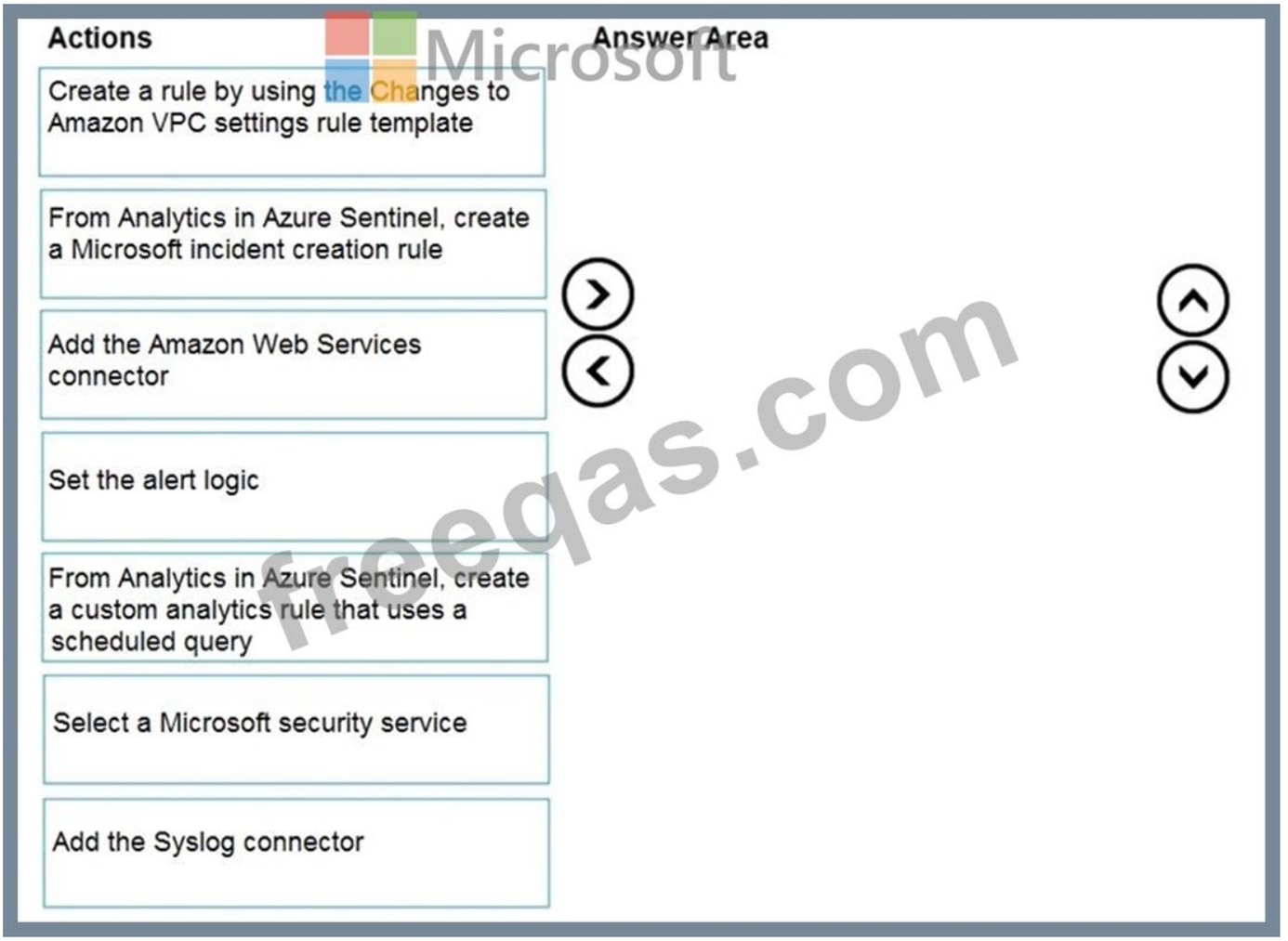
Microsoft.SC-200.v2022-07-02.q120

Exam Code:	SC-200
Exam Name:	Microsoft Security Operations Analyst
Certification Provider:	Microsoft
Free Question Number:	120
Version:	v2022-07-02
# of views:	2564
# of Questions views:	1200
https://www.freeqas.com/qa/Microsoft/SC-200/Microsoft.SC-200.v2022-07-02.q120.html	

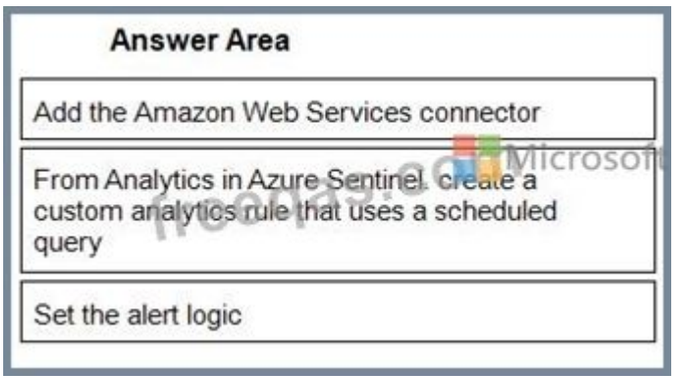
NEW QUESTION: 1

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:



1 - Add the Amazon Web Services connector

2 - From Analytics in Azure Sentinel. create a custom analytics rule that uses a scheduled query

3 - Set the alert logic

Reference:

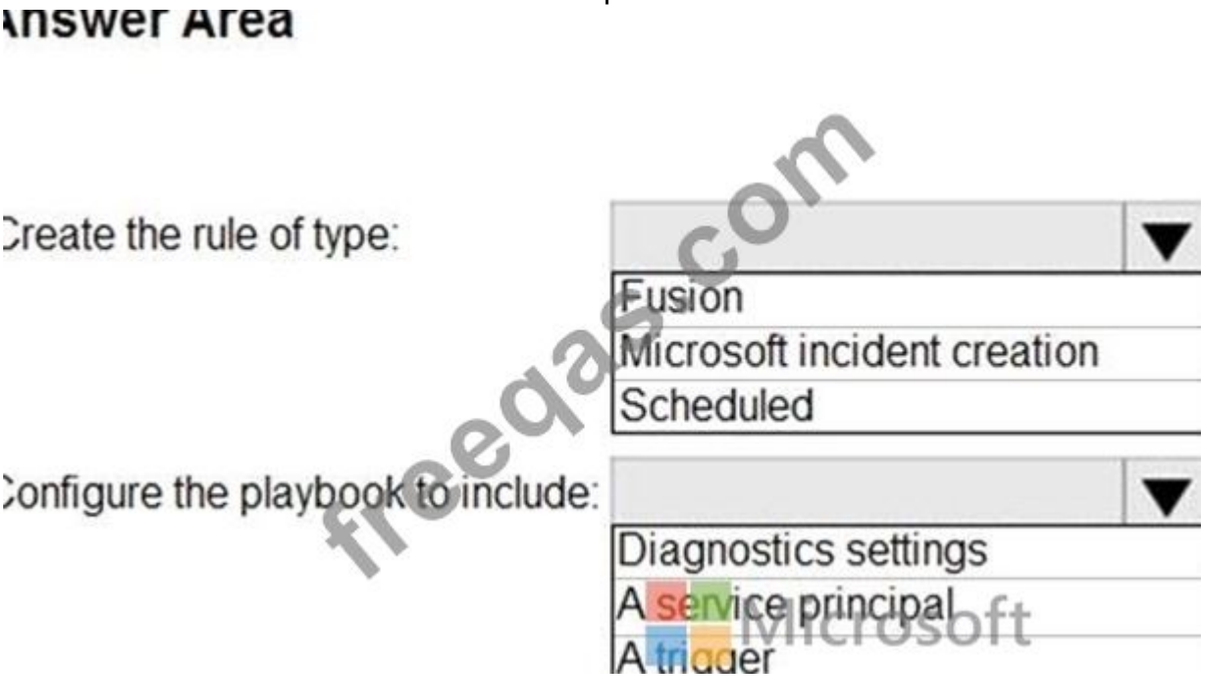
https://docs.microsoft.com/en-us/azure/sentinel/detect-threats-custom

NEW QUESTION: 2

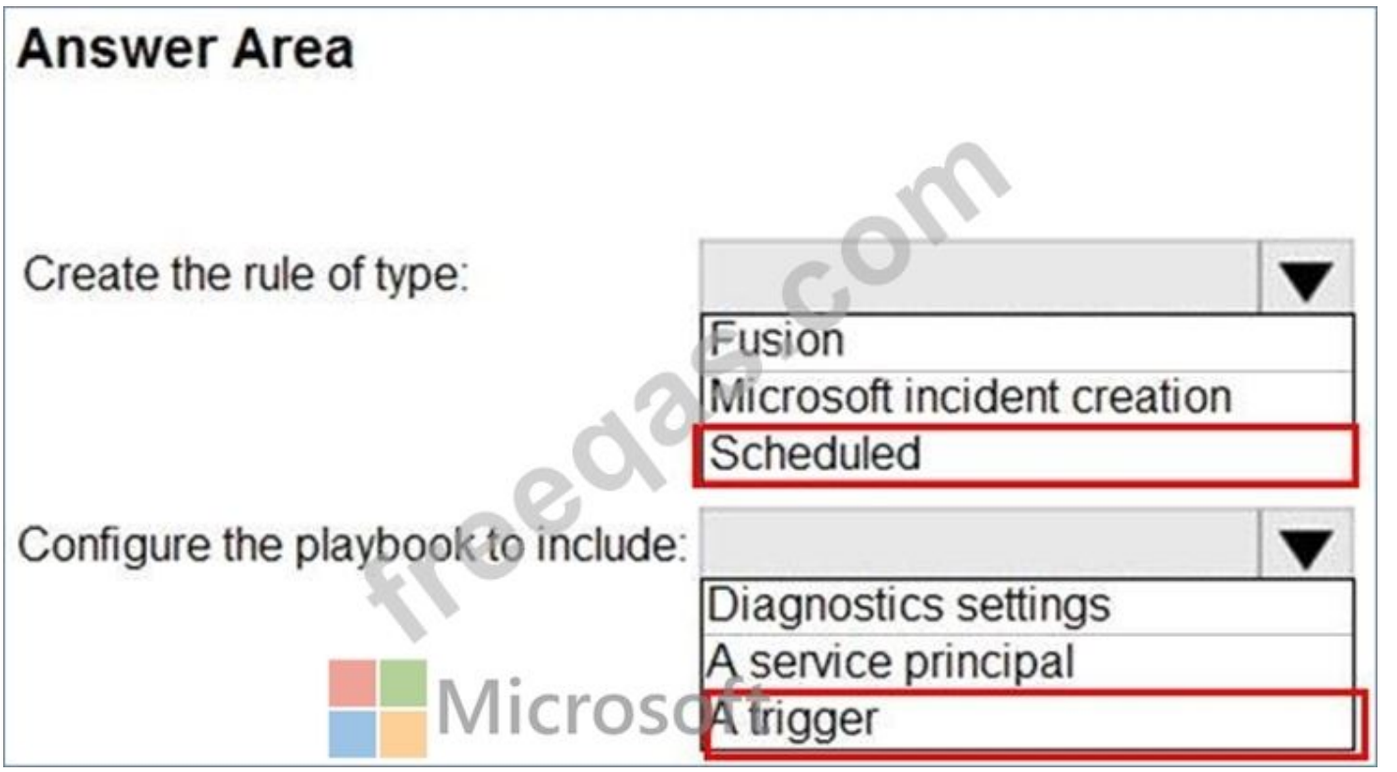
You need to create the analytics rule to meet the Azure Sentinel requirements.

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

NOTE: Each correct selection is worth one point.



Answer:

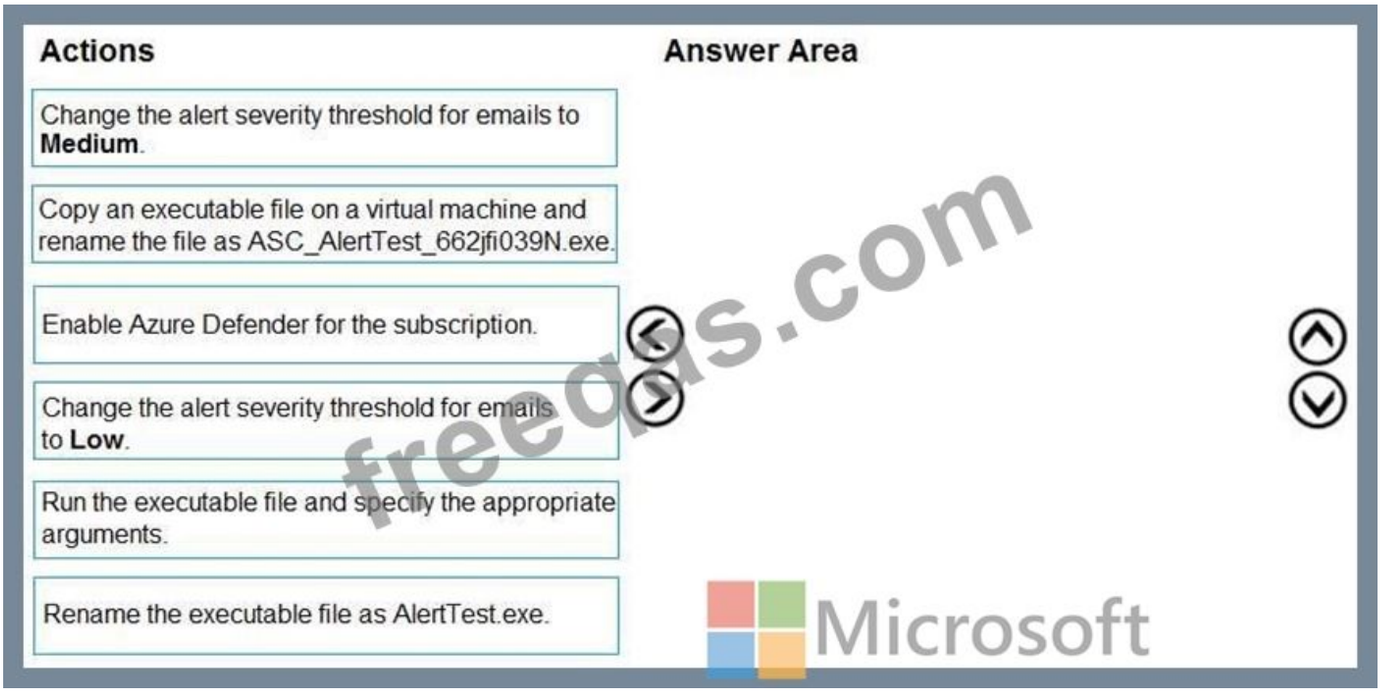


NEW QUESTION: 3
You need to implement the Azure Information Protection requirements. What should you configure first?
A. content scan jobs in Azure Information Protection from the Azure portal
B. scanner clusters in Azure Information Protection from the Azure portal
C. Advanced features from Settings in Microsoft Defender Security Center
D. Device health and compliance reports settings in Microsoft Defender Security Center
Answer: C (LEAVE A REPLY)

