2023 Updated Verified SC-200 dumps Q&As - Pass Guarantee or Full Refund [Q17-Q33

2023 Updated Verified SC-200 dumps Q&As - Pass Guarantee or Full Refund
SC-200 PDF Questions and Testing Engine With 225 Questions

Microsoft SC-200 (Microsoft Security Operations Analyst) Certification Exam is a highly sought-after certification for security professionals. It is designed to validate the skills required to proactively detect, respond to, and prevent security threats using Microsoft Azure Sentinel, Microsoft 365 Defender, and Azure Defender.

Q17. You use Azure Sentinel.

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

Which role should you assign to the analyst?
* Azure Sentinel Contributor
* Security Administrator

* Azure Sentinel Responder
* Logic App Contributor

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

Reference:

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

Q18. You have an existing Azure logic app that is used to block Azure Active Directory (Azure AD) users. The logic app is triggered manually.

You deploy Azure Sentinel.

You need to use the existing logic app as a playbook in Azure Sentinel. What should you do first?

* And a new scheduled query rule.
* Add a data connector to Azure Sentinel.
* Configure a custom Threat Intelligence connector in Azure Sentinel.
* Modify the trigger in the logic app.

Explanation

https://docs.microsoft.com/en-us/azure/sentinel/playbook-triggers-actions

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

Q19. You need to identify which mean time metrics to use to meet the Microsoft Sentinel requirements. Which workbook should you use?

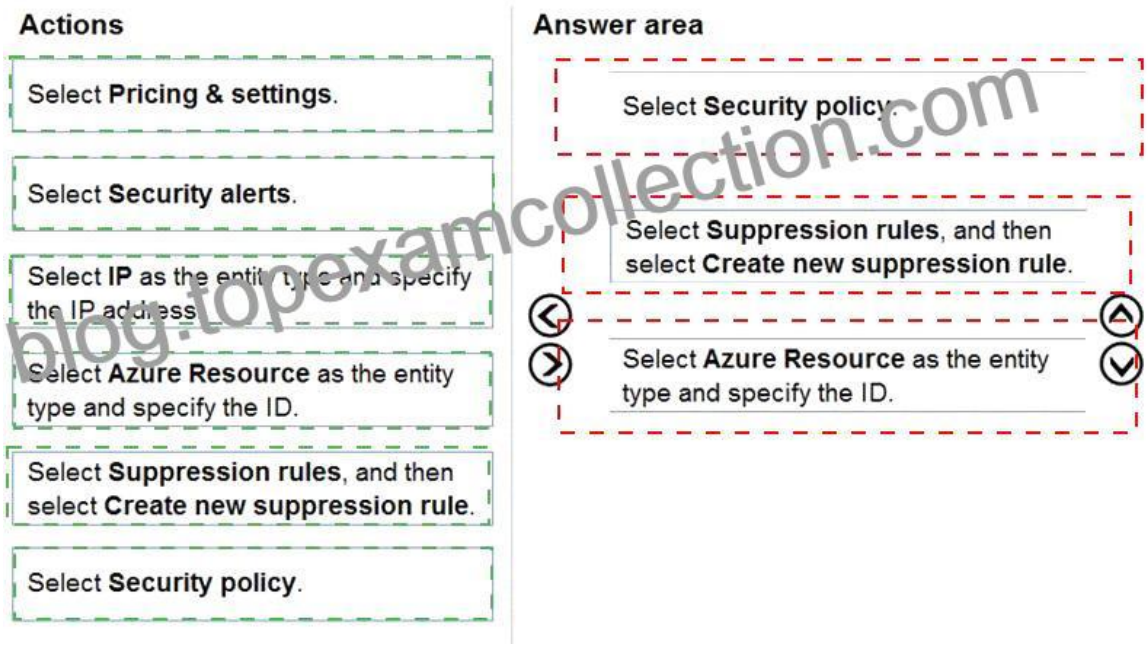
* Analytics Efficiency
* Security Operations Efficiency
* Event Analyzer
* Investigation insights

Q20. You have an Azure Functions app that generates thousands of alerts in Azure Security Center each day for normal activity.

