[Jun 05, 2022 SC-200 Dumps PDF and Test Engine Exam Questions - ValidExam [Q43-Q65

[Jun 05, 2022] SC-200 Dumps PDF and Test Engine Exam Questions - ValidExam
Verified SC-200 exam dumps Q&As with Correct 110 Questions and Answers

Exam SC-200: Microsoft Security Operations Analyst **The content of this exam was updated on July 23, 2021.**

The Microsoft Security Operations Analyst collaborates with organizational stakeholders to secure information technology systems for the organization. Their goal is to reduce organizational risk by rapidly remediating active attacks in the environment, advising on improvements to threat protection practices, and referring violations of organizational policies to appropriate stakeholders. Responsibilities include threat management, monitoring, and response by using a variety of security solutions across their environment. The role primarily investigates, responds to, and hunts for threats using Microsoft Azure Sentinel, Azure Defender, Microsoft 365 Defender, and third-party security products. Since the Security Operations Analyst consumes the operational output of these tools, they are also a critical stakeholder in the configuration and deployment of these technologies.

Part of the requirements for: Microsoft Certified: Security Operations Analyst Associate

Download exam skills outline

Microsoft SC-200 Exam Syllabus Topics:

TopicDetailsTopic 1- Design and Configure Windows Events collections- Manage data loss prevention policy alertsTopic 2- Identify, investigate, and remediate security risks related to privileged identities- Design and configure playbook in Azure DefenderTopic 3- Identify and remediate security risks related to Conditional Access events- manage data retention, alert notification, and advanced featuresTopic 4- Detect, investigate, respond, and remediate identity threats- Configure and manage custom detections and alertsTopic 5- Identify the prerequisites for a data connector- Configure detection alerts in Azure AD Identity ProtectionTopic 6- Identify and remediate security risks related to sign-in risk policies- Identify data sources to be ingested for Azure SentinelTopic 7- Investigate Azure Defender alerts and incidents- Configure device attack surface reduction rulesTopic 8- Mitigate threats using Azure Defender- Identify and remediate security risks using Secure ScoreTopic 9- Manage user data discovered during an investigation- Assess and recommend insider risk policiesTopic 10- Design and configure an Azure Defender implementation- Configure automated responses in Azure Security Center

NEW QUESTION 43

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/

NEW QUESTION 44

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

You discover that the rule fails intermittently.

What are two possible causes of the failures? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.
* The rule query takes too long to run and times out.
* The target workspace was deleted.
* Permissions to the data sources of the rule query were modified.
* There are connectivity issues between the data sources and Log Analytics

Section: [none]

Explanation:

Incorrect Answers:

B: This would cause it to fail every time, not just intermittently.

C: This would cause it to fail every time, not just intermittently.

NEW QUESTION 45

You have an Azure Sentinel workspace.

You need to test a playbook manually in the Azure portal.

From where can you run the test in Azure Sentinel?
* Playbooks
* Analytics
* Threat intelligence
* Incidents

Explanation/Reference:

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

NEW QUESTION 46

You create a hunting query in Azure Sentinel.

You need to receive a notification in the Azure portal as soon as the hunting query detects a match on the query. The solution must minimize effort.

What should you use?
* a playbook
* a notebook
* a livestream
* a bookmark

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

Reference:

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

NEW QUESTION 47

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?
* Yes
* No
Section: [none]

Explanation:

You need to resolve the existing alert, not prevent future alerts. Therefore, you need to select the ‘Mitigate the threat’ option.

Reference:

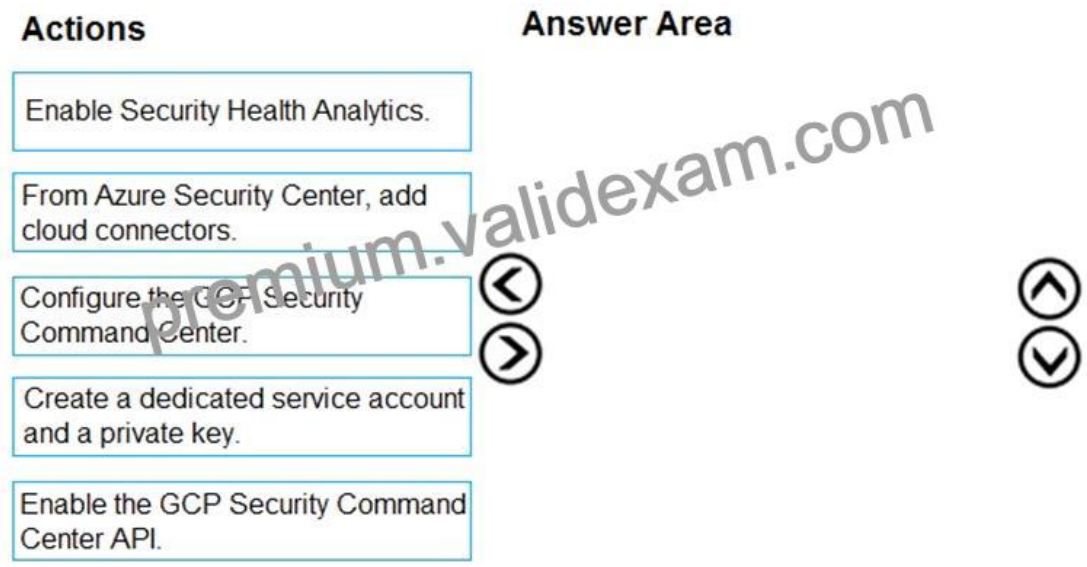
https://docs.microsoft.com/en-us/azure/security-center/security-center-managing-and-responding-alerts

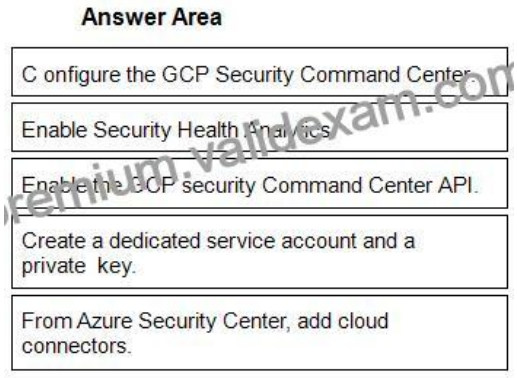
NEW QUESTION 48

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.





1 – C onfigure the GCP Security Command Center.

2 – Enable Security Health Analytics.

3 – Enable the GCP security Command Center API.

4 – Create a dedicated service account and a private key.

5 – From Azure Security Center, add cloud connectors.

Reference:

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

NEW QUESTION 49

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.

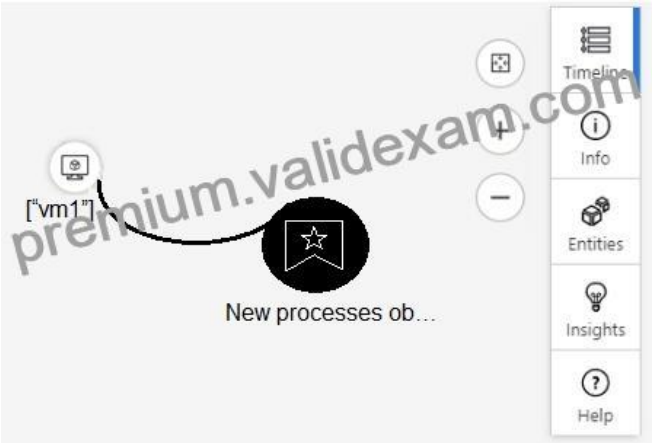
Solution: From Security alerts, you select the alert, select Take Action, and then expand the Mitigate the threat section.

Does this meet the goal?
* Yes
* No
Reference:

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

NEW QUESTION 50

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



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

NOTE: Each correct selection is worth one point.

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

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

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

- Entities
- Info
- Insights
- Timeline

Explanation

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

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

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

- Entities
- Info
- Insights
- Timeline

Reference:

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

NEW QUESTION 51

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?
* Modify the access control settings for the key vault.
* Enable the Key Vault firewall.
* Create an application security group.
* Modify the access policy for the key vault.

Section: [none]

Explanation/Reference:

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

NEW QUESTION 52

Your company uses line-of-business apps that contain Microsoft Office VBA macros.

You plan to enable protection against downloading and running additional payloads from the Office VBA macros as additional child processes.

