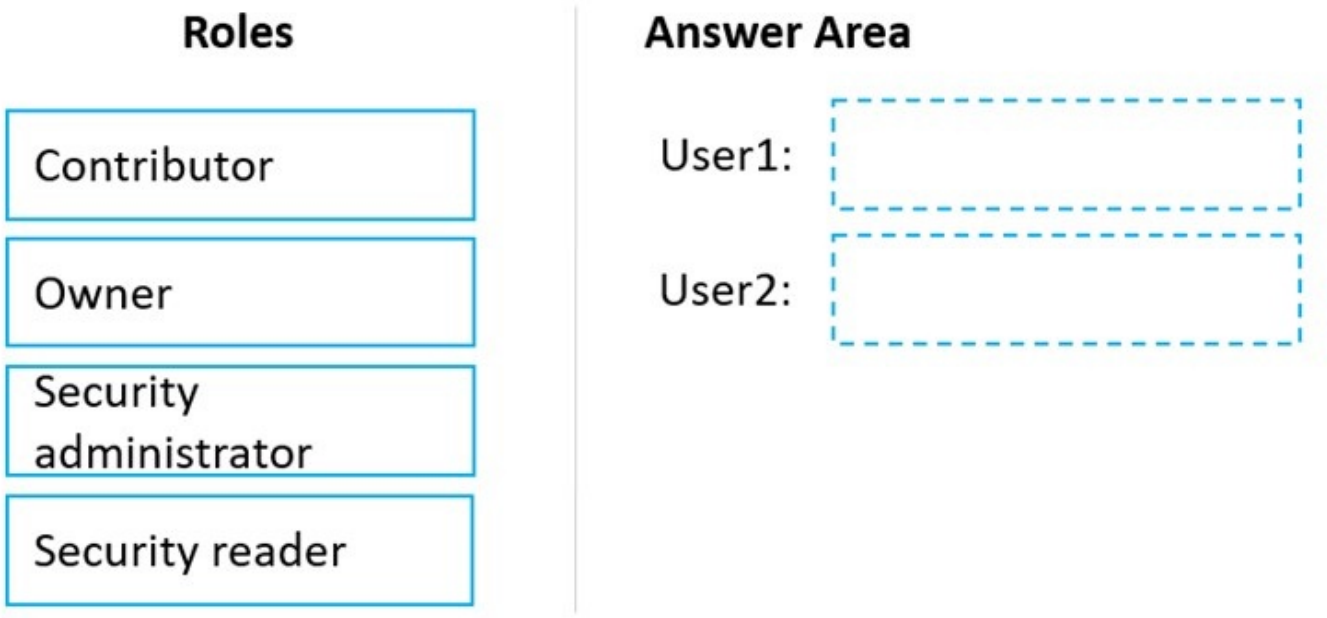
Question: 26 CertyIQ

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.

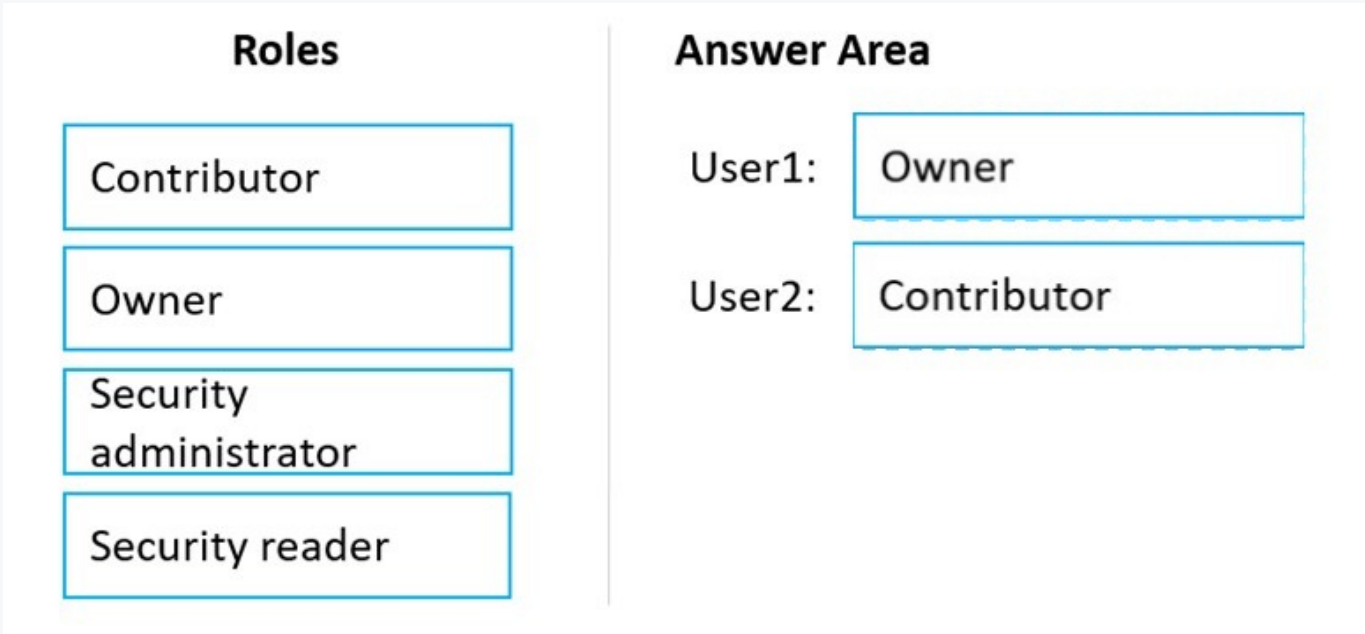
User	Task
User1	• Assign initiatives • Edit security policies • Enable automatic provisioning
User2	• View alerts and recommendations • Apply security recommendations • Dismiss alerts

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:

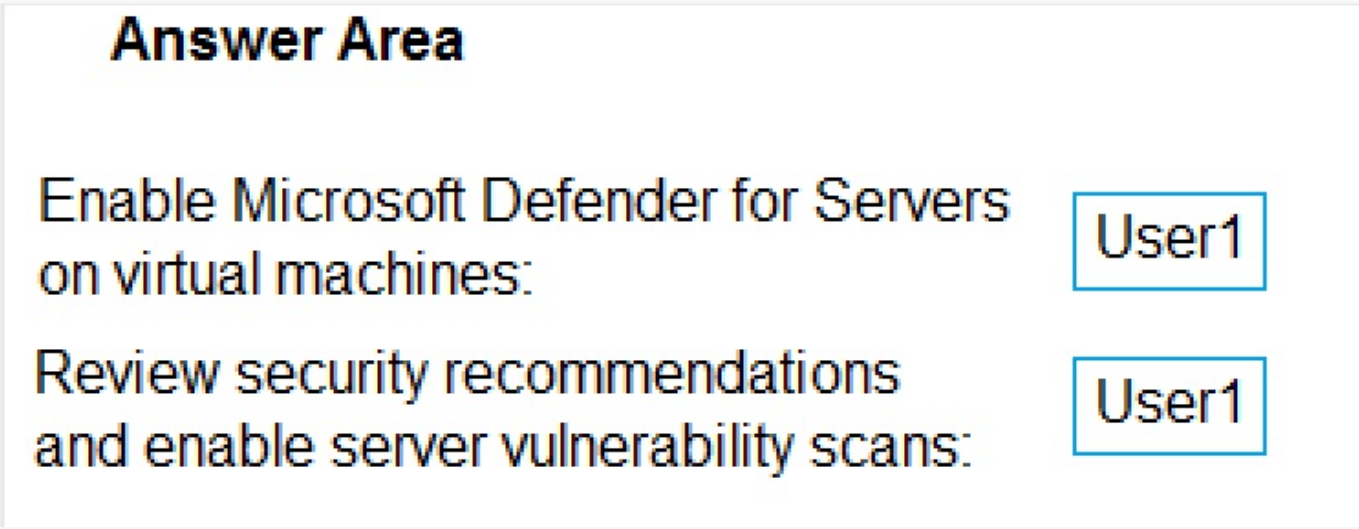
•Enable Microsoft Defender for Servers on virtual machines.