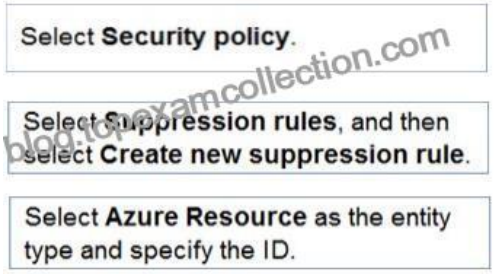
You need to hide the alerts automatically in Security Center.

Which three actions should you perform in sequence in Security Center? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.



Explanation

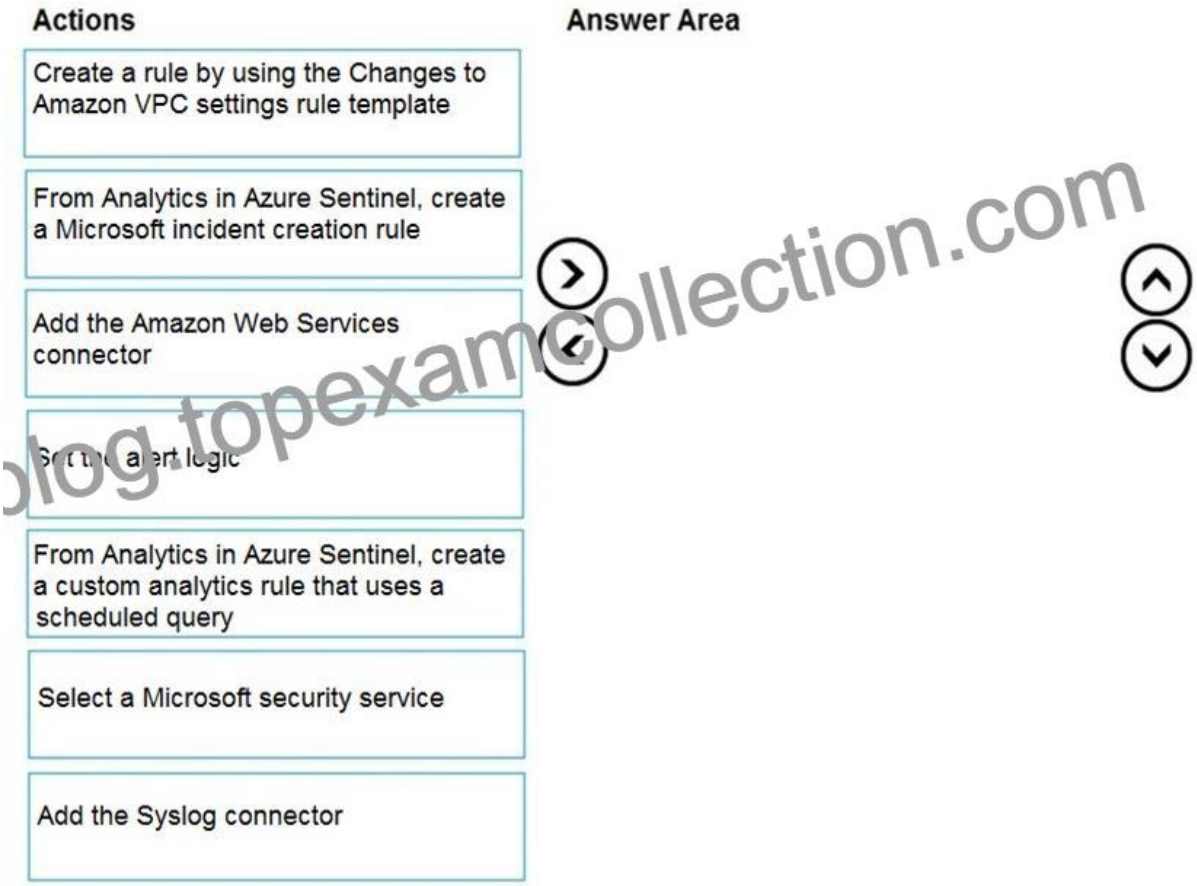


Reference:

https://techcommunity.microsoft.com/t5/azure-security-center/suppression-rules-for-azure-security-center-alerts-