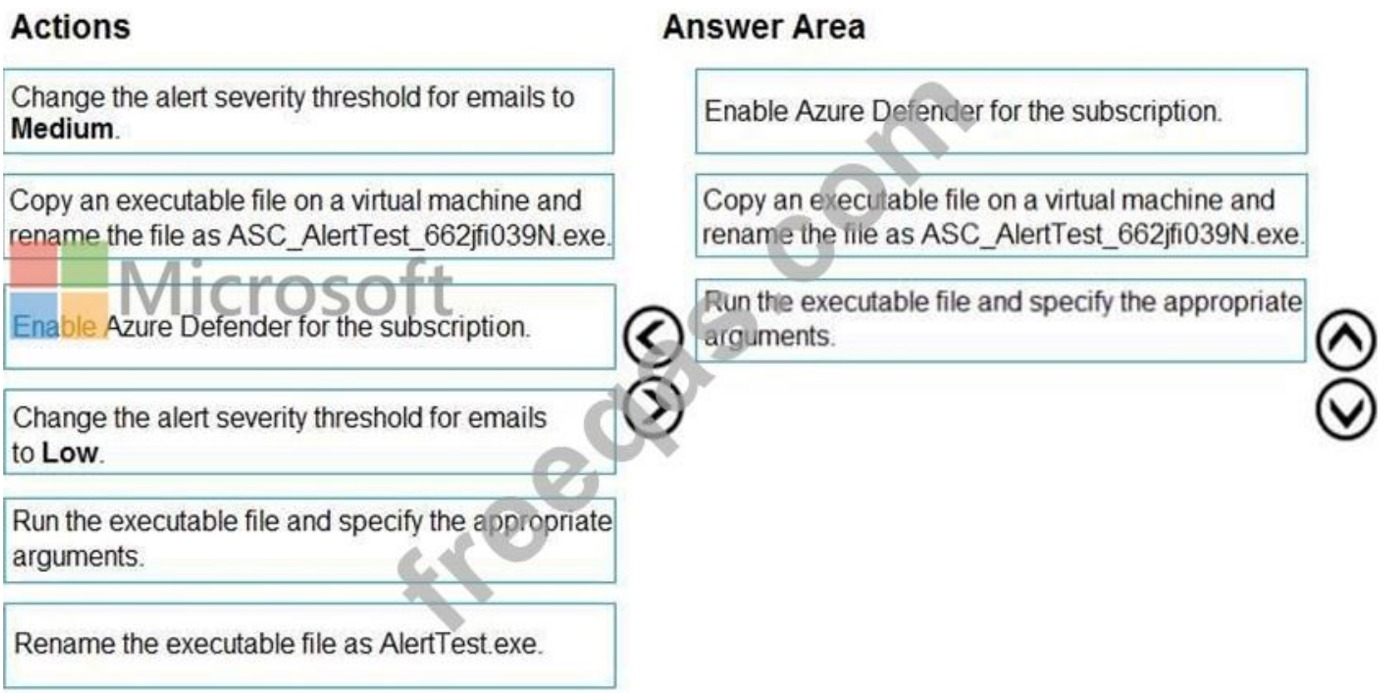
NEW QUESTION: 4
You create an Azure subscription.
You enable Azure Defender for the subscription.
You need to use Azure Defender to protect on-premises computers.
What should you do on the on-premises computers?
A. Install the Log Analytics agent.
B. Install the Dependency agent.
C. Configure the Hybrid Runbook Worker role.
D. Install the Connected Machine agent.
Answer: A (LEAVE A REPLY)
Security Center collects data from your Azure virtual machines (VMs), virtual machine scale sets, IaaS containers, and non-Azure (including on-premises) machines to monitor for security vulnerabilities and threats.
Data is collected using:

The Log Analytics agent, which reads various security-related configurations and event logs from the machine and copies the data to your workspace for analysis. Examples of such data are: operating system type and version, operating system logs (Windows event logs), running processes, machine name, IP addresses, and logged in user.
Security extensions, such as the Azure Policy Add-on for Kubernetes, which can also provide data to Security Center regarding specialized resource types.
Reference:
https://docs.microsoft.com/en-us/azure/security-center/security-center-enable-data-collection

NEW QUESTION: 5
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:



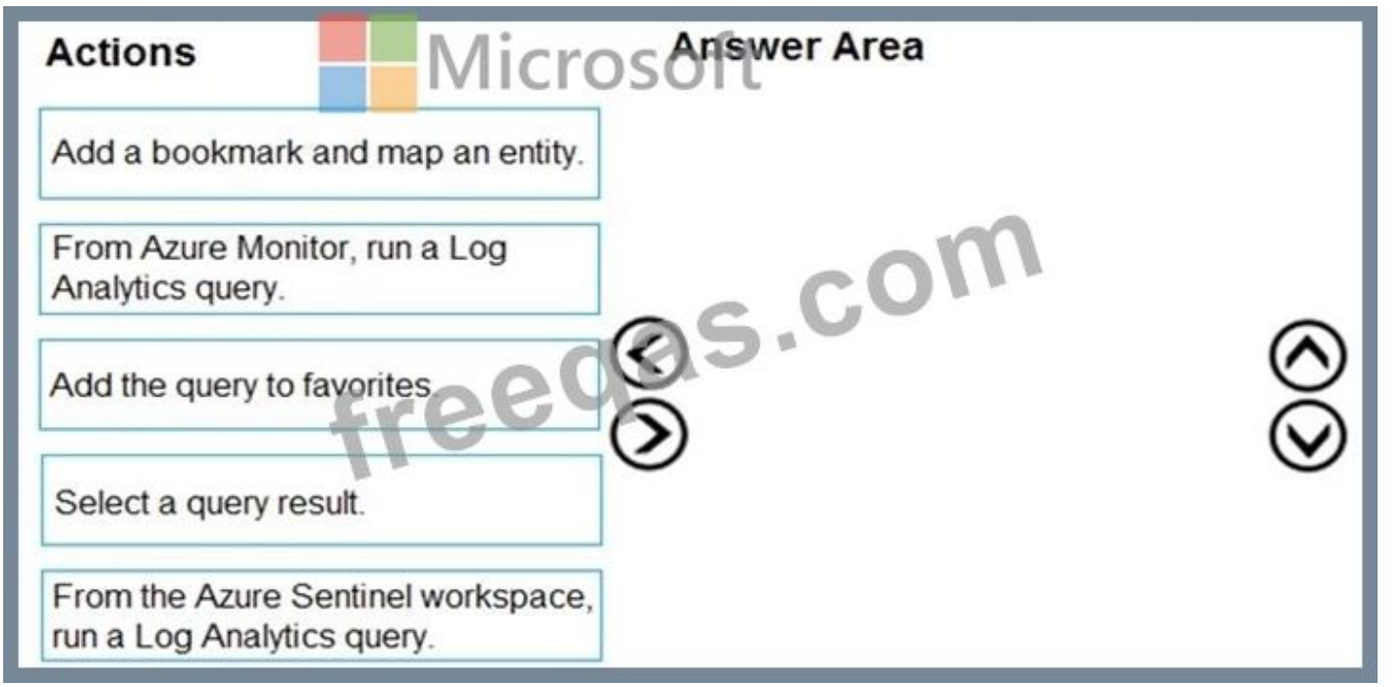
Answer:



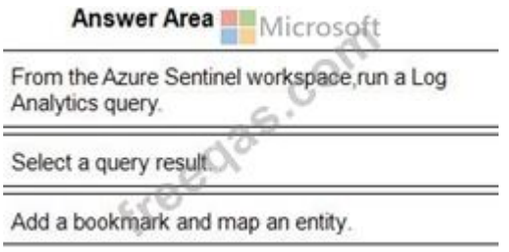
Section: [none]
Explanation/Reference:
https://docs.microsoft.com/en-us/azure/security-center/security-center-alert-validation

NEW QUESTION: 6
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 (LEAVE A REPLY)
Section: [none]
Explanation/Reference:
https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/indicator-file?view=o365-worldwide

NEW QUESTION: 7
You need to add notes to the events to meet the Azure Sentinel requirements.
Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of action to the answer area and arrange them in the correct order.



Answer:



1 - From the Azure Sentinel workspace,run a Log Analytics query.

2 - Select a query result.

3 - Add a bookmark and map an entity.

Reference:

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

NEW QUESTION: 8

You need to recommend a solution to meet the technical requirements for the Azure virtual machines. What should you include in the recommendation?

A. just-in-time (JIT) access

B. Azure Defender

C. Azure Firewall

D. Azure Application Gateway

Answer: B (LEAVE A REPLY)

Reference:

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

NEW QUESTION: 9

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 (LEAVE A REPLY)
Reference:
https://docs.microsoft.com/en-us/azure/information-protection/what-is-information-protection

NEW QUESTION: 10
You need to visualize Azure Sentinel data and enrich the data by using third-party data sources to identify indicators of compromise (IoC).
What should you use?
A. Microsoft Cloud App Security
B. Azure Monitor
C. hunting queries in Azure Sentinel
D. notebooks in Azure Sentinel
Answer: (SHOW ANSWER)
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: 11
Your company stores the data for every project in a different Azure subscription. All the subscriptions use the same Azure Active Directory (Azure AD) tenant.
Every project consists of multiple Azure virtual machines that run Windows Server. The Windows events of the virtual machines are stored in a Log Analytics workspace in each machine's respective subscription.
You deploy Azure Sentinel to a new Azure subscription.
You need to perform hunting queries in Azure Sentinel to search across all the Log Analytics workspaces of all the subscriptions.
Which two actions should you perform? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.
A. Add the Security Events connector to the Azure Sentinel workspace.
B. Create a query that uses the workspace expression and the union operator.

C. Use the alias statement.
D. Create a query that uses the resource expression and the alias operator.
E. Add the Azure Sentinel solution to each workspace.
Answer: B,E (LEAVE A REPLY)
Reference:
https://docs.microsoft.com/en-us/azure/sentinel/extend-sentinel-across-workspaces-tenants

NEW QUESTION: 12
The issue for which team can be resolved by using Microsoft Defender for Office 365?
A. executive
B. marketing
C. security
D. sales
Answer: B (LEAVE A REPLY)
Section: [none]
Explanation/Reference:
https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/atp-for-spo-odb-and-teams?
view=o365-worldwide
Testlet 2
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 company.
Litware has offices in Boston and Seattle. Litware also has remote users located across the United States. To access Litware resources, including cloud resources, the remote users establish a VPN connection to either office.
Existing Environment
Identity Environment
The network contains an Active Directory forest named litware.com that syncs to an Azure Active Directory (Azure AD) tenant named litware.com.
Microsoft 365 Environment
Litware has a Microsoft 365 E5 subscription linked to the litware.com Azure AD tenant. Microsoft Defender for Endpoint is deployed to all computers that run Windows 10. All Microsoft Cloud App Security built-in anomaly detection policies are enabled.
Azure Environment
Litware has an Azure subscription linked to the litware.com Azure AD tenant. The subscription contains resources in the East US Azure region as shown in the following table.

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

Network Environment
Each Litware office connects directly to the internet and has a site-to-site VPN connection to the virtual networks in the Azure subscription.
On-premises Environment
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
Cloud App Security frequently generates false positive alerts when users connect to both offices simultaneously.
Planned Changes
Litware plans to implement the following changes:
* Create and configure Azure Sentinel in the Azure subscription.
* Validate Azure Sentinel functionality by using Azure AD test user accounts.
Business Requirements
Litware identifies the following business requirements:
* 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 security labels and are stored on the Windows 10 computers must be available from the Azure Information Protection - Data discovery dashboard.
Microsoft Defender for Endpoint requirements
All Cloud App Security unsanctioned apps must be blocked on the Windows 10 computers by using Microsoft Defender for Endpoint.
Microsoft Cloud App Security requirements
Cloud App Security must identify whether a user connection is anomalous based on tenant-level data.
Azure Defender Requirements
All servers must send logs to the same Log Analytics workspace.
Azure Sentinel Requirements
Litware must meet the following Azure Sentinel requirements:
* Integrate Azure Sentinel and Cloud App Security.
* Ensure that a user named admin1 can configure Azure Sentinel playbooks.
* Create an Azure Sentinel analytics rule based on a custom query. The rule must automatically initiate the execution of a playbook.
* Add notes to events that represent data access from a specific IP address to provide the ability to reference the IP address when navigating through an investigation graph while hunting.
* Create a test rule that generates alerts when inbound access to Microsoft Office 365 by the Azure AD test user accounts is detected. Alerts generated by the rule must be grouped into individual incidents, with one incident per test user account.