You need to identify which Office VBA macros might be affected.

Which two commands can you run to achieve the goal? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

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

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

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

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

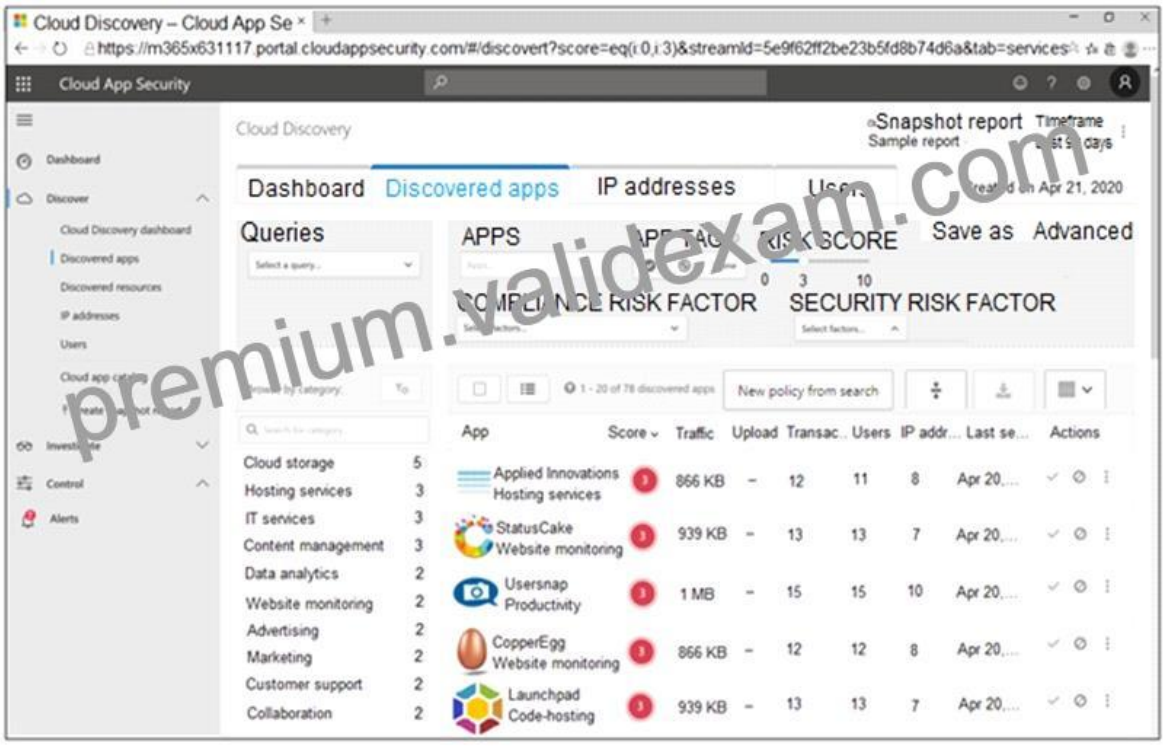
* Option A
* Option B
* Option C
* Option D

Reference:

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

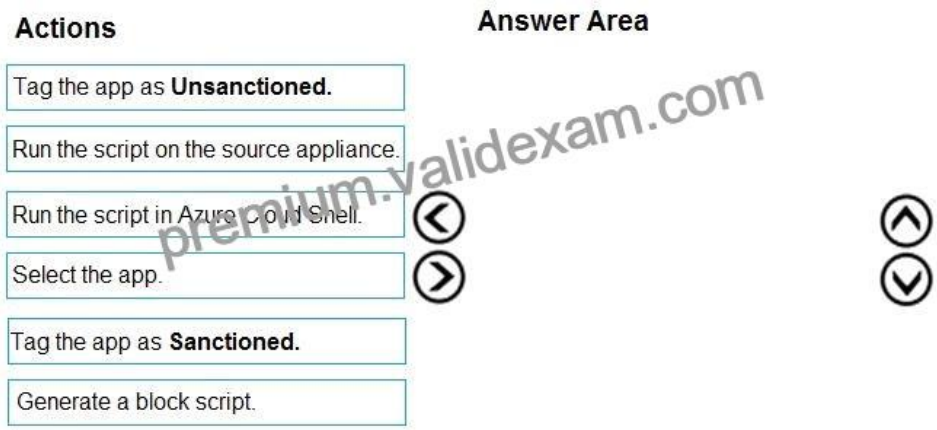
NEW QUESTION 53

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



You need to remediate the risk for the Launchpad app.