Q21. You need to use an Azure Sentinel analytics rule to search for specific criteria in Amazon Web Services (AWS) logs and to generate incidents.

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



Answer Area

Add the Amazon Web Services connector
From Analytics in Azure Sentinel, create a custom analytics rule ....
Set the alert logic

1 – Add the Amazon Web Services connector

2 – From Analytics in Azure Sentinel, create a custom analytics rule ….

3 – Set the alert logic

Reference:

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

Q22. 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.

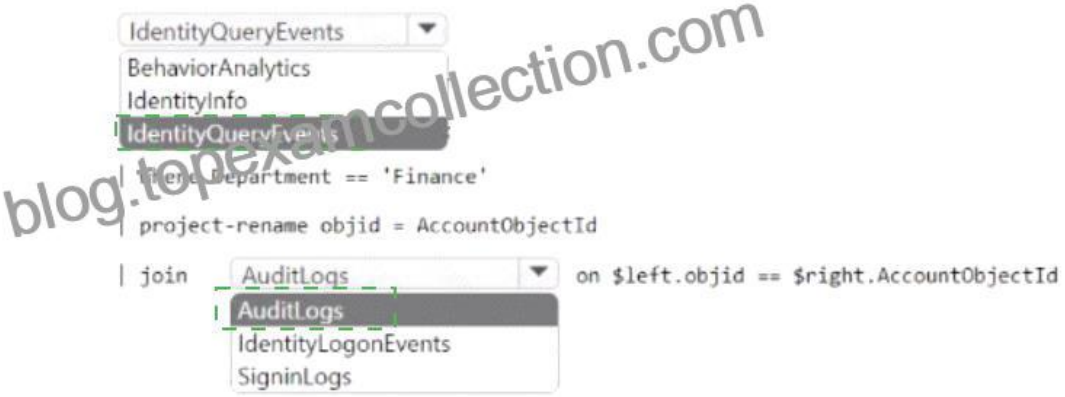
You need to identify all the interactive authentication attempts by the users in the finance department of your company.

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 Area



Explanation

Answer Area

```
IdentityQueryEvents
| where Department == "Finance"
| project-rename objid = AccountObjectId
| join AuditLogs on $left.objid == $right.AccountObjectId
```


Q23. You have an Azure subscription that uses Microsoft Defender fof Ctoud.

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

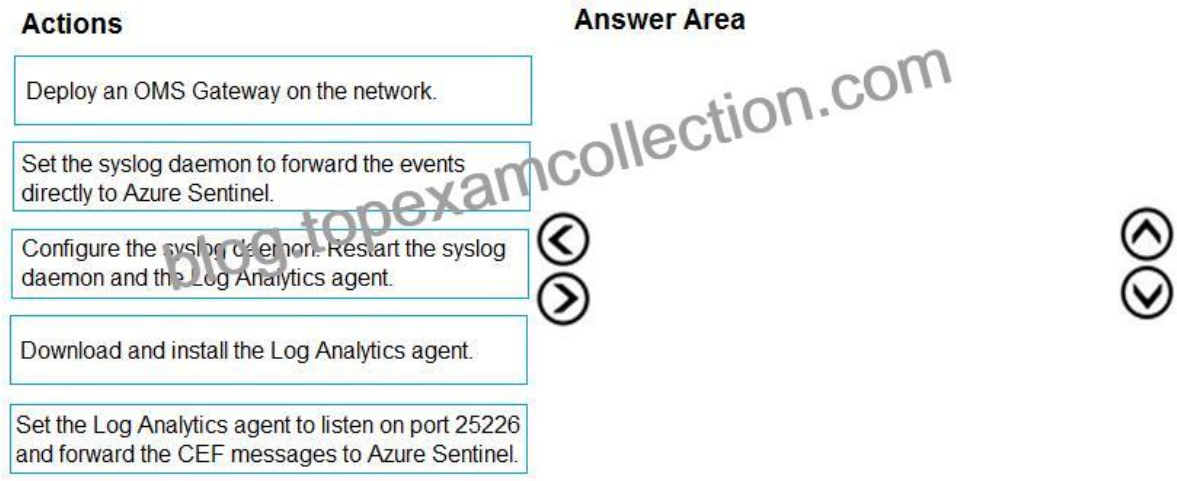
You need to onboard EC2-1 to Defender for Cloud.