•Review security recommendations and enable server vulnerability scans.

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.

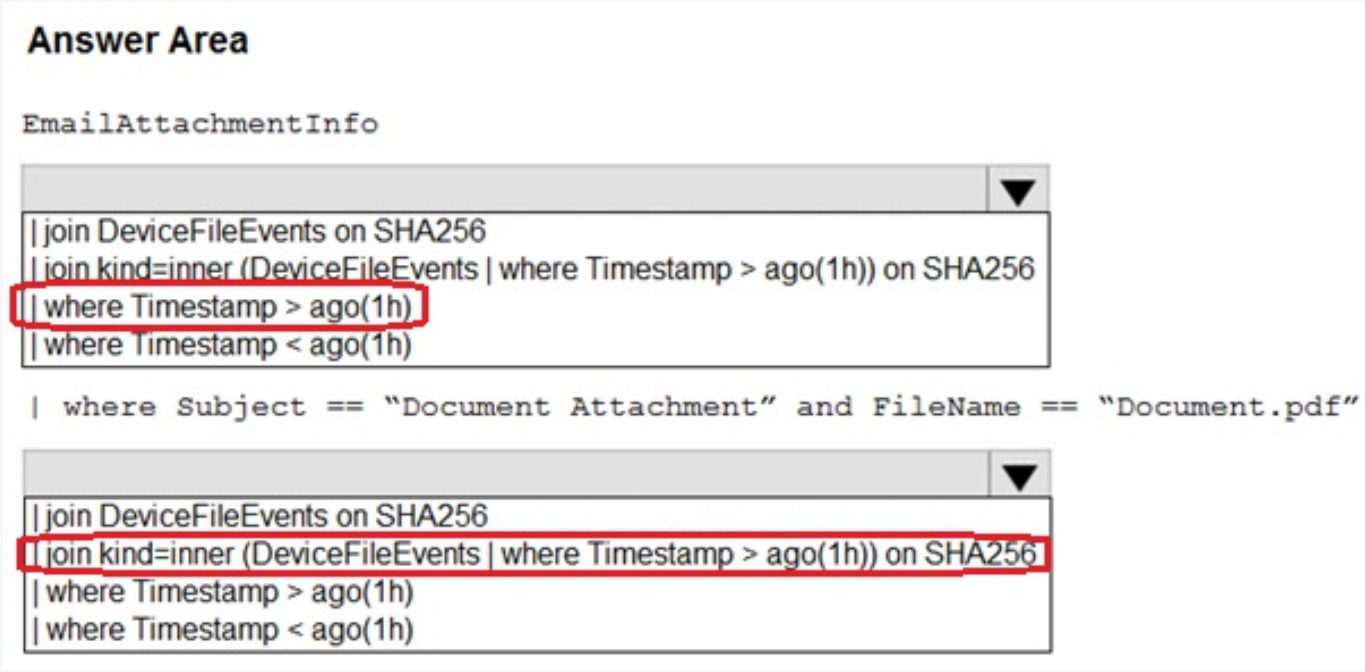
Answer Area

```
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.

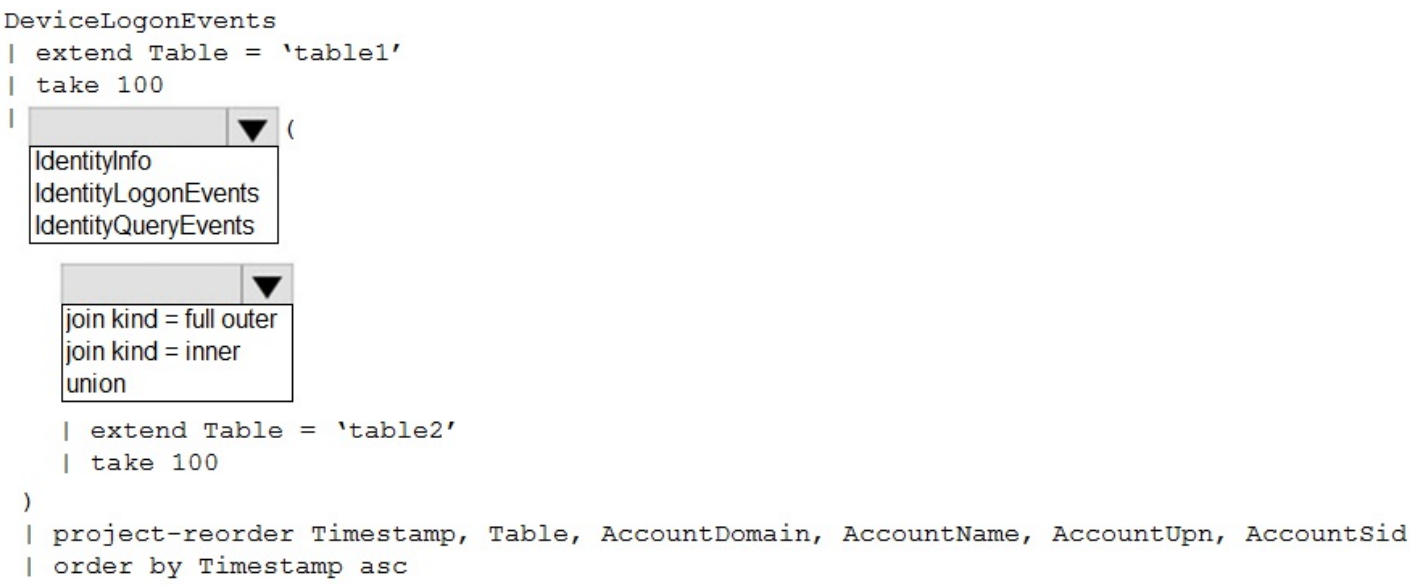
Your network contains an on-premises Active Directory Domain Services (AD DS) domain that syncs with Azure AD.

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.