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



Answer Area

Select the app.
Tag the app as Unsanctioned.
Generate a block script.
Run the script on the source appliance.

1 – Select the app.

2 – Tag the app as Unsanctioned.

3 – Generate a block script.

4 – Run the script on the source appliance.

Reference:

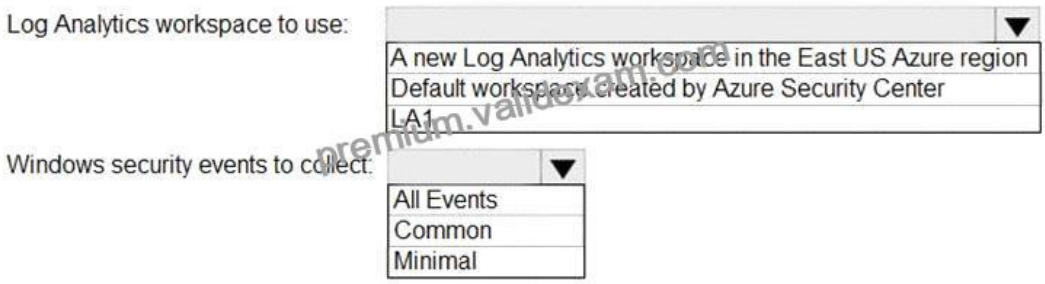
https://docs.microsoft.com/en-us/cloud-app-security/governance-discovery

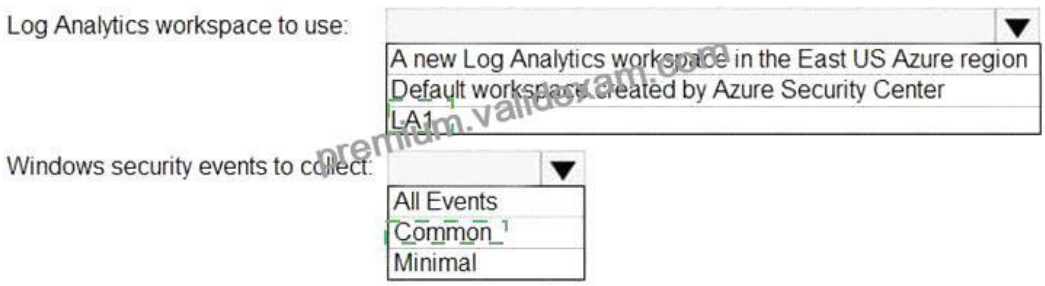
NEW QUESTION 54

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.

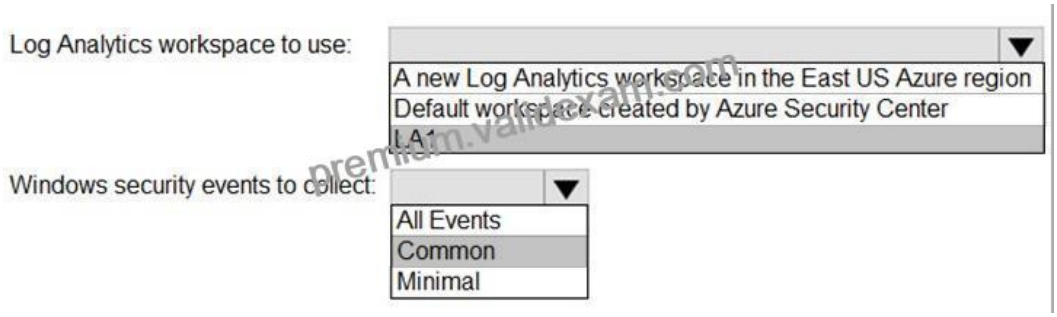
NOTE: Each correct selection is worth one point.





Explanation

Graphical user interface, application Description automatically generated



NEW QUESTION 55

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.