What should you install on EC2-1?
* the Log Analytics agent
* the Azure Connected Machine agent
* the unified Microsoft Defender for Endpoint solution package
* Microsoft Monitoring Agent

Q24. You plan to connect an external solution that will send Common Event Format (CEF) messages to Azure Sentinel.

You need to deploy the log forwarder.

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



Answer Area

Download and install the Log Analytics agent.
Set the Log Analytics agent to listen on port 25226 and forward the CEF messages to Azure Sentinel.
Configure the syslog daemon. Restart the syslog daemon and the Log Analytics agent.

1 – Download and install the Log Analytics agent.

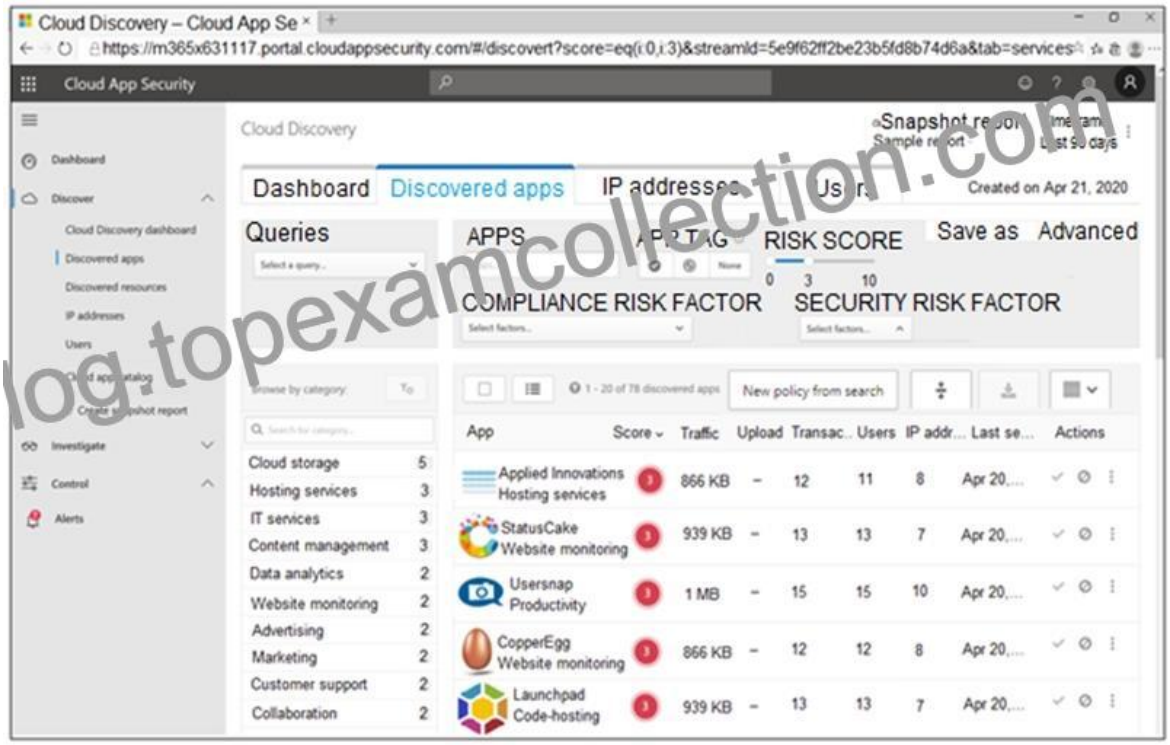
2 – Set the Log Analytics agent to listen on port 25226 and forward the CEF messages to Azure Sentinel.