NEW QUESTION: 13
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": "[ Microsoft.Automation | Microsoft.Logic | Microsoft.Security ]/automations",
    "apiVersion": "2019-01-01-preview",
    "name": "[parameters('name')]",
    "location": "[parameters('location')]",
    "properties": {
      "description": "[format(variables('description'), '{0}', parameters
('subscriptionId'))]",
      "isEnabled": true,
      "actions": [
        {
          "actionType": "LogicApp",
          "logicAppResourceId": "[resourceId('ITEM2/workflows', parameters
('appName'))]",
          "uri": "[listCallbackURL(resourceId(parameters('subscriptionId'),
parameters('resourceGroupName'), '[ Microsoft.Automation | Microsoft.Logic | Microsoft.Security ]/workflows/triggers',
parameters('appName'), 'manual'), '2019-05-01').value]"
        }
      ],
```


Answer:

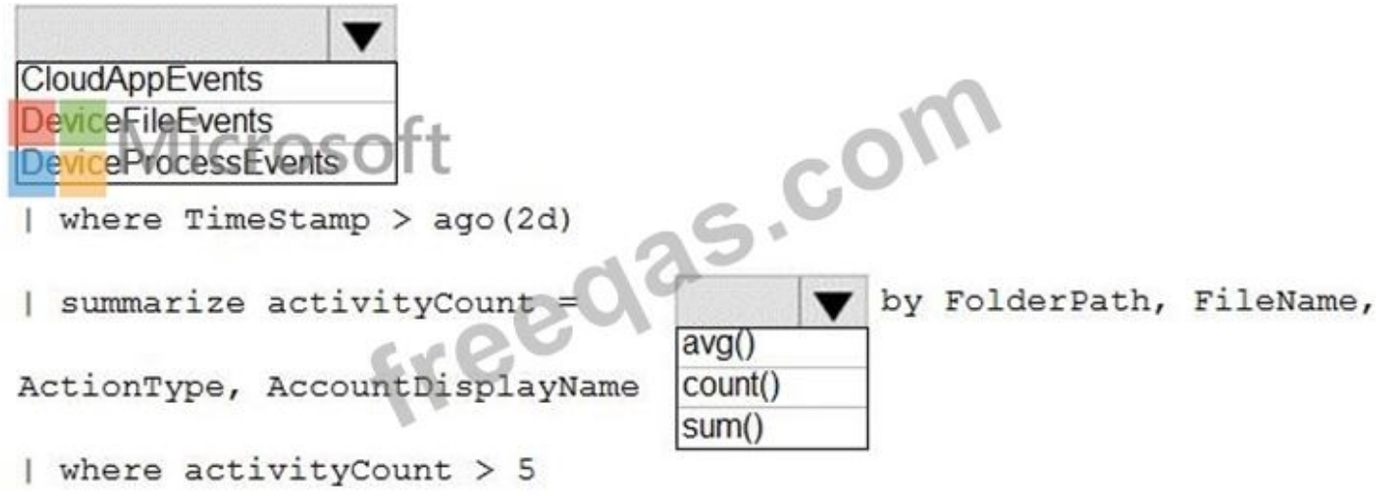
Answer Area