Section: [none]

Explanation/Reference:

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

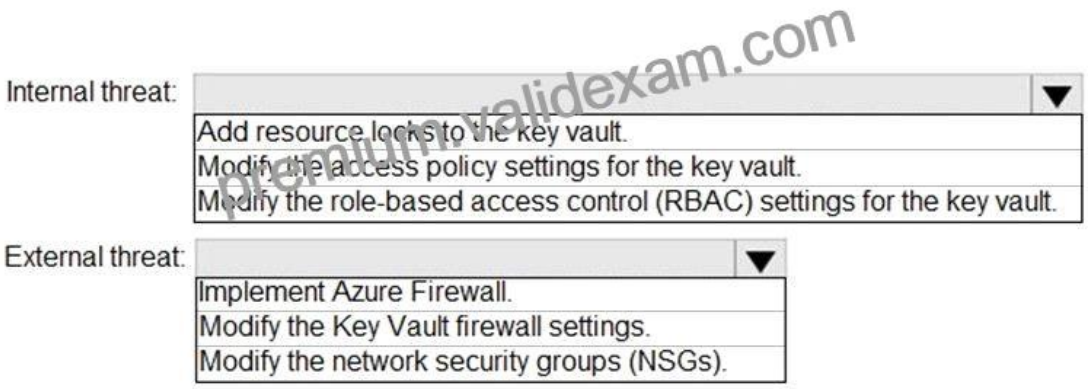
NEW QUESTION 56

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

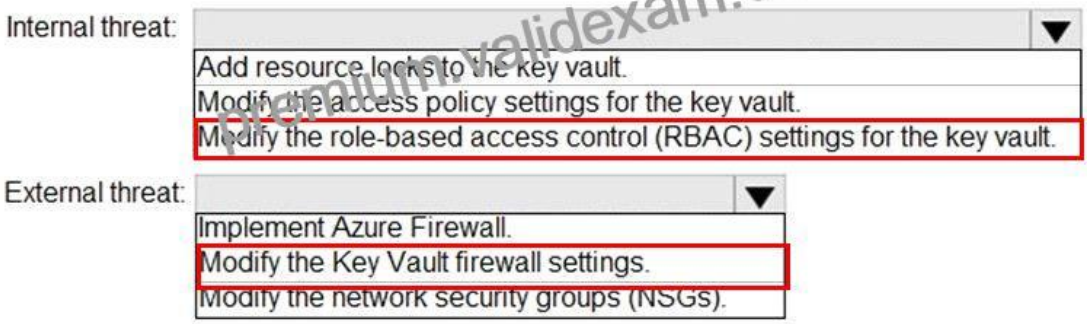
What should you recommend for each threat? To answer, select the appropriate options in the answer area.