3 – Configure the syslog daemon. Restart the syslog daemon and the Log Analytics agent.

Reference:

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

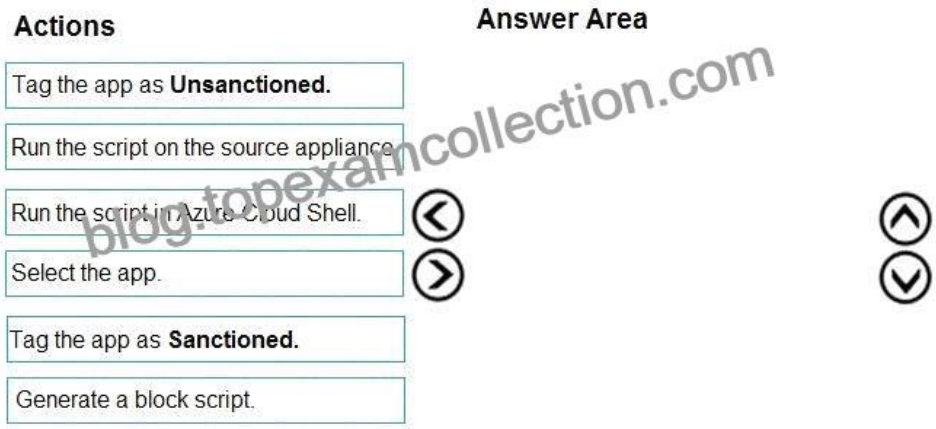
Q25. You open the Cloud App Security portal as shown in the following exhibit.



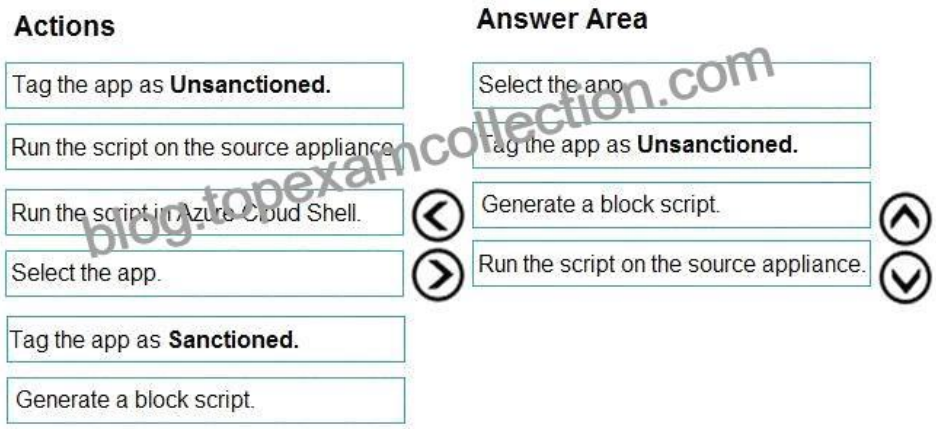
You need to remediate the risk for the Launchpad app.

Which four actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer

area and arrange them in the correct order.



Explanation



Reference:

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

Q26. You need to create the test rule to meet the Azure Sentinel requirements.

What should you do when you create the rule?
* From Set rule logic, turn off suppression.
* From Analytics rule details, configure the tactics.
* From Set rule logic, map the entities.
* From Analytics rule details, configure the severity.