```
"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]"
           }
     ],
```

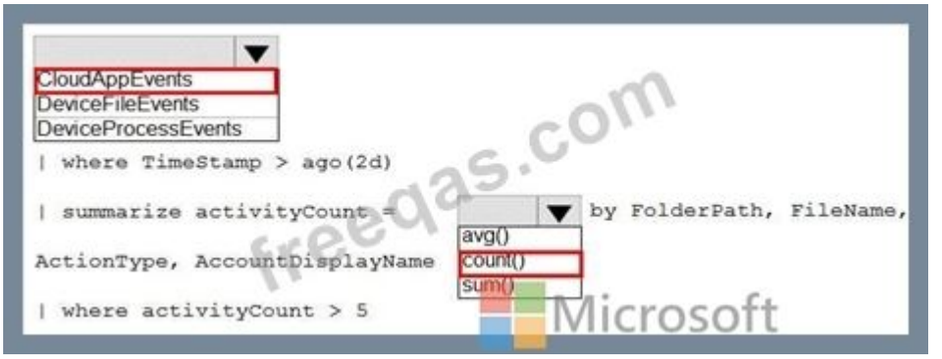
- Microsoft.Automation
- Microsoft.Logic
- Microsoft.Security

Section: [none]
Explanation/Reference:
https://docs.microsoft.com/en-us/azure/security-center/quickstart-automation-alert

NEW QUESTION: 14
You need to create an advanced hunting query to investigate the executive team issue.
How should you complete the query? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



Answer:



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

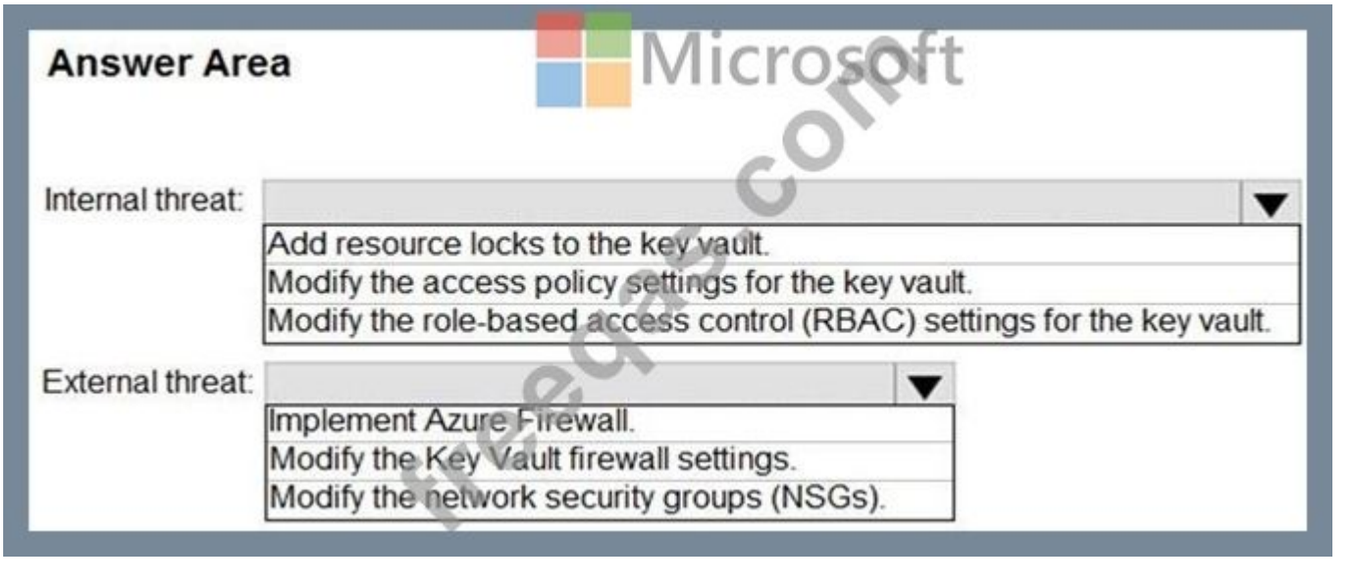
To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. 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.

NEW QUESTION: 15

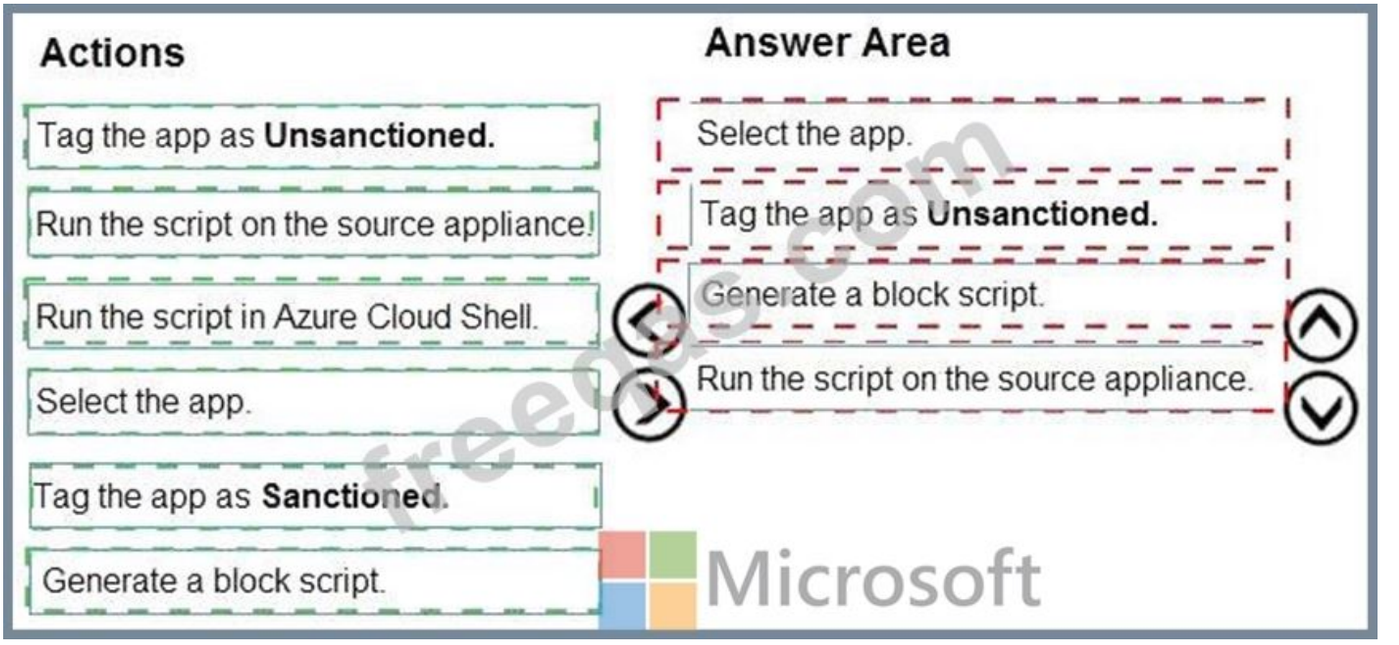
You need to recommend remediation actions for the Azure Defender alerts for Fabrikam.

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

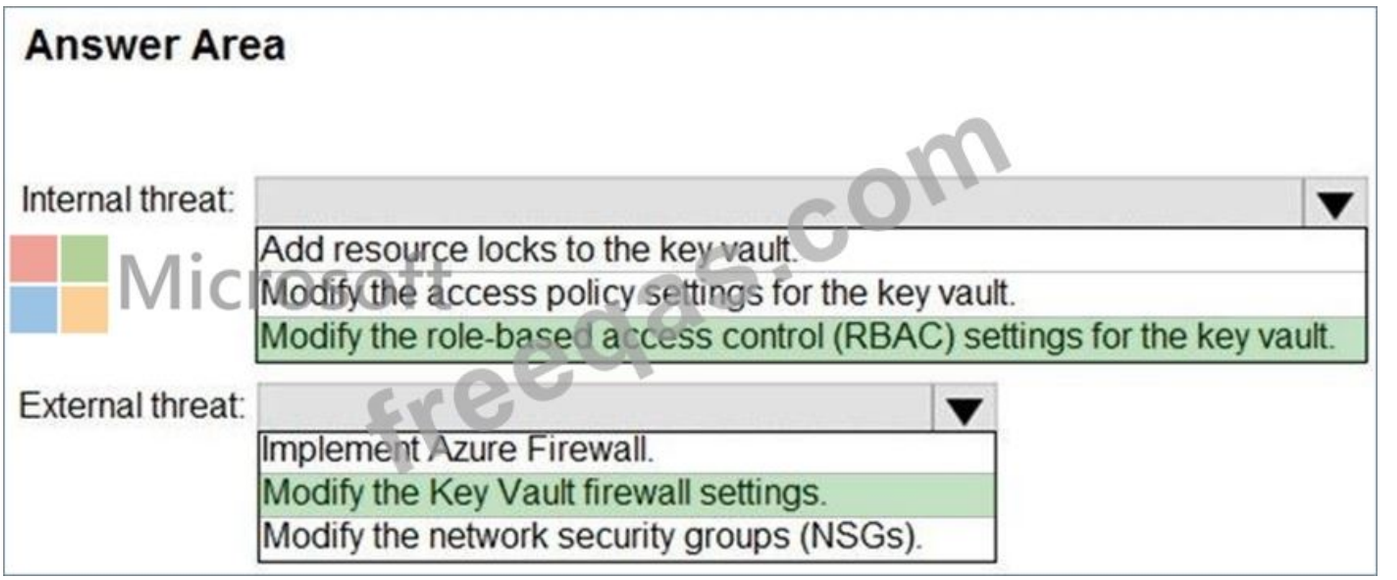
NOTE: Each correct selection is worth one point.



Answer:



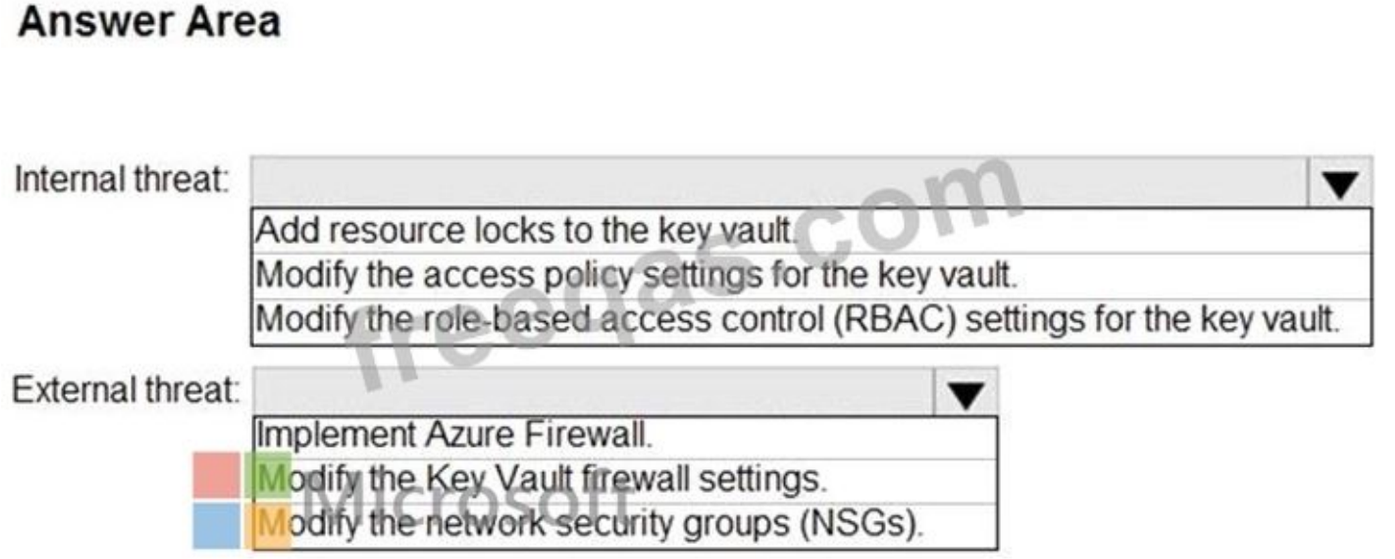
Explanation



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

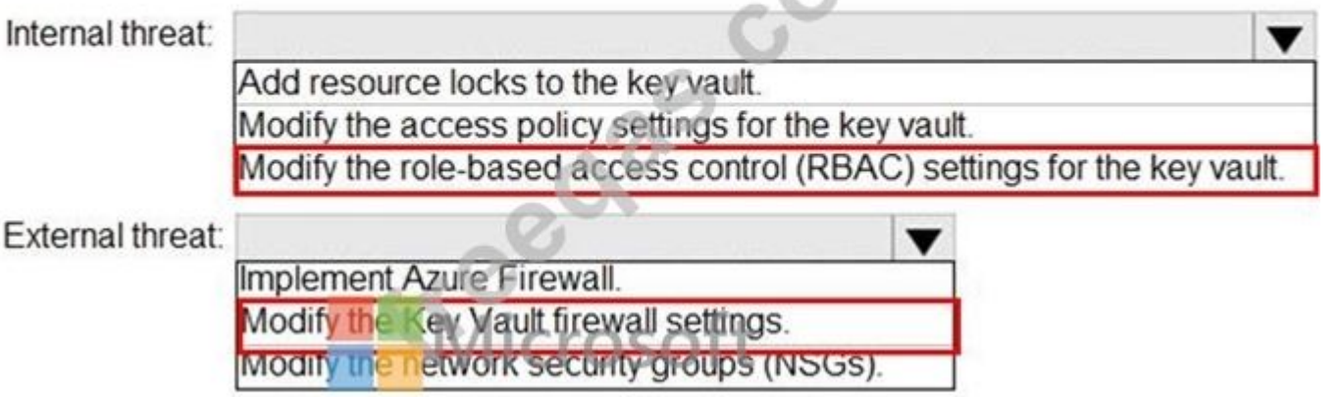
NEW QUESTION: 16

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:

Answer Area



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

NEW QUESTION: 17
The issue for which team can be resolved by using Microsoft Defender for Office 365?
A. executive
B. marketing
C. security
D. sales
Answer: B (LEAVE A REPLY)
Reference:
https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/atp-for-spo-odb-and-teams? view=o365-worldwide

NEW QUESTION: 18
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 ensure that Security Center processes events from the Azure virtual machines that report to workspace1.

What should you do?

A. In workspace1, install a solution.

B. In sub1, register a provider.

C. From Security Center, create a Workflow automation.

D. In workspace1, create a workbook.

Answer: (SHOW ANSWER)

Reference:

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

NEW QUESTION: 19

You use Azure Defender.

You have an Azure Storage account that contains sensitive information.

You need to run a PowerShell script if someone accesses the storage account from a suspicious IP address.

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

NOTE: Each correct selection is worth one point.

A. From Azure Security Center, enable workflow automation.

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

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

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

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

Answer: A,C (LEAVE A REPLY)

Section: [none]

Explanation/Reference:

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

https://docs.microsoft.com/en-us/azure/security-center/workflow-automation Testlet 1 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

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: 20

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.

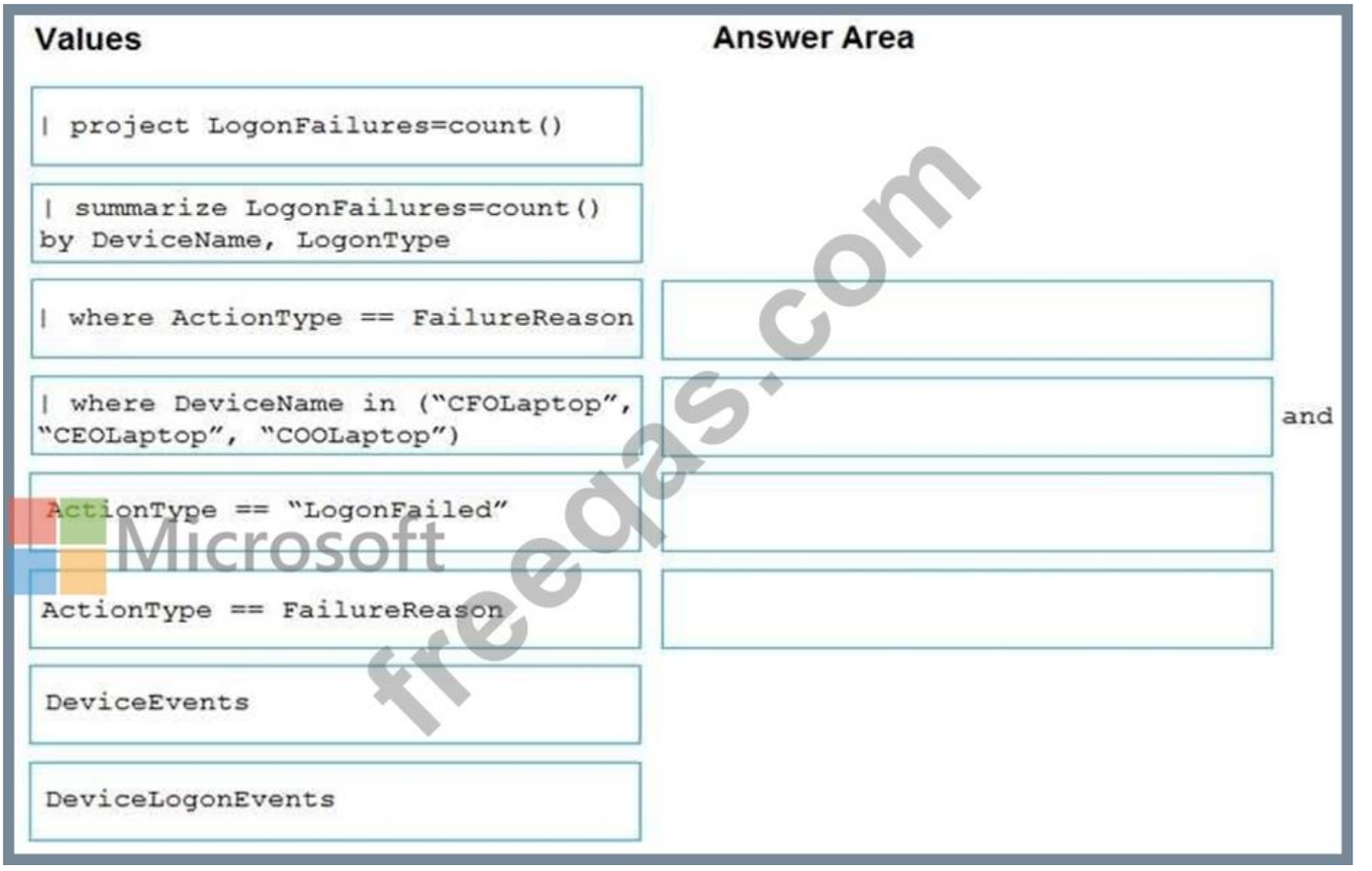
A. the Compliance Data Administrator in Azure Active Directory (Azure AD)
B. the Active remediation actions role in Microsoft Defender for Endpoint
C. the Security Administrator role in Azure Active Directory (Azure AD)
D. the Security Reader role in Azure Active Directory (Azure AD)

Answer: B,D (LEAVE A REPLY)

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

NEW QUESTION: 21

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:



Answer:

Section: [none]

NEW QUESTION: 22

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

NEW QUESTION: 23
You need to implement the Azure Information Protection requirements. What should you configure first?
A. content scan jobs in Azure Information Protection from the Azure portal
B. scanner clusters in Azure Information Protection from the Azure portal
C. Device health and compliance reports settings in Microsoft Defender Security Center
D. Advanced features from Settings in Microsoft Defender Security Center
Answer: (SHOW ANSWER)
Topic 2, Litware inc.
Existing Environment
Identity Environment
The network contains an Active Directory forest named litware.com that syncs to an Azure Active Directory (Azure AD) tenant named litware.com.
Microsoft 365 Environment
Litware has a Microsoft 365 E5 subscription linked to the litware.com Azure AD tenant. Microsoft Defender for Endpoint is deployed to all computers that run Windows 10. All Microsoft Cloud App Security built-in anomaly detection policies are enabled.
Azure Environment
Litware has an Azure subscription linked to the litware.com Azure AD tenant. The subscription contains resources in the East US Azure region as shown in the following table.

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

Network Environment

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

On-premises Environment

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

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

Planned Changes

Litware plans to implement the following changes:

Create and configure Azure Sentinel in the Azure subscription.

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

Business Requirements

Litware identifies the following business requirements:

* Azure Information Protection Requirements

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

* Microsoft Defender for Endpoint Requirements

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

Microsoft Cloud App Security Requirements

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

Azure Defender Requirements

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

Azure Sentinel Requirements

Litware must meet the following Azure Sentinel requirements:

Integrate Azure Sentinel and Cloud App Security.

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

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

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

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

NEW QUESTION: 24

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

A. executive

B. marketing

C. security

D. sales

Answer: (SHOW ANSWER)

Explanation/Reference:

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

view=o365-worldwide

Mitigate threats using Microsoft 365 Defender

Testlet 2

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 company.

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

Existing Environment

Identity Environment

The network contains an Active Directory forest named litware.com that syncs to an Azure Active Directory (Azure AD) tenant named litware.com.

Microsoft 365 Environment

Litware has a Microsoft 365 E5 subscription linked to the litware.com Azure AD tenant. Microsoft Defender for Endpoint is deployed to all computers that run Windows 10. All Microsoft Cloud App Security built-in anomaly detection policies are enabled.

Azure Environment

Litware has an Azure subscription linked to the litware.com Azure AD tenant. The subscription contains resources in the East US Azure region as shown in the following table.

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

Network Environment

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

On-premises Environment

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

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

Planned Changes

Litware plans to implement the following changes:

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

Business Requirements

Litware identifies the following business requirements:

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

Microsoft Defender for Endpoint requirements

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

Microsoft Cloud App Security requirements

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

Azure Defender Requirements
All servers must send logs to the same Log Analytics workspace.
Azure Sentinel Requirements
Litware must meet the following Azure Sentinel requirements:
* Integrate Azure Sentinel and Cloud App Security.
* Ensure that a user named admin1 can configure Azure Sentinel playbooks.
* Create an Azure Sentinel analytics rule based on a custom query. The rule must automatically initiate the execution of a playbook.
* Add notes to events that represent data access from a specific IP address to provide the ability to reference the IP address when navigating through an investigation graph while hunting.
* Create a test rule that generates alerts when inbound access to Microsoft Office 365 by the Azure AD test user accounts is detected. Alerts generated by the rule must be grouped into individual incidents, with one incident per test user account.

NEW QUESTION: 25
You are investigating an incident by using Microsoft 365 Defender.
You need to create an advanced hunting query to detect 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.

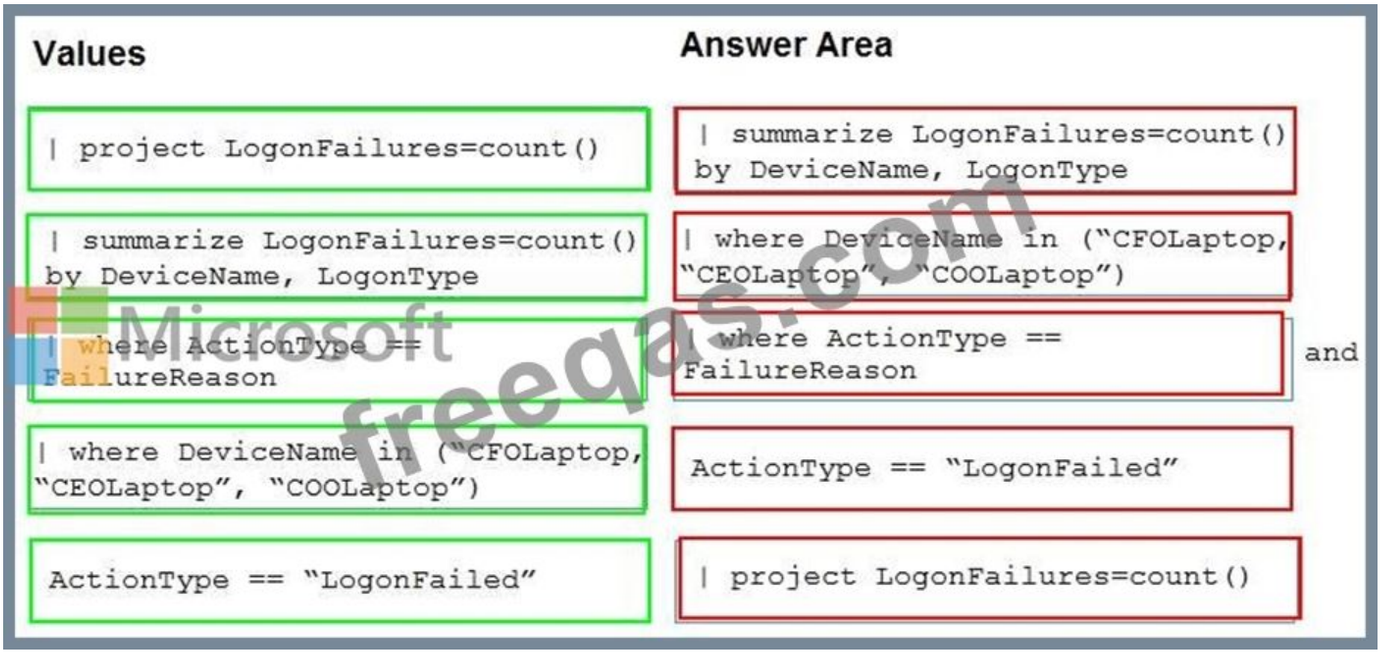
Values

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

Answer Area