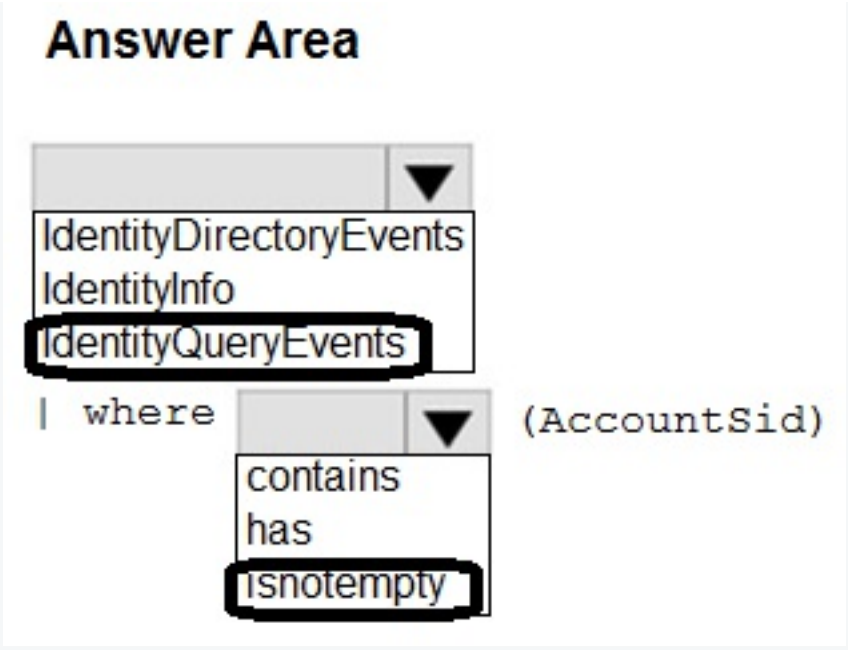
How should you complete the KQL query? To answer, select the appropriate options in the answer area.

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.

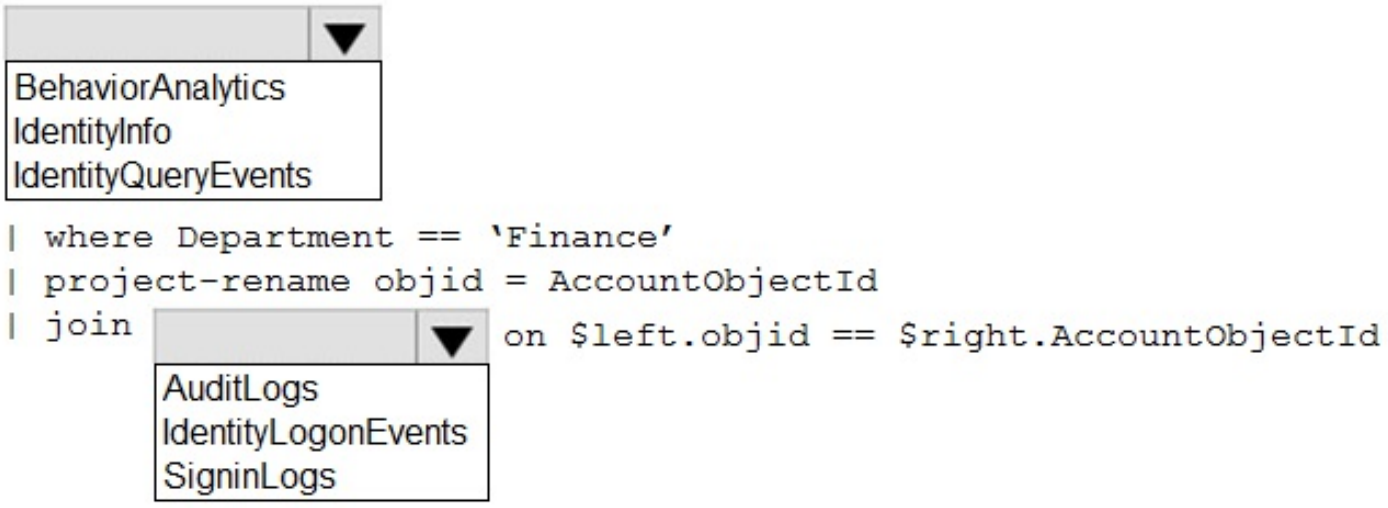
You have a Microsoft 365 E5 subscription that uses Microsoft Defender 365.

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.

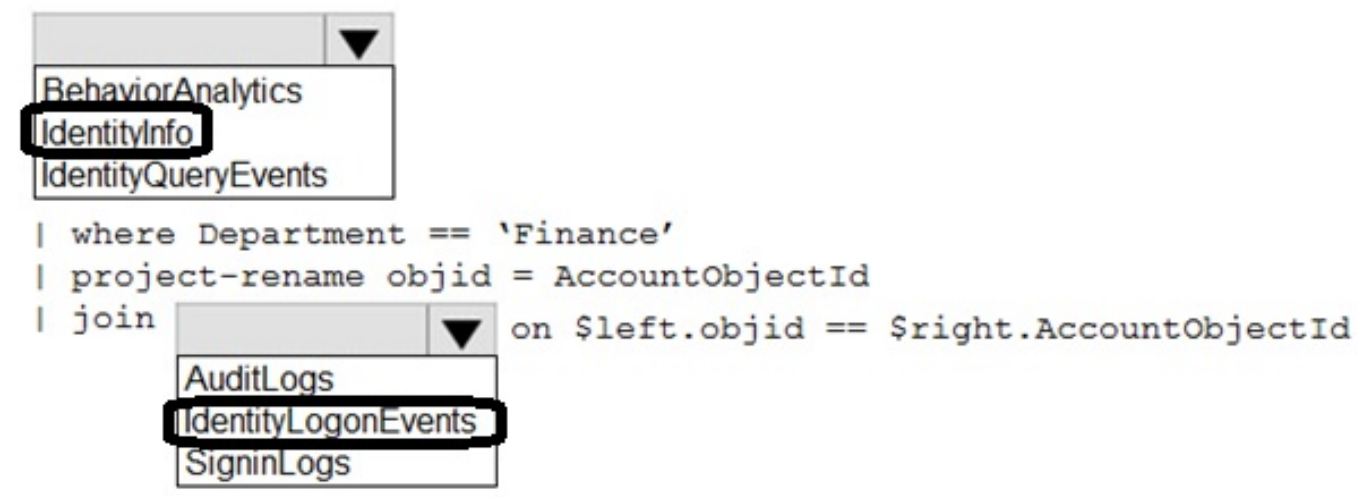
NOTE: Each correct selection is worth one point.