Section: [none]

Explanation/Reference:

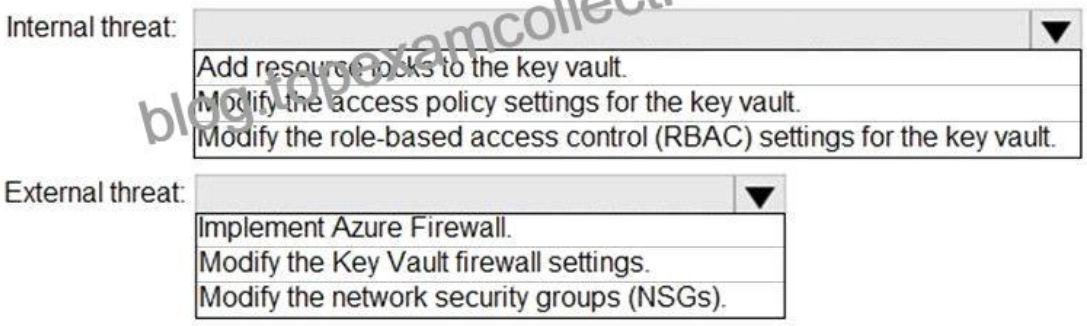
https://docs.microsoft.com/en-us/azure/sentinel/tutorial-detect-threats-custom

Q27. You need to recommend remediation actions for the Azure Defender alerts for Fabrikam.

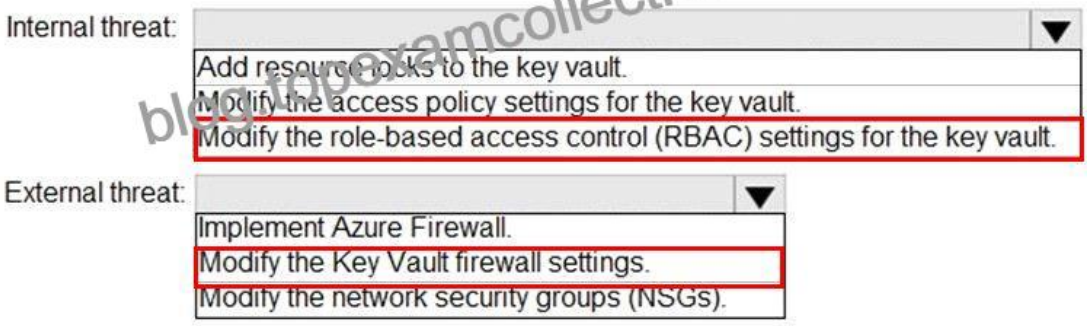
What should you recommend for each threat? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area