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

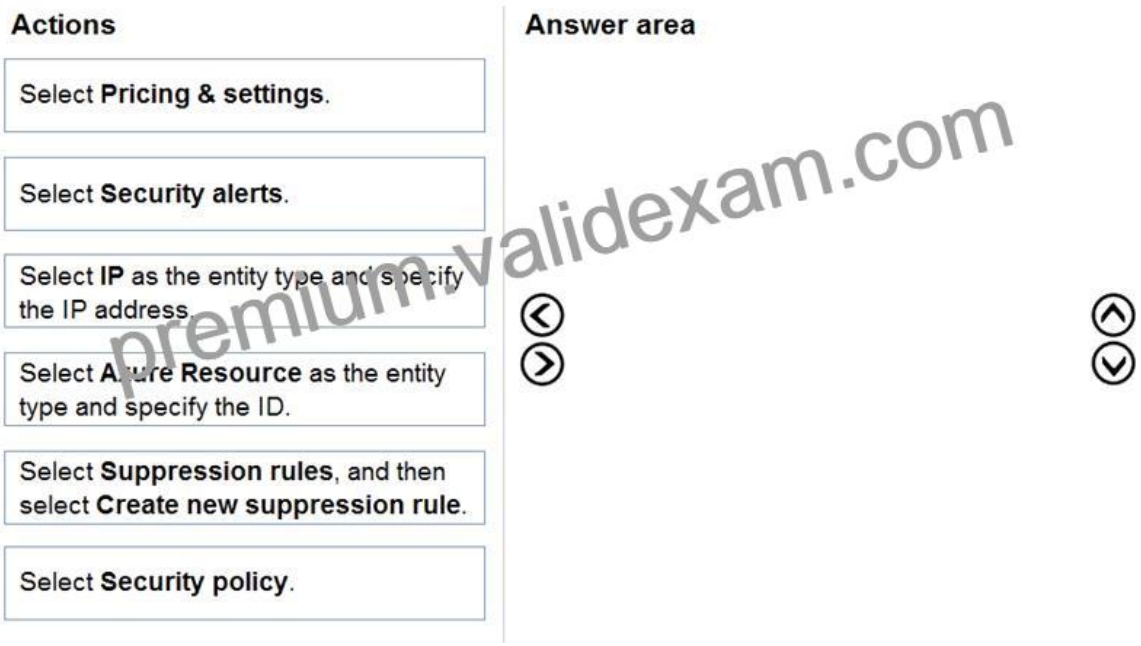
NEW QUESTION 57

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.



Answer Area

Select Security policy.

Select Suppression rules, and then select Create new suppression rule.

Select Azure Resource as the entity type and specify the ID.

1 – Select Security policy.

2 – Select Suppression rules, and then select Create new suppression rule.

3 – Select Azure Resource as the entity type and specify the ID.

Reference:

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

NEW QUESTION 58

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?
* Yes
* No
Section: [none]

Explanation/Reference:

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

NEW QUESTION 59

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?
* Yes
* No
Explanation/Reference:

https://docs.microsoft.com/en-us/defender-for-identity/manage-sensitive-honeytoken-accounts Mitigate threats using Azure Defender Question Set 1

NEW QUESTION 60

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

You create an Azure logic app named LA1.

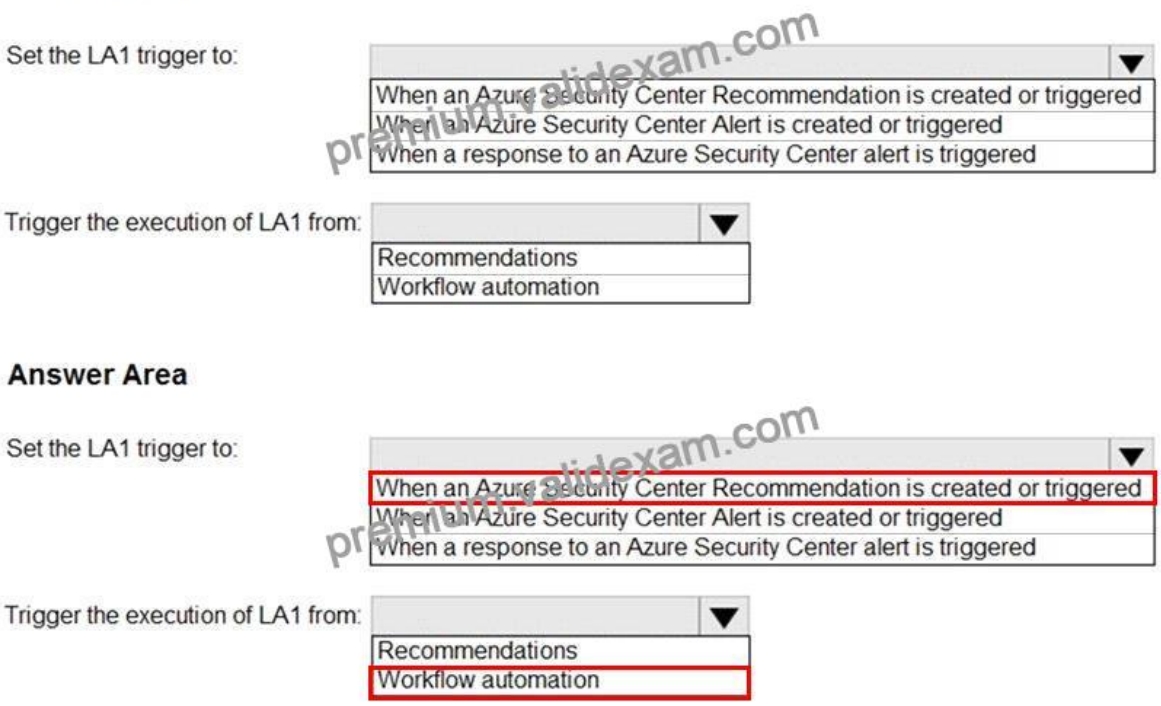
You plan to use LA1 to automatically remediate security risks detected in Azure Security Center.