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

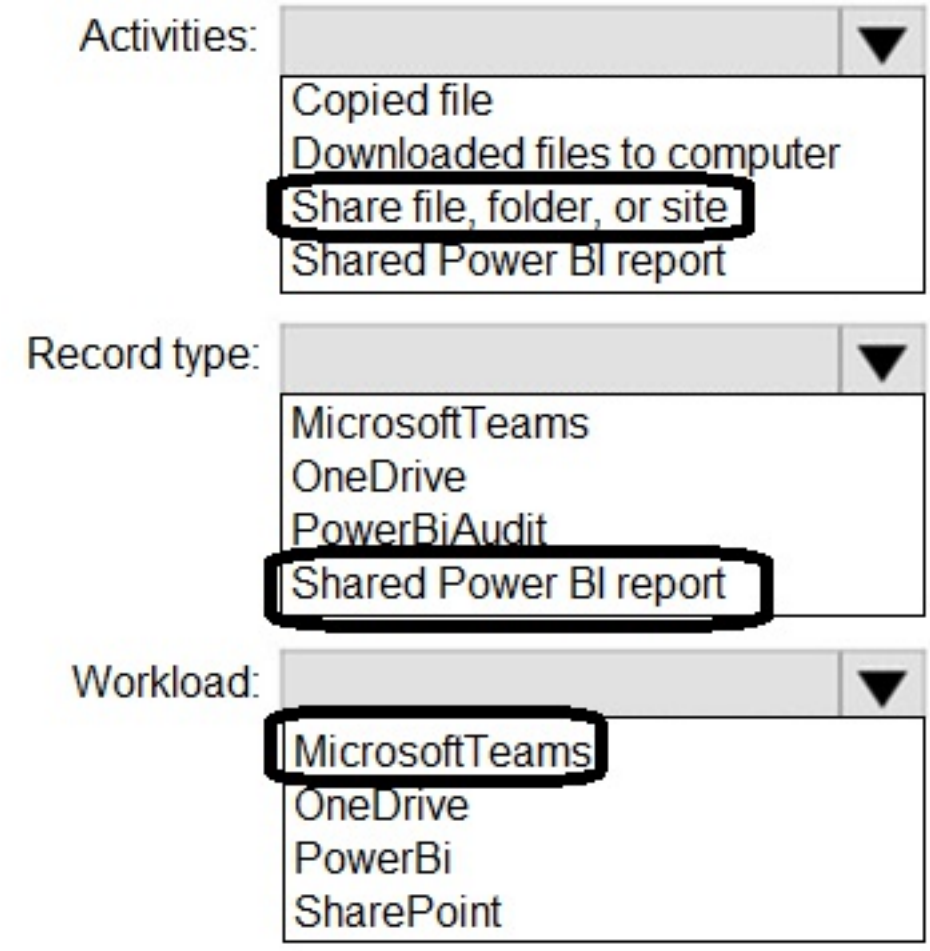
Activities:
- Copied file
- Downloaded files to computer
- Share file, folder, or site
- Shared Power BI report

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.

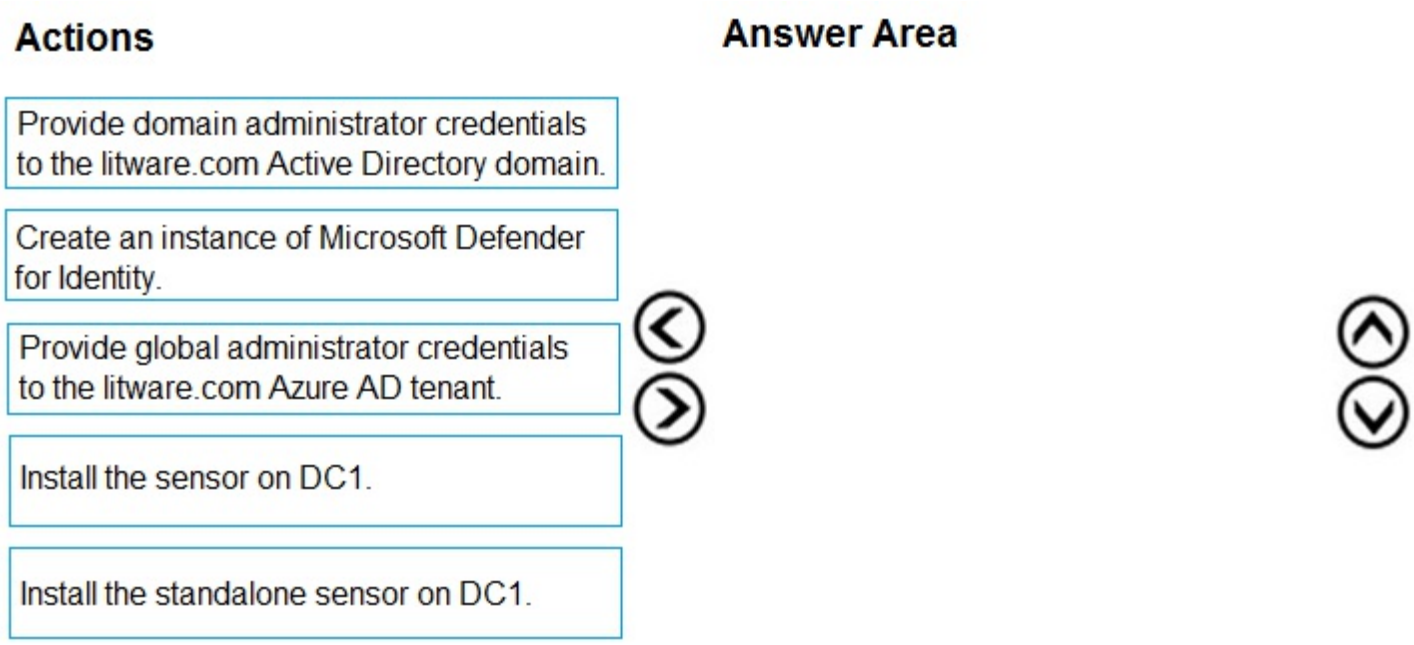
Microsoft Sentinel Requirements

Litware must meet the following Microsoft Sentinel requirements:

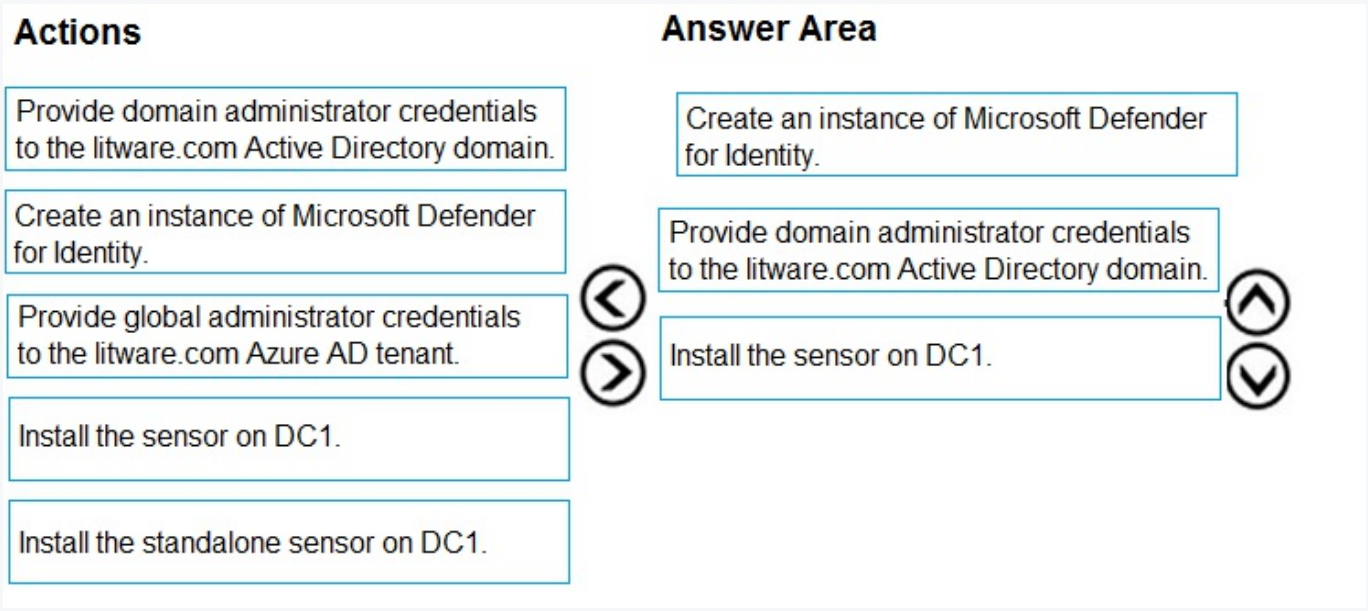
•Integrate Microsoft Sentinel and Microsoft Defender for Cloud Apps.