```
                                    and
```


Answer:



NEW QUESTION: 26

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 Contributor for the subscription

B. the Owner role for RG1

C. the Contributor role for RG1

D. the Security Reader role for the subscription

Answer: C (LEAVE A REPLY)

NEW QUESTION: 27

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You are configuring Azure Sentinel.

You need to create an incident in Azure Sentinel when a sign-in to an Azure virtual machine from a malicious IP address is detected.

Solution: You create a hunting bookmark.

Does this meet the goal?

A. Yes

B. No

Answer: B (LEAVE A REPLY)

Section: [none]

Explanation/Reference:

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

NEW QUESTION: 28

You need to receive a security alert when a user attempts to sign in from a location that was never used by the other users in your organization to sign in.

Which anomaly detection policy should you use?

A. Impossible travel

B. Activity from anonymous IP addresses

C. Activity from infrequent country

D. Malware detection

Answer: C (LEAVE A REPLY)

Section: [none]

Explanation/Reference:

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

NEW QUESTION: 29

You are investigating an incident by using Microsoft 365 Defender.

You need to create an advanced hunting query to detect failed sign-in authentications on three devices named CFOLaptop, CEOLaptop, and COOLaptop.

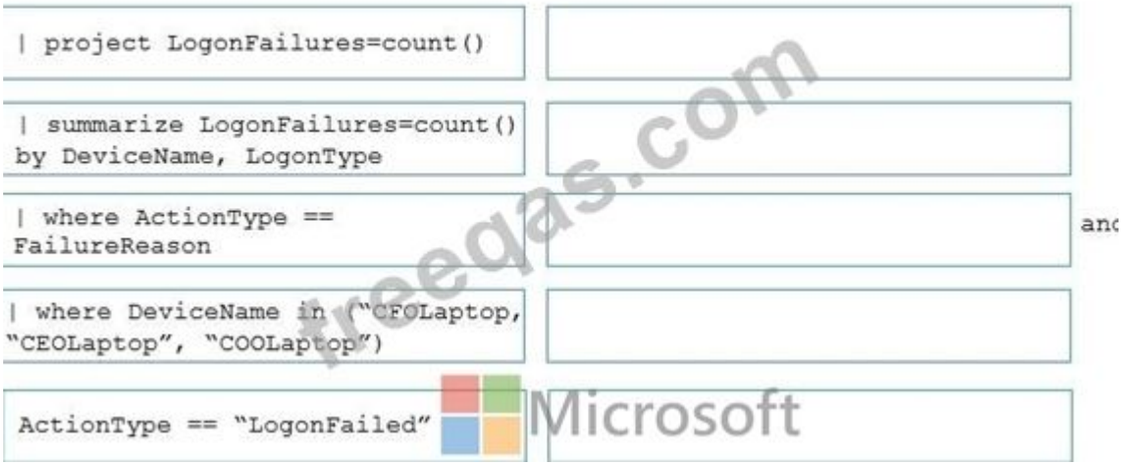
How should you complete the query? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

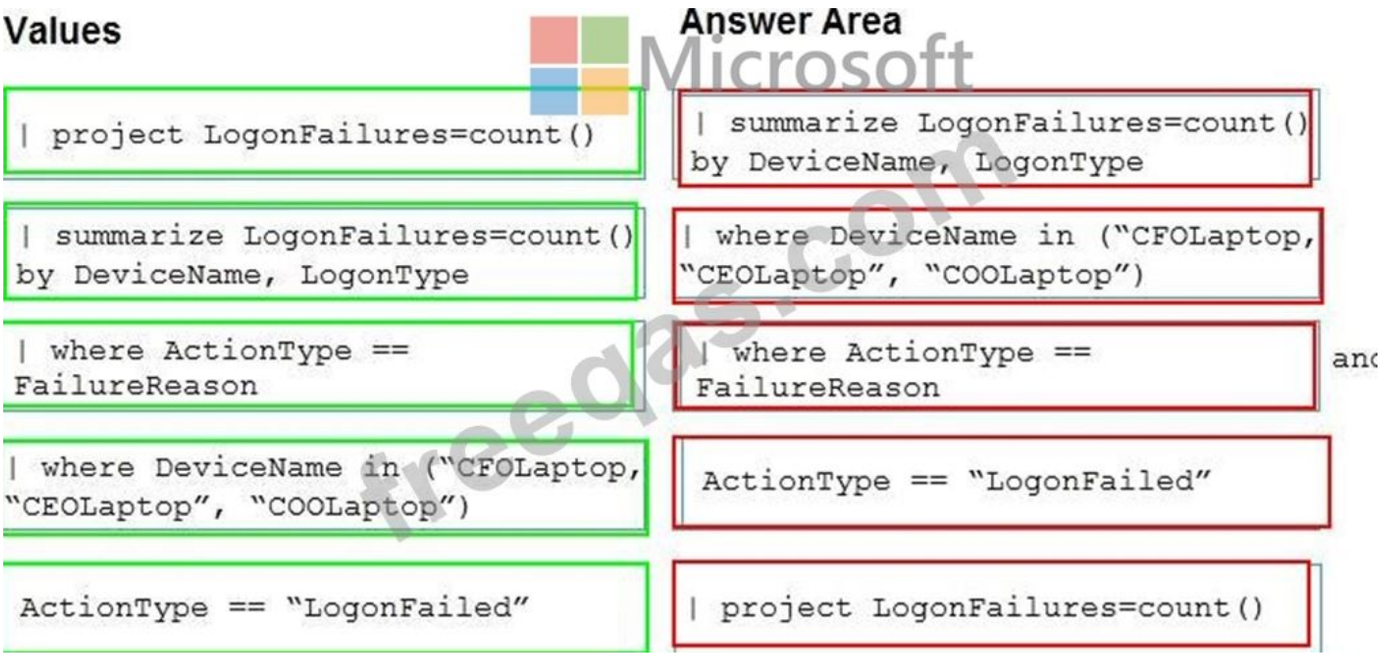
Values

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

Answer Area



Answer:



NEW QUESTION: 30

HOTSPOT

You use Azure Sentinel to monitor irregular Azure activity.

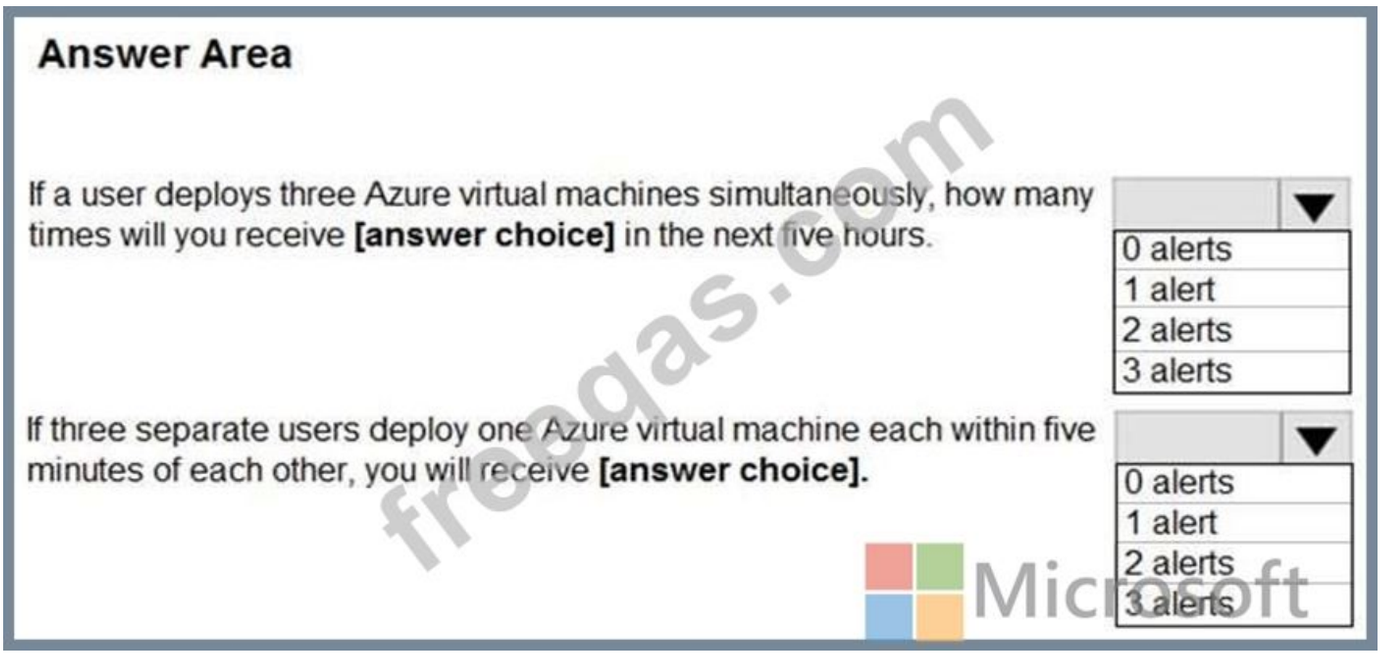
You create custom analytics rules to detect threats as shown in the following exhibit.

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

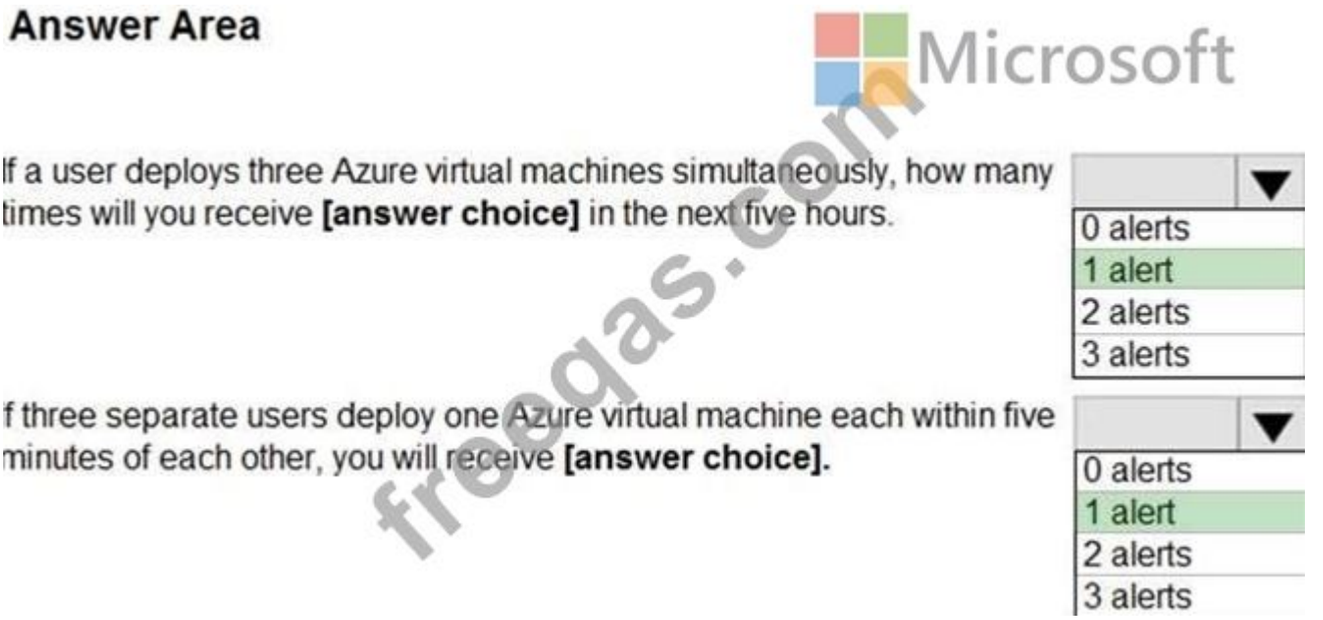
Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.

NOTE: Each correct selection is worth one point.

Hot Area:



Answer:



Section: [none]

Explanation/Reference:

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

NEW QUESTION: 31

You use Azure Sentinel to monitor irregular Azure activity.

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

Home > Azure Sentinel workspaces > Azure Sentinel

Analytics rule wizard – Edit existing rule

DeployVM

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

Define the logic for your new analytics rule.

Rule query

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

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

View query results >

Map entities

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

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

Query scheduling

Run query every *

5 | Minutes

Lookup data from the last * ⓘ

5 | Hours

Alert threshold

Generate alert when number of query results *

Is greater than | 2

Event grouping

Configure how rule query results are grouped into alerts

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

Suppression

Stop running query after alert is generated ⓘ

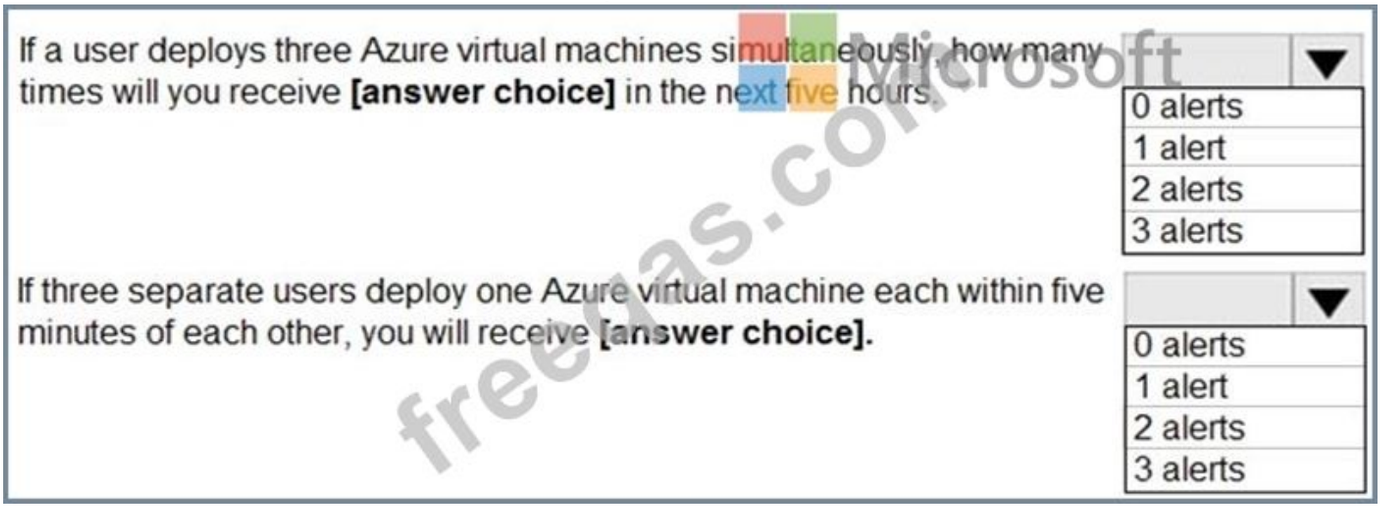
On | Off

Stop running query for *

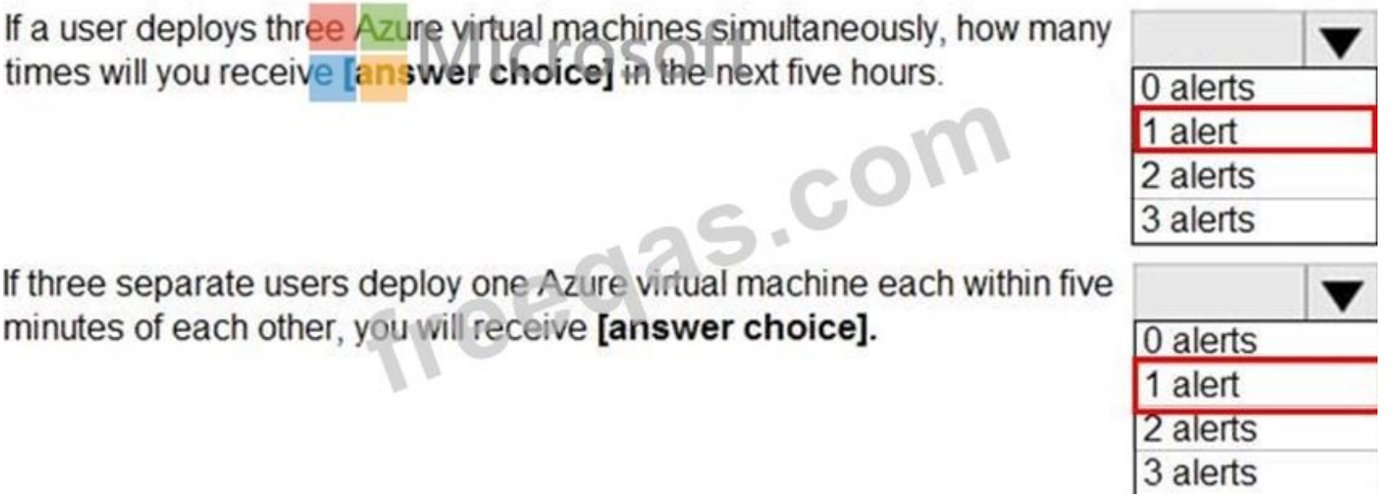
5 | Hours

Previous | Next : Incident settings >

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



Answer:



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

NEW QUESTION: 32
You have an Azure subscription.
You need to delegate permissions to meet the following requirements:

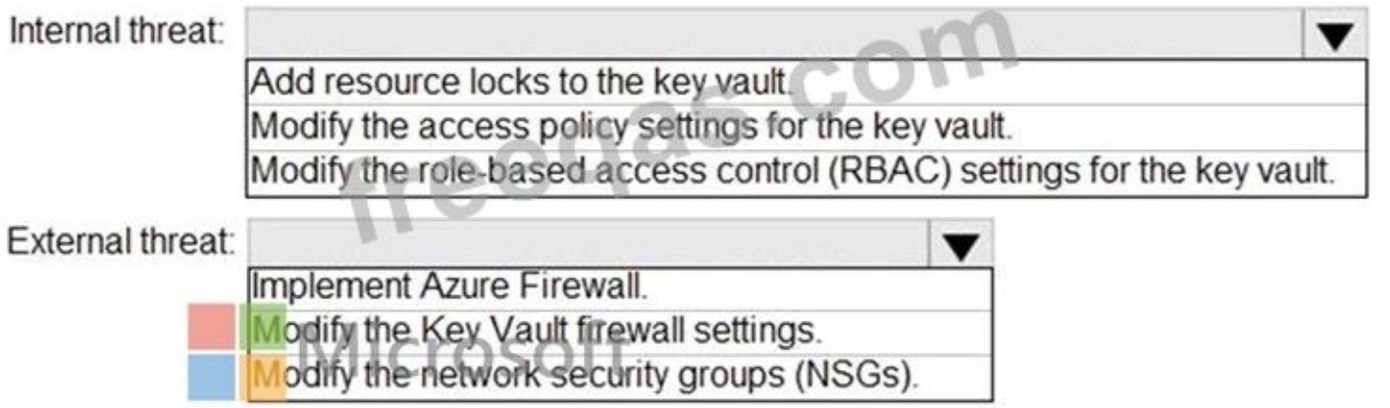
Enable and disable Azure Defender.
Apply security recommendations to resource.
The solution must use the principle of least privilege.
Which Azure Security Center role should you use for each requirement? To answer, drag the appropriate roles to the correct requirements. Each role may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.
NOTE: Each correct selection is worth one point.

Answer:

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

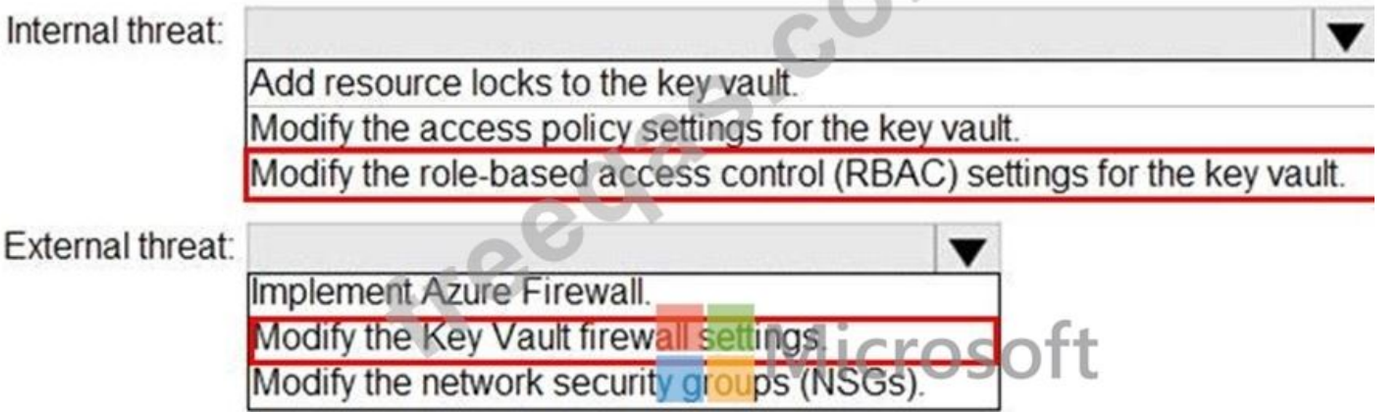
NEW QUESTION: 33
You need to recommend remediation actions for the Azure Defender alerts for Fabrikam.
What should you recommend for each threat? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Answer Area



Answer:

Answer Area



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

NEW QUESTION: 34
Your company uses Azure Sentinel.
A new security analyst reports that she cannot assign and dismiss incidents in Azure Sentinel.
You need to resolve the issue for the analyst. The solution must use the principle of least privilege. Which role should you assign to the analyst?
A. Azure Sentinel Responder
B. Logic App Contributor
C. Azure Sentinel Contributor
D. Azure Sentinel Reader
Answer: A (LEAVE A REPLY)
Reference:
https://docs.microsoft.com/en-us/azure/sentinel/roles

NEW QUESTION: 35
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: (SHOW ANSWER)
Reference:
https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/indicator-file?view=o365-worldwide

NEW QUESTION: 36
You plan to create a custom Azure Sentinel query that will provide a visual representation of the security alerts generated by Azure Security Center.
You need to create a query that will be used to display a bar graph.
What should you include in the query?
A. extend
B. bin
C. count
D. workspace
Answer: C (LEAVE A REPLY)
Section: [none]
Explanation/Reference:
https://docs.microsoft.com/en-us/azure/azure-monitor/visualize/workbooks-chart-visualizations

NEW QUESTION: 37
You have a custom analytics rule to detect threats in Azure Sentinel.
You discover that the analytics rule stopped running. The rule was disabled, and the rule name has a prefix of AUTO DISABLED.
What is a possible cause of the issue?
A. There are connectivity issues between the data sources and Log Analytics.
B. The number of alerts exceeded 10,000 within two minutes.
C. The rule query takes too long to run and times out.
D. Permissions to one of the data sources of the rule query were modified.
Answer: (SHOW ANSWER)
Reference:
https://docs.microsoft.com/en-us/azure/sentinel/tutorial-detect-threats-custom

NEW QUESTION: 38

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. Override 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: A,D (LEAVE A REPLY)

Topic 1, Litware inc.

Existing Environment

Identity Environment

The network contains an Active Directory forest named litware.com that syncs to an Azure Active Directory (Azure AD) tenant named litware.com.

Microsoft 365 Environment

Litware has a Microsoft 365 E5 subscription linked to the litware.com Azure AD tenant. Microsoft Defender for Endpoint is deployed to all computers that run Windows 10. All Microsoft Cloud App Security built-in anomaly detection policies are enabled.

Azure Environment

Litware has an Azure subscription linked to the litware.com Azure AD tenant. The subscription contains resources in the East US Azure region as shown in the following table.

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

Network Environment

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

On-premises Environment

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

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

Planned Changes

Litware plans to implement the following changes:

Create and configure Azure Sentinel in the Azure subscription.

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

Business Requirements

Litware identifies the following business requirements:

Azure Information Protection Requirements

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

Microsoft Defender for Endpoint Requirements

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

Microsoft Cloud App Security Requirements

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

Azure Defender Requirements

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

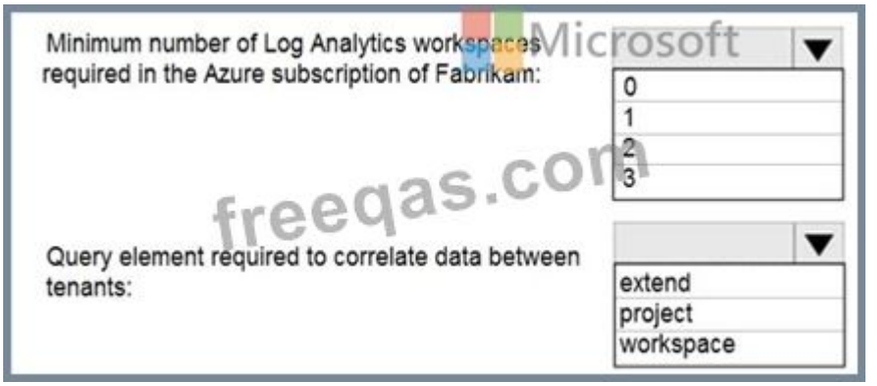
Azure Sentinel Requirements

Litware must meet the following Azure Sentinel requirements:

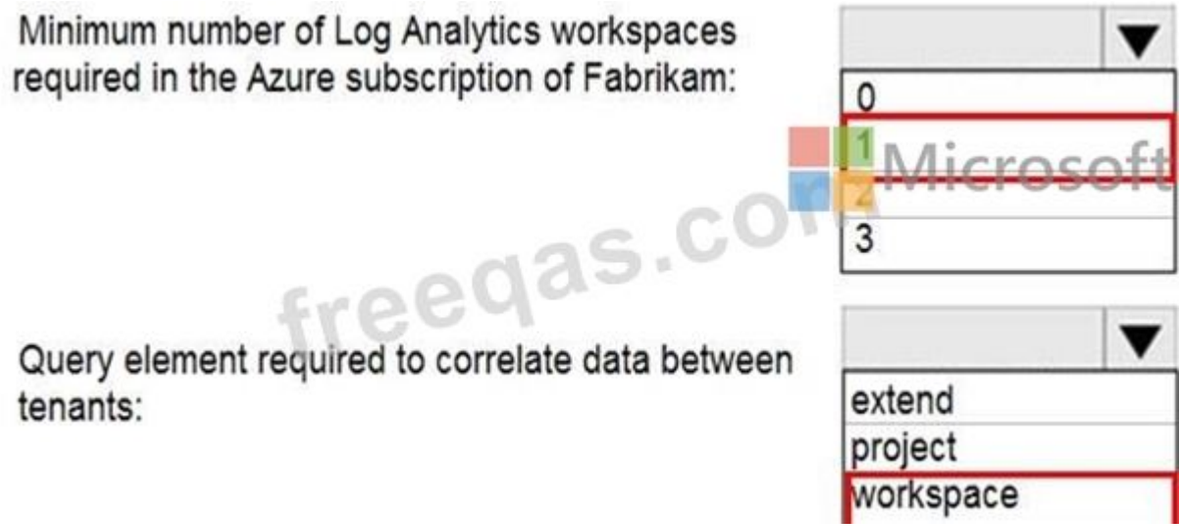