Answer Area



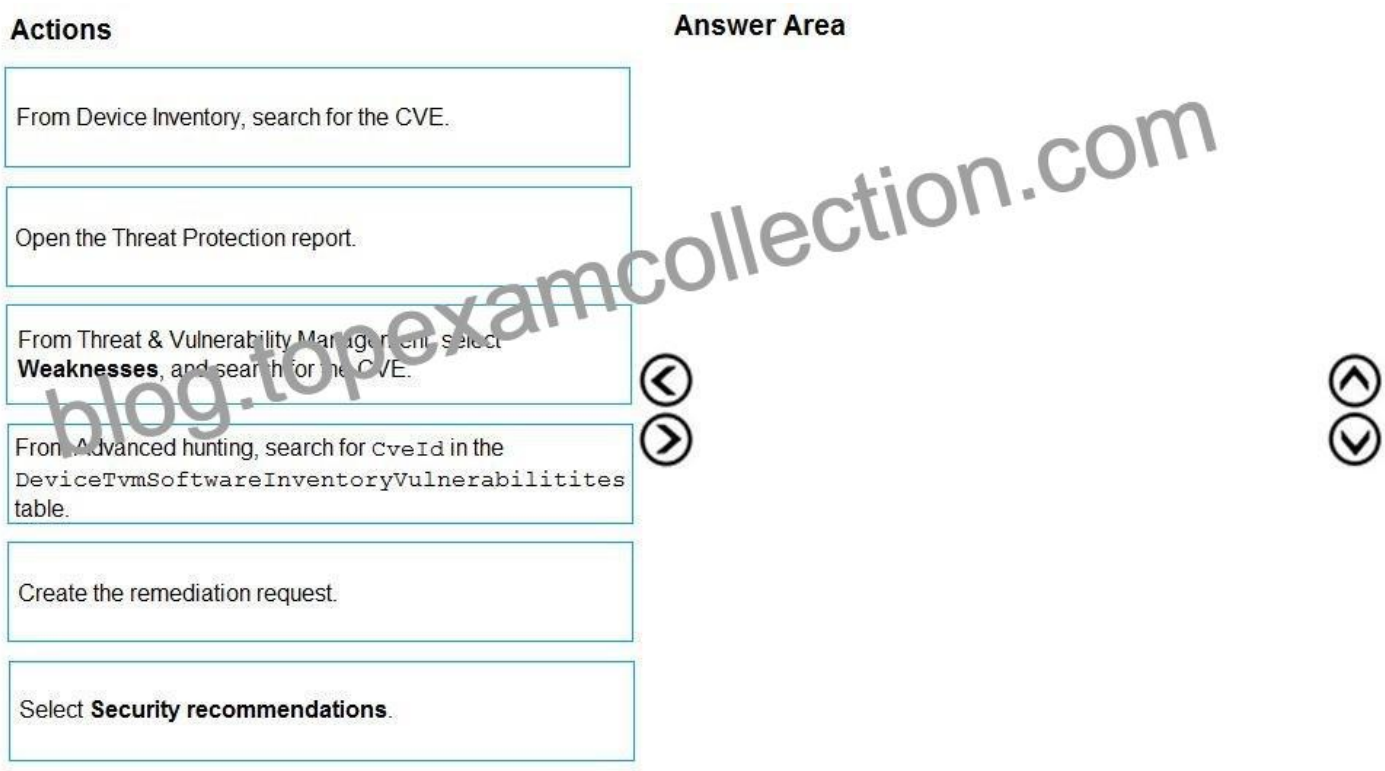
Reference:

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

Q28. You are informed of a new common vulnerabilities and exposures (CVE) vulnerability that affects your environment.

You need to use Microsoft Defender Security Center to request remediation from the team responsible for the affected systems if there is a documented active exploit available.

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



Answer Area

From Threate & Vulnerability Management...
Select Security recommendations.
Create the remediation request.

1 – From Threate & Vulnerability Management…

2 – Select Security recommendations.

3 – Create the remediation request.

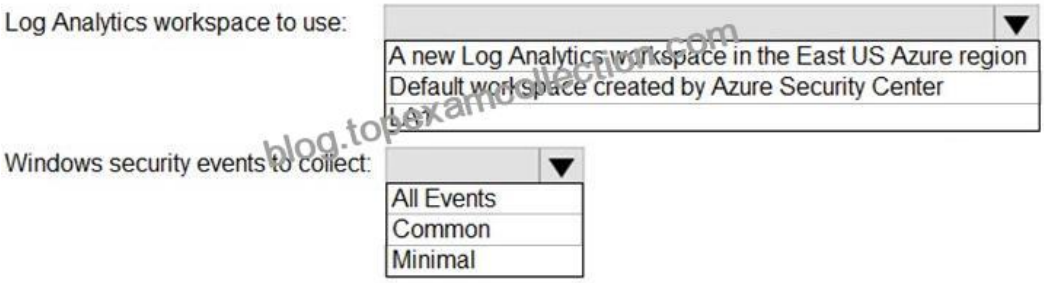
Reference:

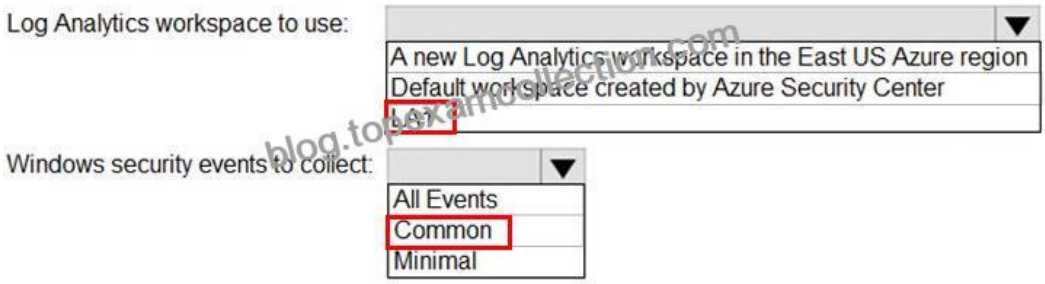
https://techcommunity.microsoft.com/t5/core-infrastructure-and-security/microsoft-defender-atp-remediate-apps-using-mem/ba-p/1599271

Q29. You need to implement Azure Defender to meet the Azure Defender requirements and the business requirements.

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

NOTE: Each correct selection is worth one point.





Q30. You have an Azure subscription that has Azure Defender enabled for all supported resource types.

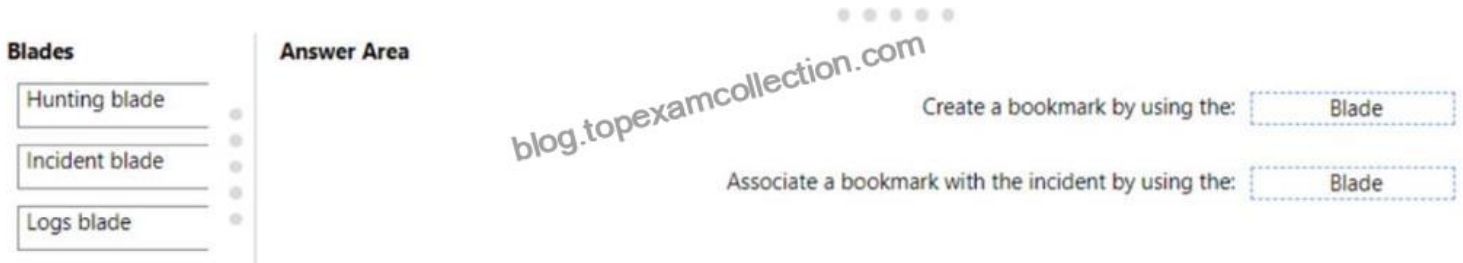
You need to configure the continuous export of high-severity alerts to enable their retrieval from a third-party security information and event management (SIEM) solution.

To which service should you export the alerts?
* Azure Cosmos DB
* Azure Event Grid
* Azure Event Hubs
* Azure Data Lake

Q31. You have a Microsoft Sentinel workspace that contains an Azure AD data connector.

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

What should you do? To answer, drag the appropriate blades to the correct tasks. Each blade may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content NOTE: Each correct selection is worth one point.



Q32. You have a Microsoft 365 E5 subscription.

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

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

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

NOTE: Each correct selection is worth one point.

Answer Area

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

Answer Area

Reference:

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

Q33. You have a playbook in Azure Sentinel.

When you trigger the playbook, it sends an email to a distribution group.

You need to modify the playbook to send the email to the owner of the resource instead of the distribution group.

What should you do?

* Add a parameter and modify the trigger.
* Add a custom data connector and modify the trigger.
* Add a condition and modify the action.
* Add a parameter and modify the action.

Reference:

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

Exam Engine for SC-200 Exam Free Demo & 365 Day Updates:
https://www.topexamcollection.com/SC-200-vce-collection.html]