•Ensure that a user named admin1 can configure Microsoft Sentinel playbooks.
•Create a Microsoft Sentinel analytics rule based on a custom query. The rule must automatically initiate the execution of a playbook.
•Add notes to events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

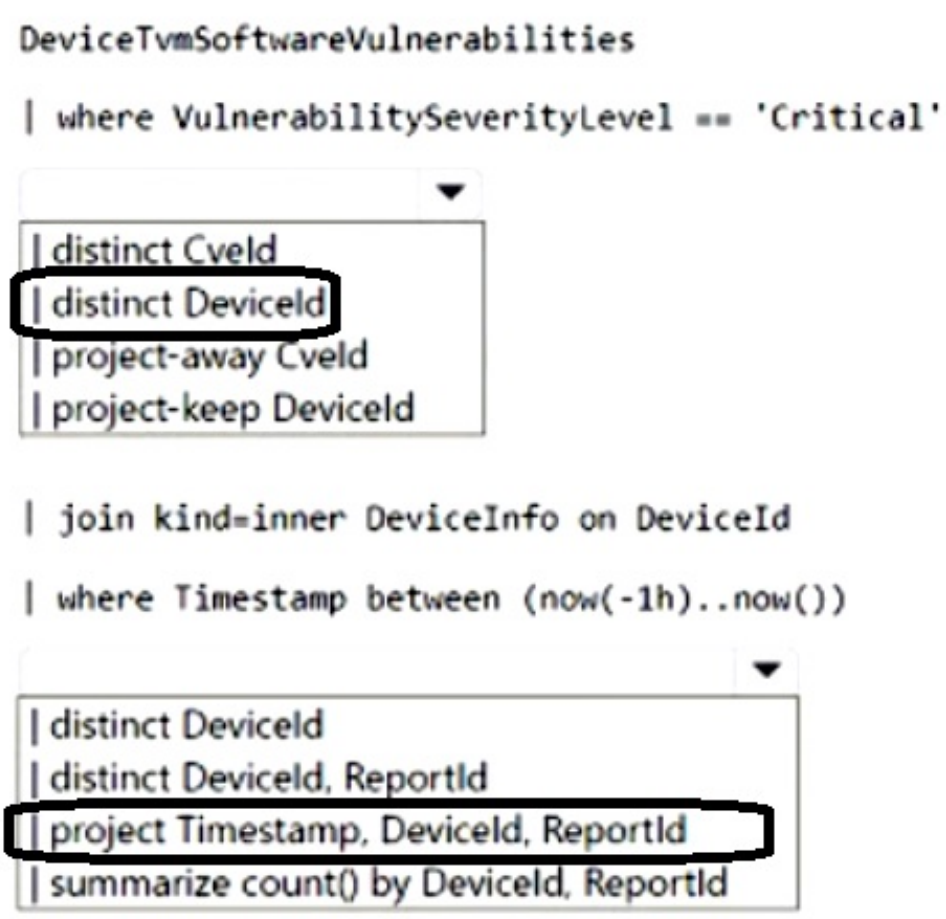
```
| join kind=inner DeviceInfo on DeviceId
| where Timestamp between (now(-1h)..now())
```

[▼]

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

Answer:

Answer Area



Question: 57 CertyIQ

HOTSPOT
-

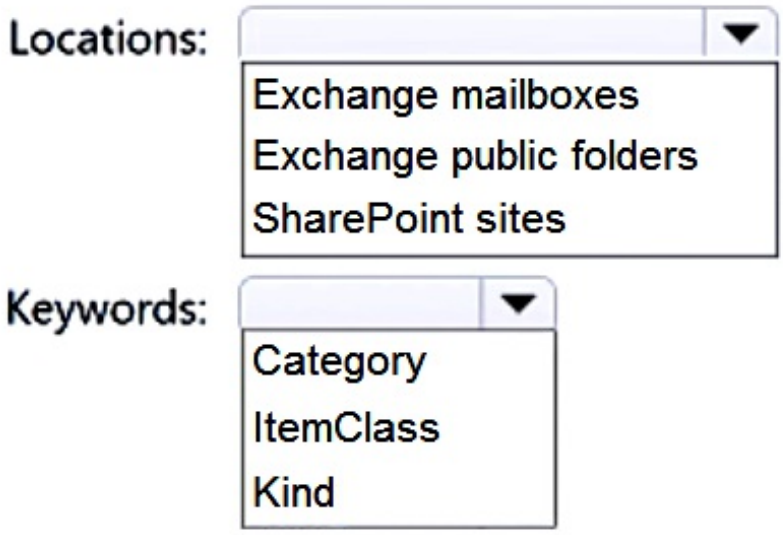
You have a Microsoft 365 E5 subscription that uses Microsoft Teams.

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.

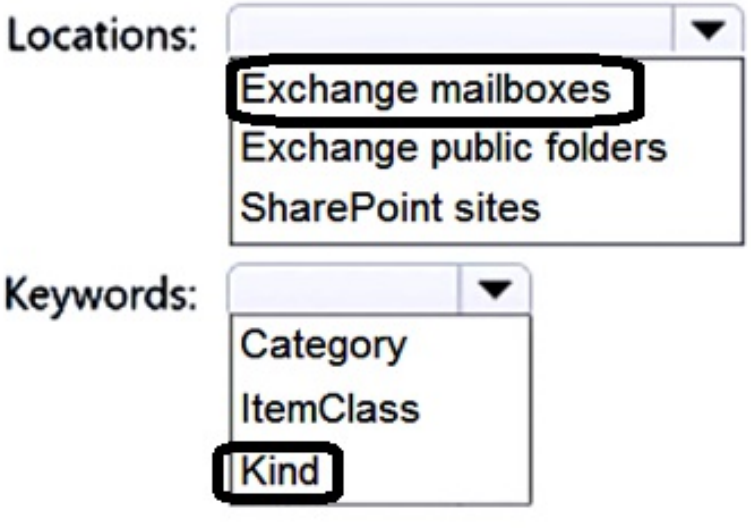
NOTE: Each correct selection is worth one point.

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

You have a Microsoft 365 subscription that uses Microsoft Purview.

Your company has a project named Project1.

You need to identify all the email messages that have the word Project1 in the subject line. The solution must search only the mailboxes of users that worked on Project1.