Integrate Azure Sentinel and Cloud App Security.

Ensure that a user named admin1 can configure Azure Sentinel playbooks.
Create an Azure Sentinel analytics rule based on a custom query. The rule must automatically initiate the execution of a playbook.
Add notes to events that represent data access from a specific IP address to provide the ability to reference the IP address when navigating through an investigation graph while hunting.
Create a test rule that generates alerts when inbound access to Microsoft Office 365 by the Azure AD test user accounts is detected. Alerts generated by the rule must be grouped into individual incidents, with one incident per test user account.

NEW QUESTION: 39
You need to implement Azure Sentinel queries for Contoso and Fabrikam to meet the technical requirements.
What should you include in the solution? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



Answer:



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

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.
At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.
To start the case study
To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.
Overview
Litware Inc. is a renewable company.
Litware has offices in Boston and Seattle. Litware also has remote users located across the United States. To access Litware resources, including cloud resources, the remote users establish a VPN connection to either office.

NEW QUESTION: 40
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 Identity Protection, you configure the sign-in risk policy.
Does this meet the goal?
A. Yes
B. No
Answer: B (LEAVE A REPLY)
Reference:
https://docs.microsoft.com/en-us/defender-for-identity/manage-sensitive-honeytoken-accounts

NEW QUESTION: 41
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.

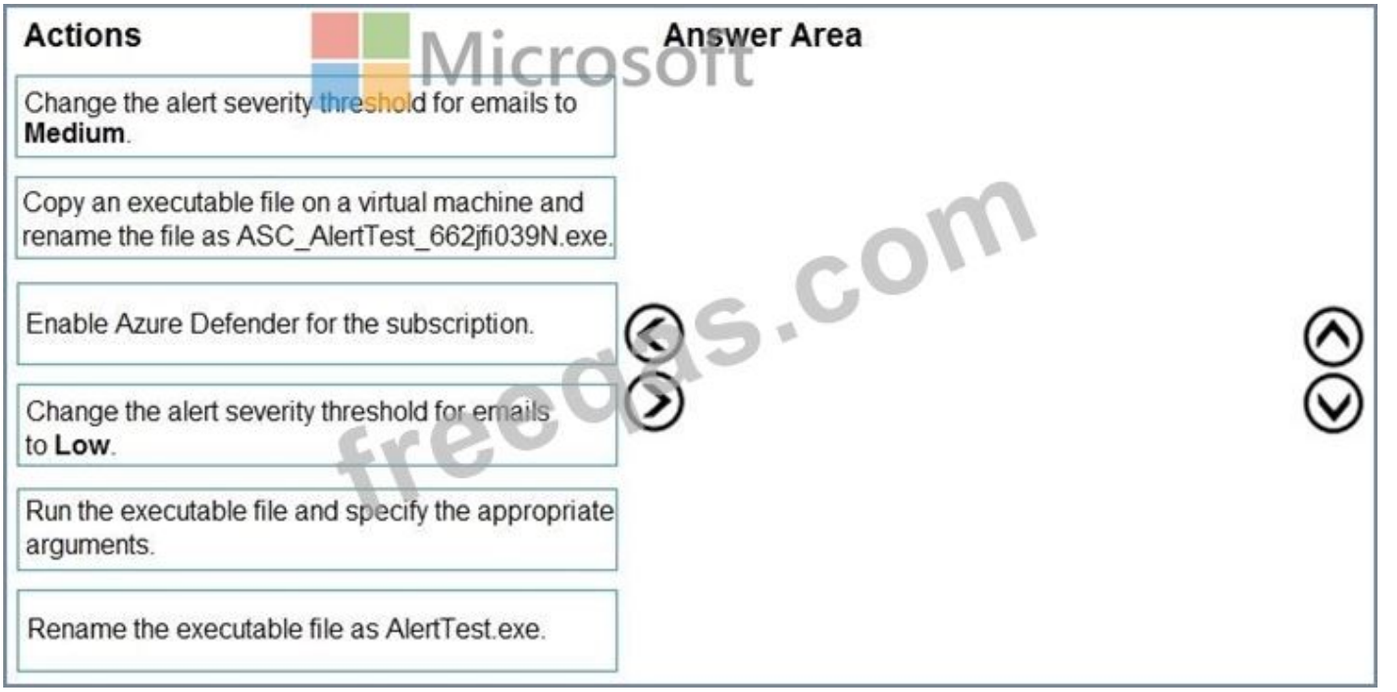
You need to ensure that SecAdmin1 can apply quick fixes to the virtual machines by using Azure Defender. The solution must use the principle of least privilege.
Which role should you assign to SecAdmin1?
A. the Security Reader role for the subscription
B. the Contributor for the subscription
C. the Contributor role for RG1
D. the Owner role for RG1
Answer: C (LEAVE A REPLY)
Section: [none]

NEW QUESTION: 42
You have an Azure Storage account that will be accessed by multiple Azure Function apps during the development of an application.
You need to hide Azure Defender alerts for the storage account.
Which entity type and field should you use in a suppression rule? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

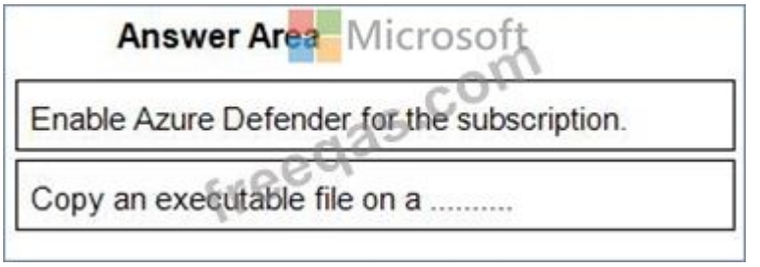
Answer:

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

NEW QUESTION: 43
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.



Answer:



1 - Enable Azure Defender for the subscription.

2 - Copy an executable file on a .....

Reference:

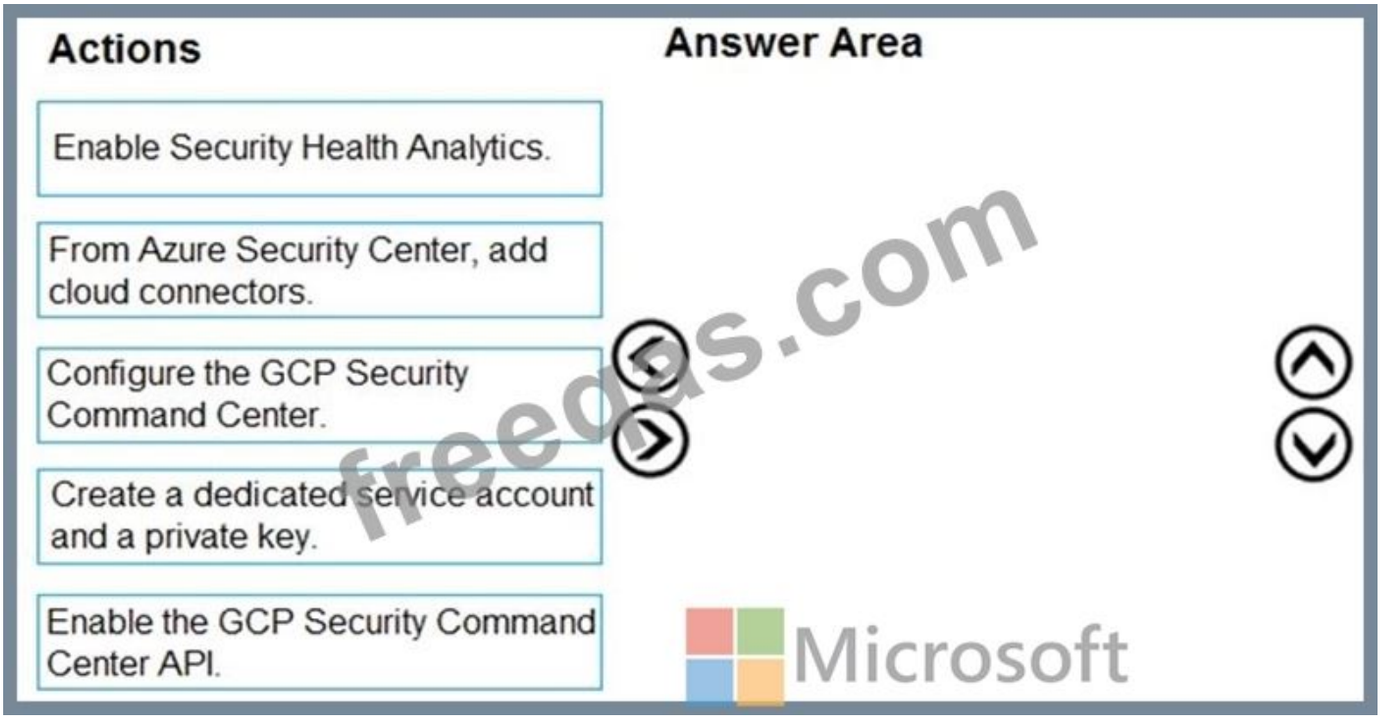
https://docs.microsoft.com/en-us/azure/security-center/security-center-alert-validation

NEW QUESTION: 44

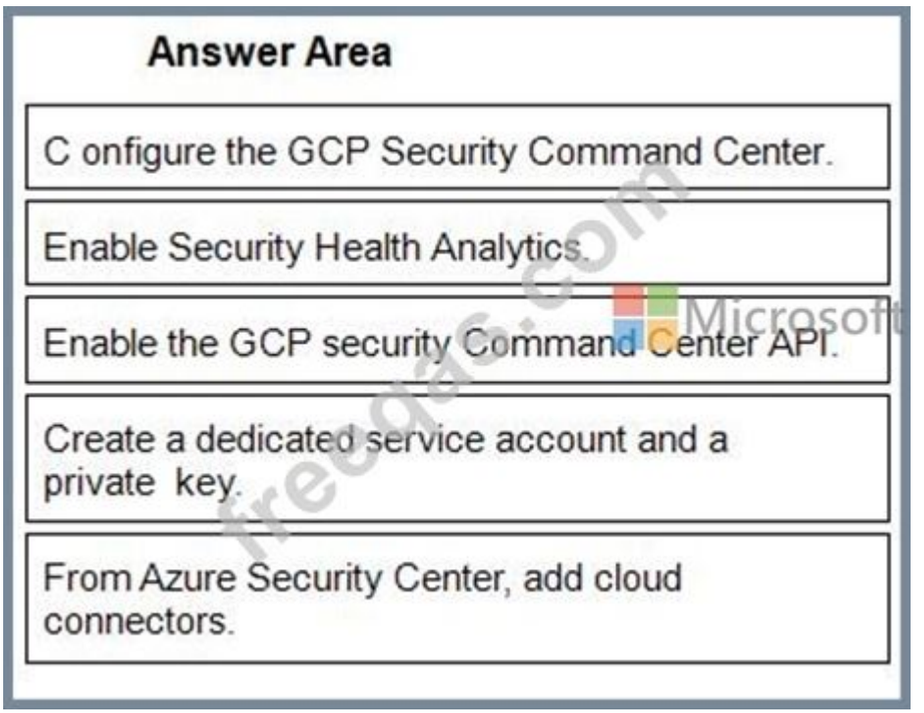
You have resources in Azure and Google cloud.

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.



Answer:



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: 45
The issue for which team can be resolved by using Microsoft Defender for Endpoint?
A. executive
B. sales
C. marketing
Answer: B (LEAVE A REPLY)
Section: [none]
Explanation/Reference:
https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/microsoft-defender-atp-ios
Testlet 1
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

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.

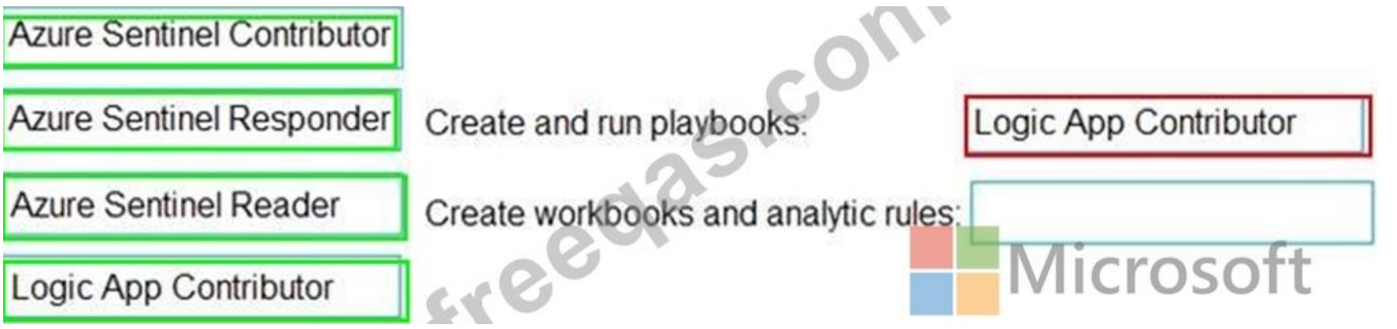
The executive team at Contoso suspects a security breach. The executive team requests that you identify which files had more than five activities during the past 48 hours, including data access, download, or deletion for Microsoft Cloud App Security-protected applications.
Requirements
Planned Changes
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: 46