You need to test LA1 in Security Center.

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

NOTE: Each correct selection is worth one point.

Answer Area



Answer Area

Reference:

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

NEW QUESTION 61

DRAG DROP

Your company deploys Azure Sentinel.

You plan to delegate the administration of Azure Sentinel to various groups.

You need to delegate the following tasks:

* Create and run playbooks

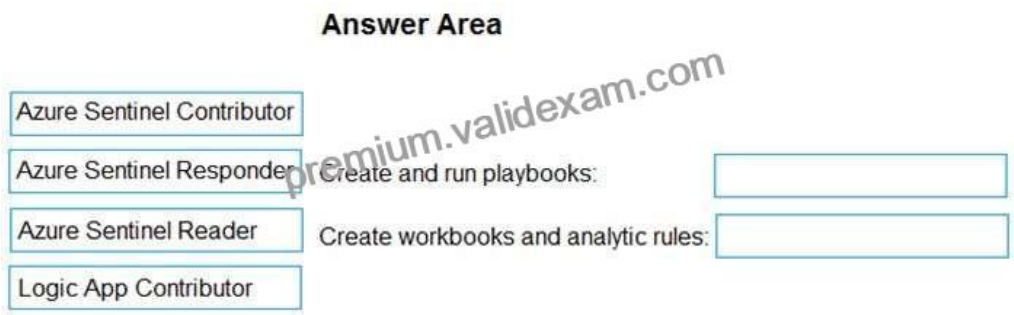
* Create workbooks and analytic rules.

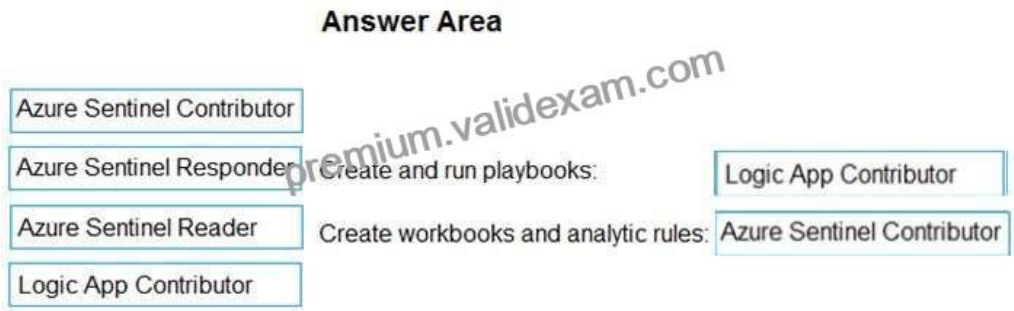
The solution must use the principle of least privilege.

Which role should you assign for each task? To answer, drag the appropriate roles to the correct tasks. Each role may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

Select and Place:





Section: [none]

Explanation/Reference:

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

NEW QUESTION 62

You need to visualize Azure Sentinel data and enrich the data by using third-party data sources to identify indicators of compromise (IoC).

What should you use?
* Microsoft Cloud App Security
* Azure Monitor
* hunting queries in Azure Sentinel
* notebooks in Azure Sentinel

Topic 1, Contoso Ltd

Overview

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

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

Existing Environment

End-User Environment

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

Cloud and Hybrid Infrastructure

All Contoso applications are deployed to Azure.

You enable Microsoft Cloud App Security.

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

Current Problems

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

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

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

The executive team at Contoso suspects a security breach. The executive team requests that you identify which files had more than five activities during the past 48 hours, including data access, download, or deletion for Microsoft Cloud App Security-protected applications.

Requirements

Planned Changes

Contoso plans to integrate the security operations of both companies and manage all security operations centrally.

Technical Requirements

Contoso identifies the following technical requirements:

Receive alerts if an Azure virtual machine is under brute force attack.

Use Azure Sentinel to reduce organizational risk by rapidly remediating active attacks on the environment.

Implement Azure Sentinel queries that correlate data across the Azure AD tenants of Contoso and Fabrikam.