What should you do?

A.Perform a user data search.
B.Create a records management disposition.
C.Perform an audit search.
D.Perform a content search.

Answer: D

Explanation:

Perform a content search.

Question: 61 CertyIQ

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

You discover that when Microsoft Defender for Endpoint generates alerts for a commonly used executable file, it causes alert fatigue.

You need to tune the alerts.

Which two actions can an alert tuning rule perform for the alerts? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

A.delete
B.hide
C.resolve
D.merge
E.assign

Answer: BC

Explanation:

https://techcommunity.microsoft.com/blog/microsoftthreatprotectionblog/boost-your-detection-and-response-workflows-with-alert-tuning/3824712

Question: 62 CertyIQ

Note: This section contains one or more sets of questions with the same scenario and problem. Each question presents a unique solution to the problem. You must determine whether the solution meets the stated goals. More than one solution in the set might solve the problem. It is also possible that none of the solutions in the set solve the problem.

After you answer a question in this section, you will NOT be able to return. As a result, these questions do not appear on the Review Screen.

You have a Microsoft 365 subscription.

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

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

Solution: You configure endpoint detection and response (EDR) in block mode.

Does this meet the goal?

A.Yes
B.No

Answer: A

Explanation:

A. YesConfiguring Endpoint Detection and Response (EDR) in block mode meets the goal.EDR in block mode allows Microsoft Defender for Endpoint to detect and remediate malicious artifacts even when Microsoft Defender Antivirus is in passive mode due to the presence of a third-party antivirus. This ensures that threats missed by the third-party antivirus can still be addressed by Microsoft Defender for Endpoint's advanced detection and response capabilities.Thus, enabling EDR in block mode effectively provides the required protection in this scenario.

Question: 63 CertyIQ

Note: This section contains one or more sets of questions with the same scenario and problem. Each question presents a unique solution to the problem. You must determine whether the solution meets the stated goals. More than one solution in the set might solve the problem. It is also possible that none of the solutions in the set solve the problem.

After you answer a question in this section, you will NOT be able to return. As a result, these questions do not appear on the Review Screen.

You have a Microsoft 365 subscription.

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

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

Solution: You configure Controlled folder access.

Does this meet the goal?

A.Yes
B.No

Answer: B

Explanation:

B. NoConfiguring Controlled Folder Access does not meet the goal. Controlled Folder Access is a feature of Microsoft Defender Antivirus that protects specific folders from unauthorized changes by ransomware or other malicious apps. However, this feature requires Microsoft Defender Antivirus to be active and does not

address the scenario where Defender Antivirus is in passive mode due to the presence of a third-party antivirus.To meet the goal of protecting the devices from malicious artifacts undetected by the third-party antivirus, you should enable EDR in block mode. EDR in block mode works even when Microsoft Defender Antivirus is in passive mode, allowing Microsoft Defender for Endpoint to remediate threats missed by the third-party antivirus.Thus, configuring Controlled Folder Access is not the correct solution in this scenario.

Question: 64 CertyIQ

Note: This section contains one or more sets of questions with the same scenario and problem. Each question presents a unique solution to the problem. You must determine whether the solution meets the stated goals. More than one solution in the set might solve the problem. It is also possible that none of the solutions in the set solve the problem.

After you answer a question in this section, you will NOT be able to return. As a result, these questions do not appear on the Review Screen.

You have a Microsoft 365 subscription.

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

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

Solution: You enable automated investigation and response (AIR).

Does this meet the goal?

A.Yes
B.No

Answer: B

Explanation:

B. No Enabling automated investigation and response (AIR) alone does not meet the goal. While AIR can investigate and respond to threats, it requires that Microsoft Defender Antivirus is active or that other components of Microsoft Defender for Endpoint, such as endpoint detection and response (EDR), are operational.Since Microsoft Defender Antivirus is in passive mode, it cannot actively scan and detect malicious artifacts that were missed by the third-party antivirus. To achieve the goal, you need to enable EDR in block mode in addition to AIR. EDR in block mode works even when Microsoft Defender Antivirus is in passive mode, allowing Microsoft Defender for Endpoint to detect and remediate threats that the third-party antivirus missed.Thus, simply enabling AIR is not sufficient to protect the devices in this scenario.

Question: 65 CertyIQ

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

You need to implement deception rules. The solution must ensure that you can limit the scope of the rules.

What should you create first?

A.device groups
B.device tags
C.honeytoken entity tags

D.sensitive entity tags

Answer: B

Explanation:

When configuring a deception role there's no option to use a device group, only device tags.
https://learn.microsoft.com/en-us/defender-xdr/configure-deception

Question: 66 CertyIQ

Note: This section contains one or more sets of questions with the same scenario and problem. Each question presents a unique solution to the problem. You must determine whether the solution meets the stated goals. More than one solution in the set might solve the problem. It is also possible that none of the solutions in the set solve the problem.

After you answer a question in this section, you will NOT be able to return. As a result, these questions do not appear on the Review Screen.

You have a Microsoft 365 subscription.

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

All Windows devices are onboarded to Microsoft Defender for Endpoint.

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

Solution: You enable Live Response.

Does this meet the goal?

A.Yes
B.No

Answer: B

Explanation:

Live Response in Microsoft Defender for Endpoint (MDE) is a tool used for investigating and remediating threats manually through an interactive remote shell. However, it does not automatically block or remediate threats missed by the third-party antivirus.To ensure protection from undetected threats, you need to enable EDR in Block Mode, which allows Defender for Endpoint to automatically block and remediate threats, even when Microsoft Defender Antivirus is in passive mode.

Question: 67 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: 68 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: 69 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

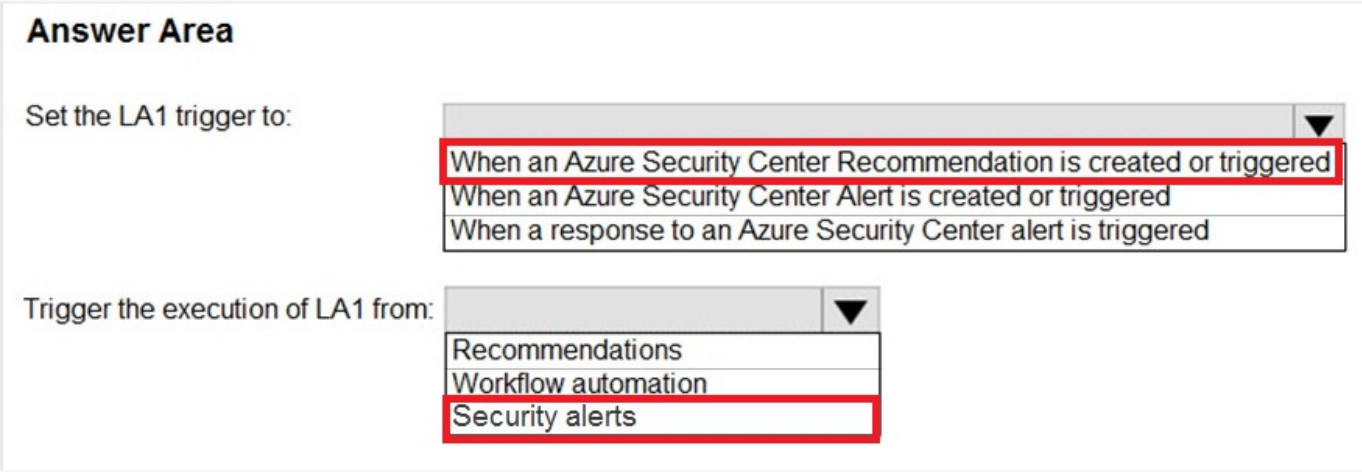
Set the LA1 trigger to:

- 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: 70 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: 71 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: 72 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:

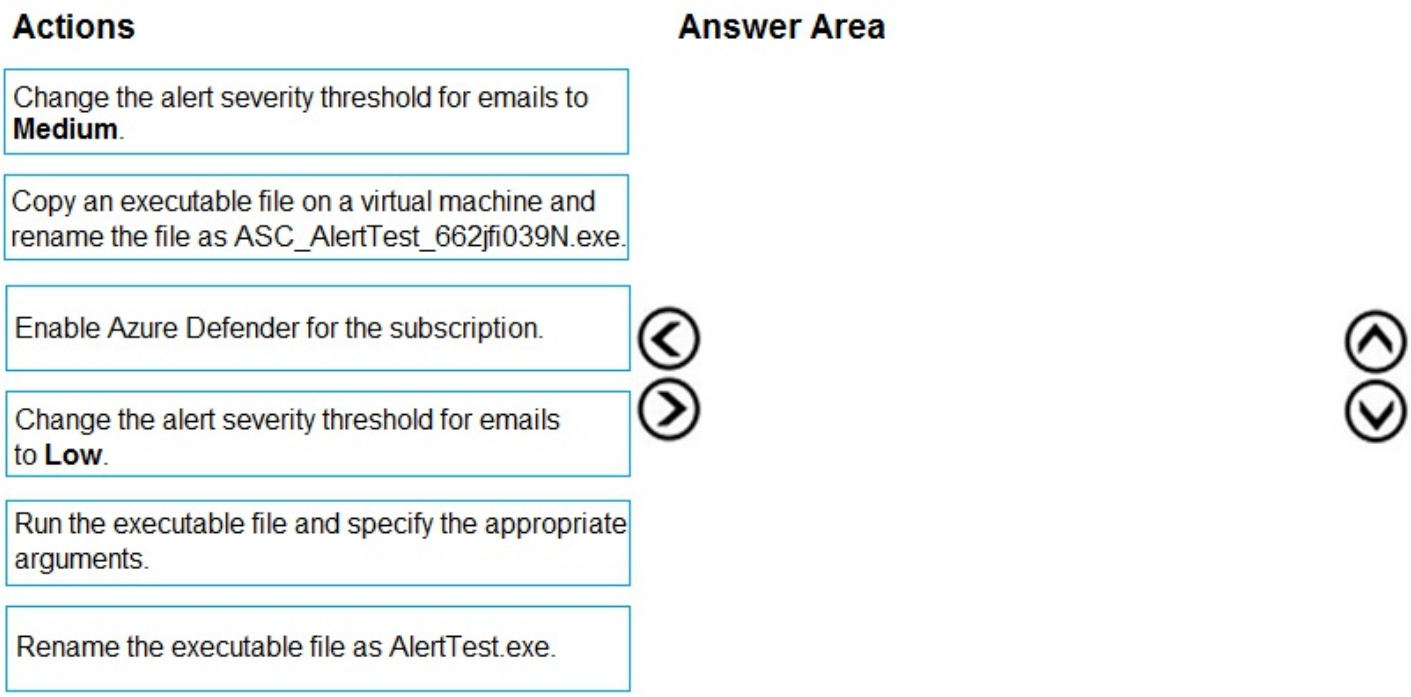
Data collectionStore additional raw data - Windows security eventsTo help audit, investigate, and analyze threats, you can collect raw events, logs, and additional security data and save it to your Log Analytics workspace.

Reference:

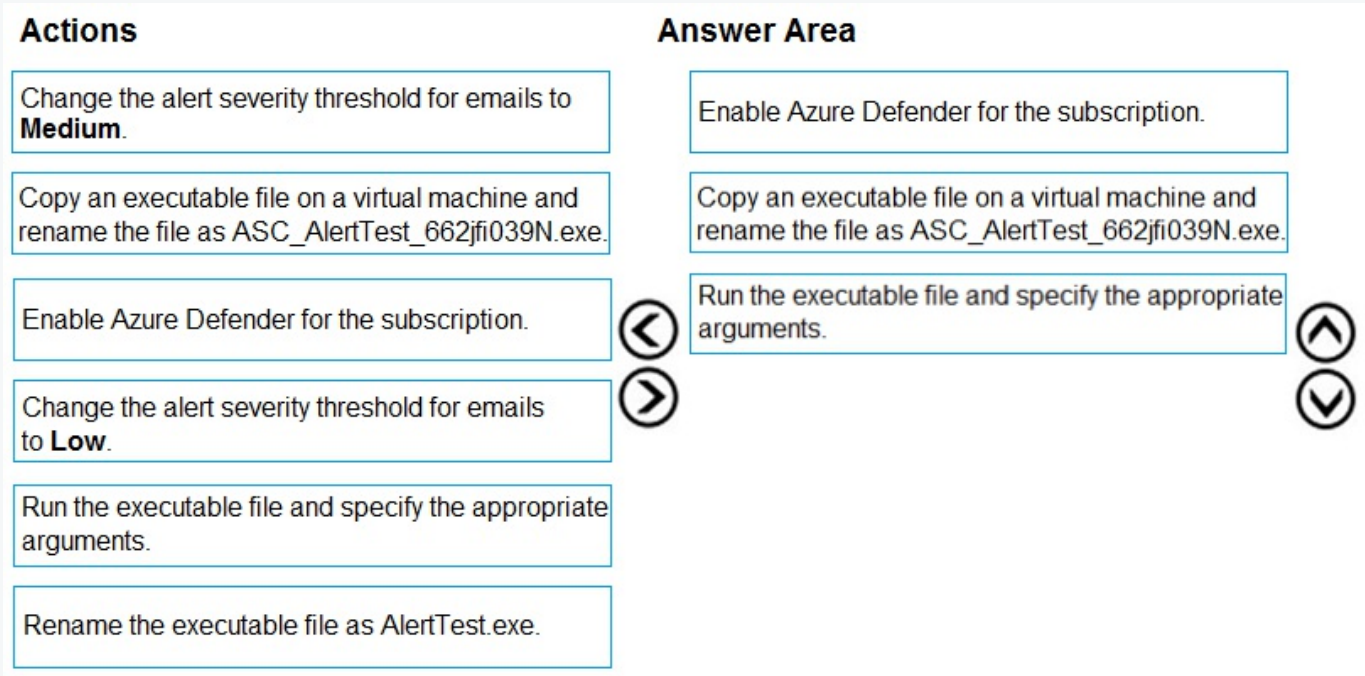
https://docs.microsoft.com/en-us/azure/security-center/security-center-enable-data-collection

Question: 73 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: 74 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