Develop a procedure to remediate Azure Defender for Key Vault alerts for Fabrikam in case of external attackers and a potential compromise of its own Azure AD applications.

Identify all cases of users who failed to sign in to an Azure resource for the first time from a given country. A junior security administrator provides you with the following incomplete query.

BehaviorAnalytics

| where ActivityType == “FailedLogOn”

| where _____ == True

NEW QUESTION 63

You need to implement the Azure Information Protection requirements. What should you configure first?
* Device health and compliance reports settings in Microsoft Defender Security Center
* scanner clusters in Azure Information Protection from the Azure portal
* content scan jobs in Azure Information Protection from the Azure portal
* Advanced features from Settings in Microsoft Defender Security Center

Explanation

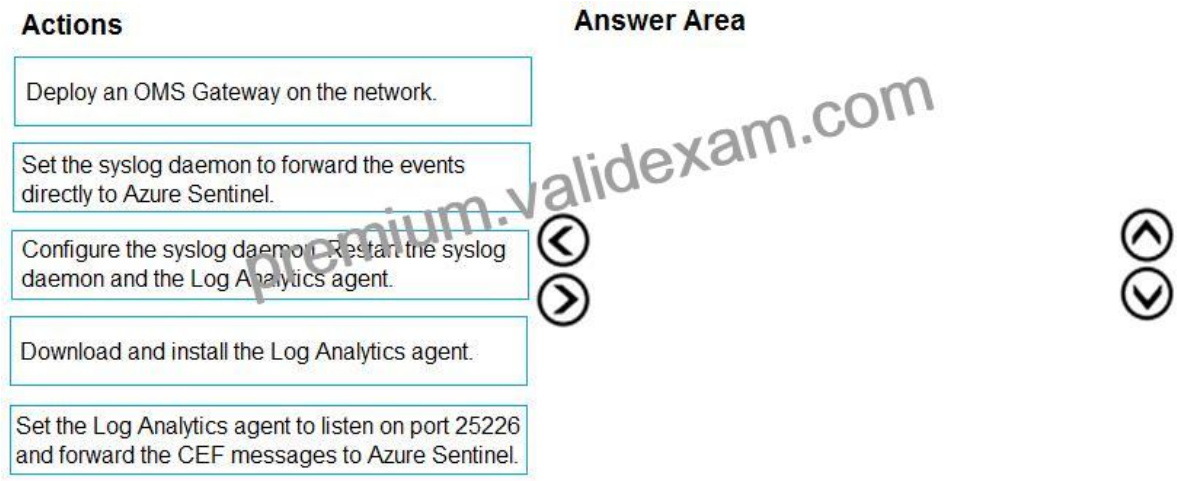
https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/information-protection-in-windows-overview

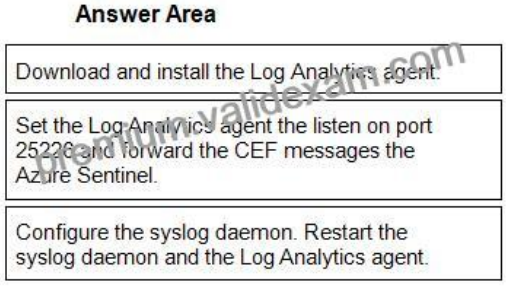
NEW QUESTION 64

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.





1 – Download and install the Log Analytics agent.

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

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

Reference:

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

NEW QUESTION 65

You need to recommend a solution to meet the technical requirements for the Azure virtual machines.

What should you include in the recommendation?
* just-in-time (JIT) access
* Azure Defender
* Azure Firewall
* Azure Application Gateway

Section: [none]

Explanation/Reference:

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

Question Set 3

Schedule exam **Languages:** English, Japanese, Chinese (Simplified), Korean, French, German, Spanish, Portuguese (Brazil), Russian, Arabic (Saudi Arabia), Chinese (Traditional), Italian
Retirement date: none
This exam measures your ability to accomplish the following technical tasks: mitigate threats using Microsoft 365 Defender; mitigate threats using Azure Defender; and mitigate threats using Azure Sentinel.

Microsoft SC-200 Test Engine PDF - All Free Dumps: https://www.validexam.com/SC-200-latest-dumps.html]