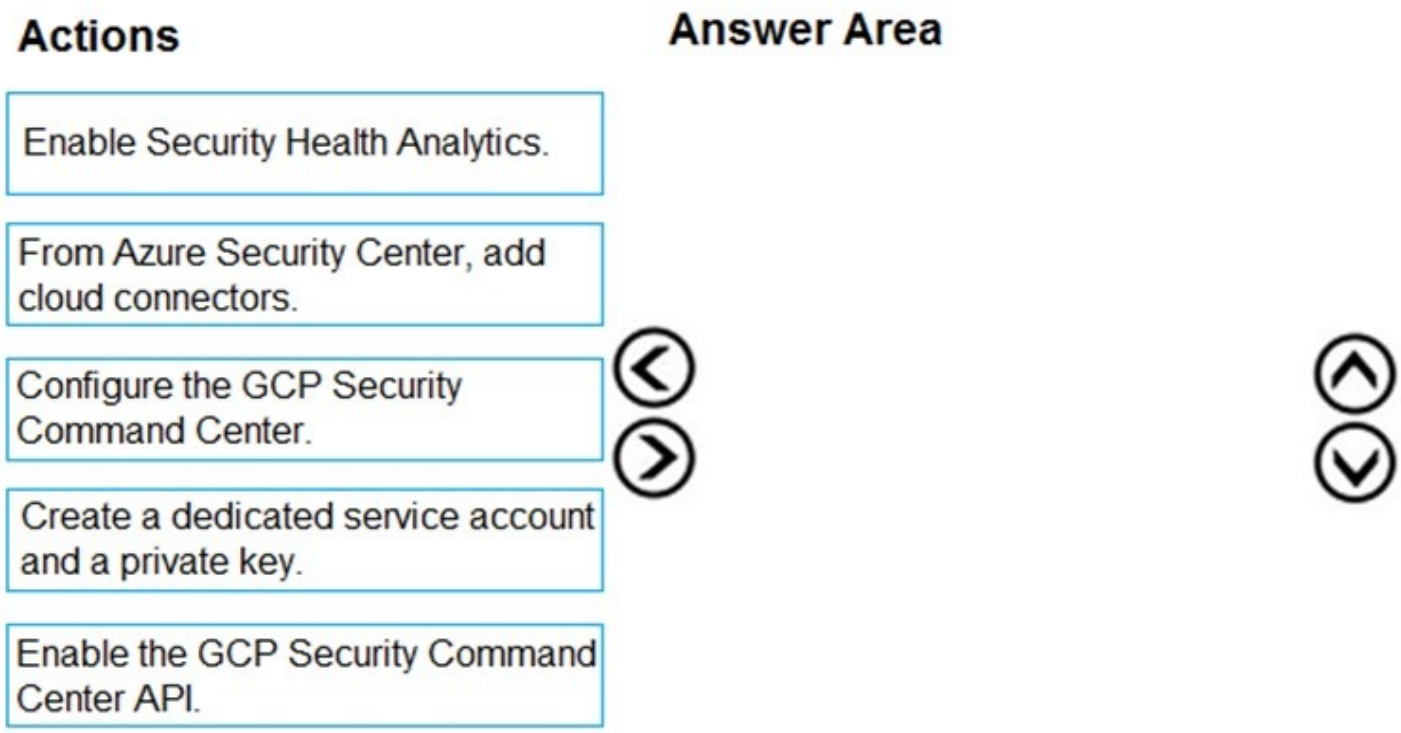
Answer: C

Explanation:

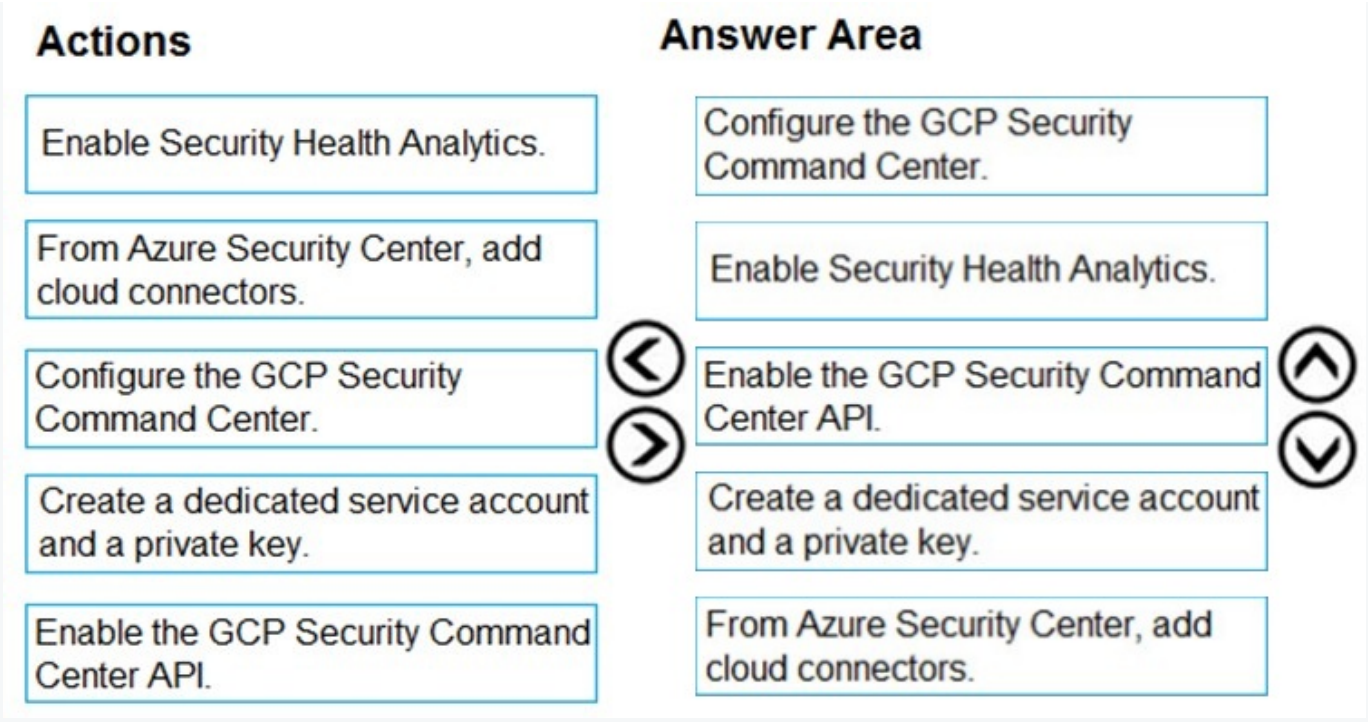
Reference:
https://docs.microsoft.com/en-us/azure/security-center/security-center-provide-security-contact-details

Question: 75 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: 76 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: 77 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: 78 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: 79 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: 80 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

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.

But Wait

I wanted to let you know that there is more content available in the full version.
The full paper contains additional sections and information that you may find helpful, and I encourage you to download it to get a more comprehensive and detailed view of all the subject matter.