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You are configuring Azure Sentinel.
You need to create an incident in Azure Sentinel when a sign-in to an Azure virtual machine from a malicious IP address is detected.
Solution: You create a hunting bookmark.
Does this meet the goal?
A. Yes
B. No
Answer: B (LEAVE A REPLY)
Reference:
https://docs.microsoft.com/en-us/azure/sentinel/connect-azure-security-center

NEW QUESTION: 47
Your company uses Azure Sentinel.
A new security analyst reports that she cannot assign and resolve incidents in Azure Sentinel.
You need to ensure that the analyst can assign and resolve incidents. The solution must use the principle of least privilege.
Which role should you assign to the analyst?
A. Azure Sentinel Responder
B. Logic App Contributor
C. Azure Sentinel Contributor
D. Azure Sentinel Reader
Answer: (SHOW ANSWER)
Section: [none]
Explanation/Reference:
https://docs.microsoft.com/en-us/azure/sentinel/roles

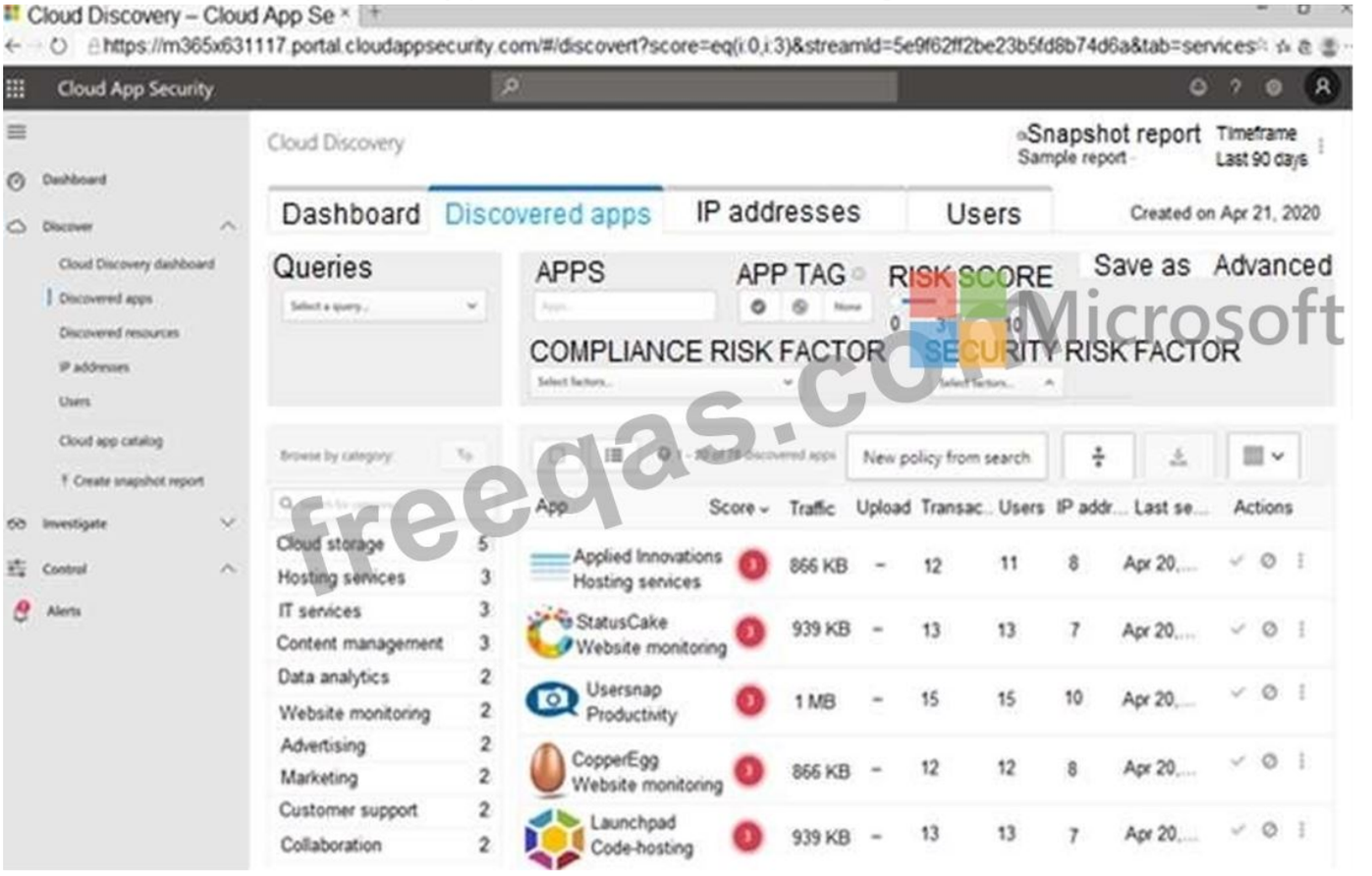
NEW QUESTION: 48
Your company deploys Azure Sentinel.
You plan to delegate the administration of Azure Sentinel to various groups.
You need to delegate the following tasks:
Create and run playbooks
Create workbooks and analytic rules.
The solution must use the principle of least privilege.
Which role 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.

Answer:



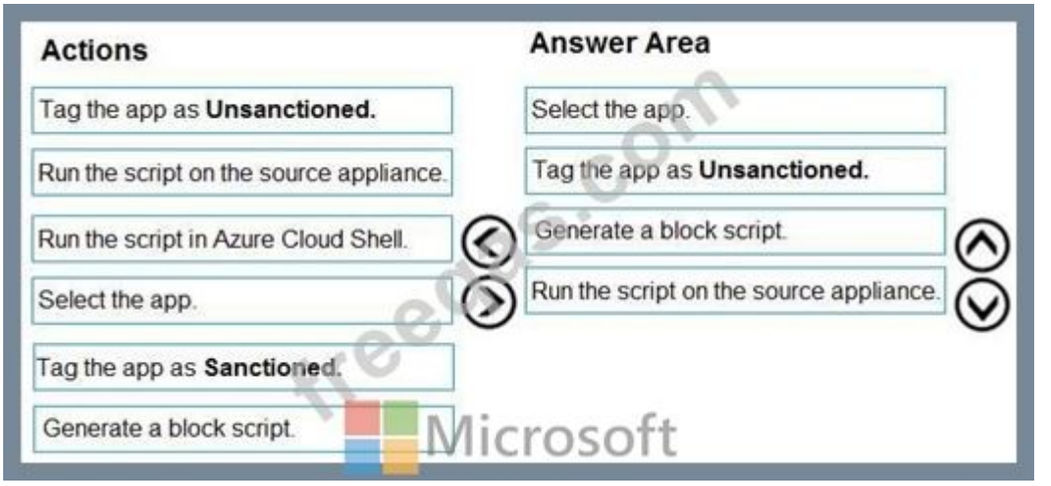
Reference:
https://docs.microsoft.com/en-us/azure/sentinel/roles

NEW QUESTION: 49
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:

Answer:



Section: [none]

Explanation/Reference:

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

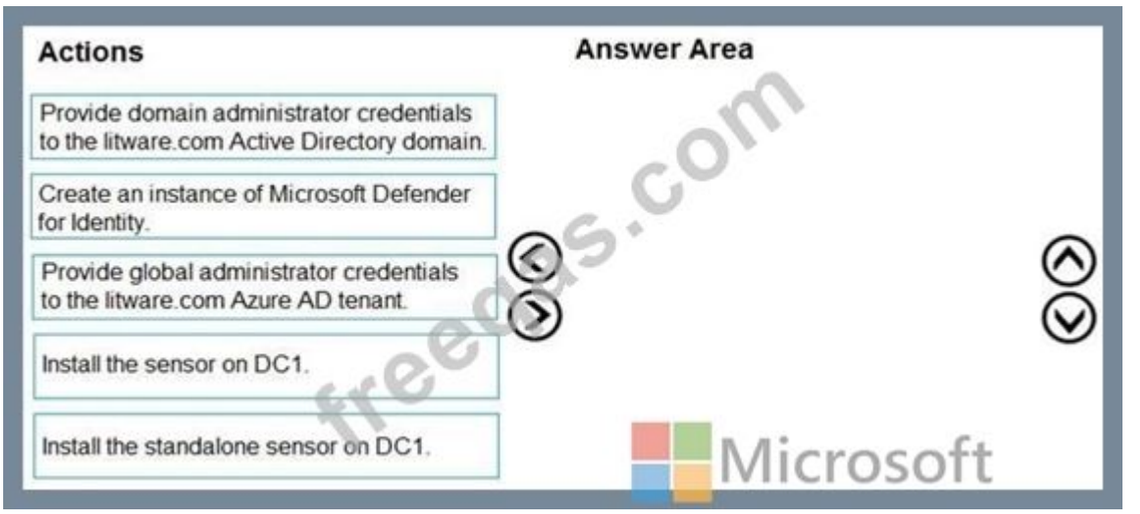
NEW QUESTION: 50

DRAG DROP

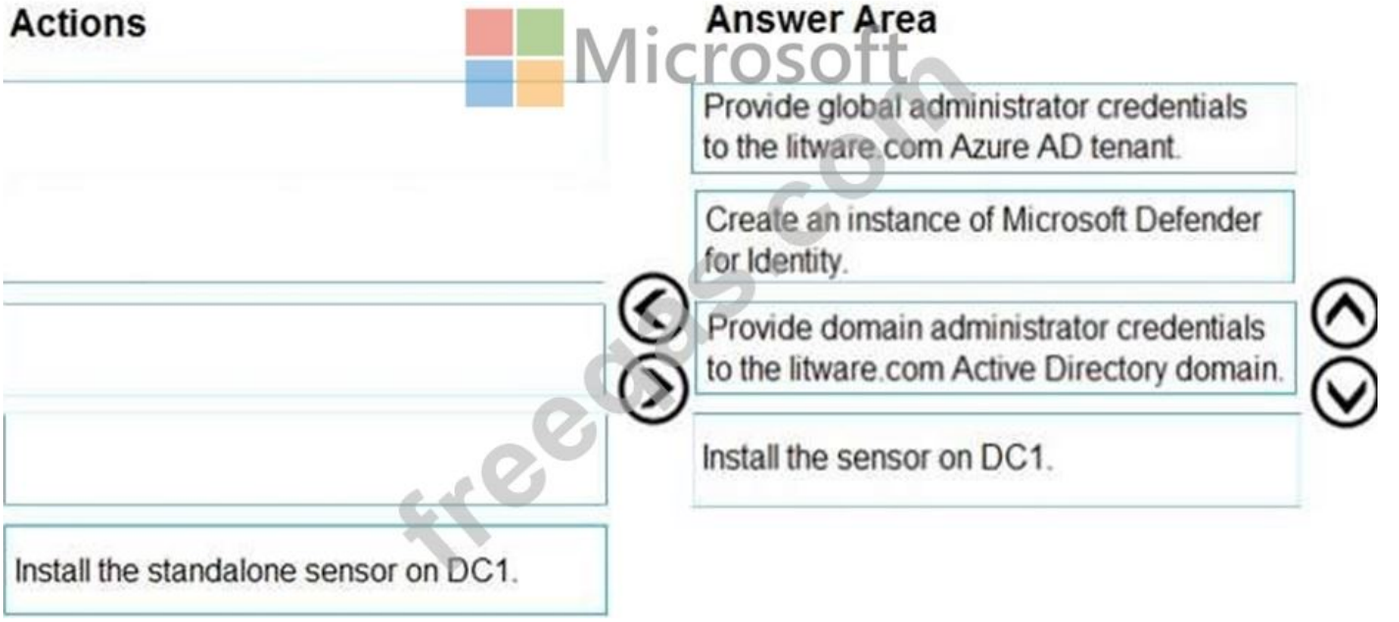
You need to configure DC1 to meet the business requirements.

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

Select and Place:



Answer:



Section: [none]

Explanation:

Step 1: log in to https://portal.atp.azure.com as a global admin

Step 2: Create the instance

Step 3. Connect the instance to Active Directory

Step 4. Download and install the sensor.

Reference:

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

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

Question Set 3

NEW QUESTION: 51

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

You discover that the rule fails intermittently.

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

NOTE: Each correct selection is worth one point.

A. Permissions to the data sources of the rule query were modified.
B. The target workspace was deleted.
C. There are connectivity issues between the data sources and Log Analytics
D. The rule query takes too long to run and times out.
Answer: C,D (LEAVE A REPLY)

NEW QUESTION: 52
You have an Azure subscription that has Azure Defender enabled for all supported resource types.
You create an Azure logic app named LA1.
You plan to use LA1 to automatically remediate security risks detected in Azure Security Center.
You need to test LA1 in Security Center.
What should you do? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Answer:

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

NEW QUESTION: 53
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You have Linux virtual machines on Amazon Web Services (AWS).
You deploy Azure Defender and enable auto-provisioning.
You need to monitor the virtual machines by using Azure Defender.
Solution: You manually install the Log Analytics agent on the virtual machines.
Does this meet the goal?
A. Yes
B. No
Answer: B (LEAVE A REPLY)
Reference:
https://docs.microsoft.com/en-us/azure/defender-for-cloud/quickstart-onboard-machines?pivots=azure-arc

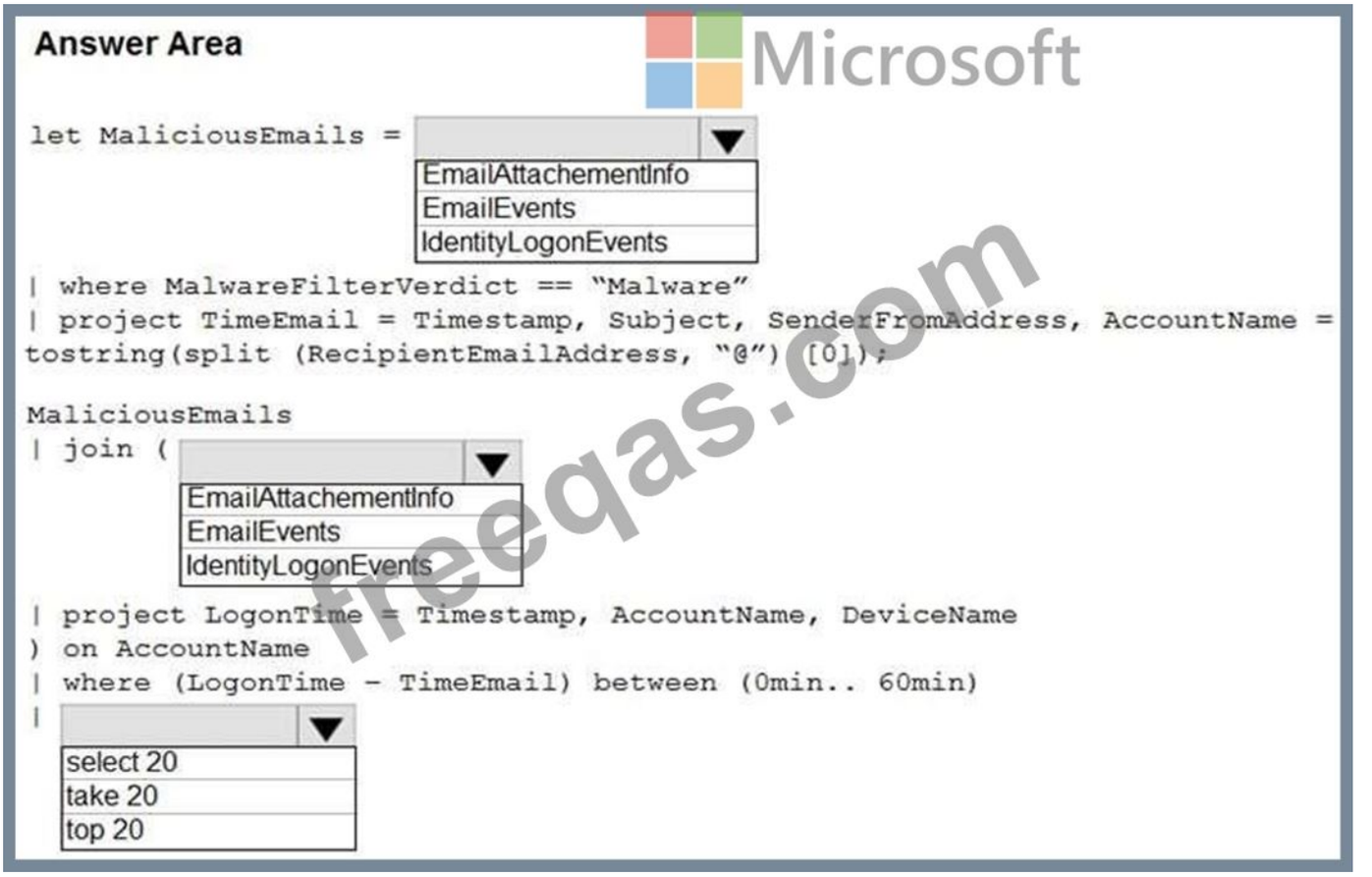
NEW QUESTION: 54
The issue for which team can be resolved by using Microsoft Defender for Office 365?
A. executive
B. marketing
C. security
D. sales
Answer: (SHOW ANSWER)
Reference:
https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/atp-for-spo-odb-and-teams?view=o365-worldwide

NEW QUESTION: 55
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 (LEAVE A REPLY)

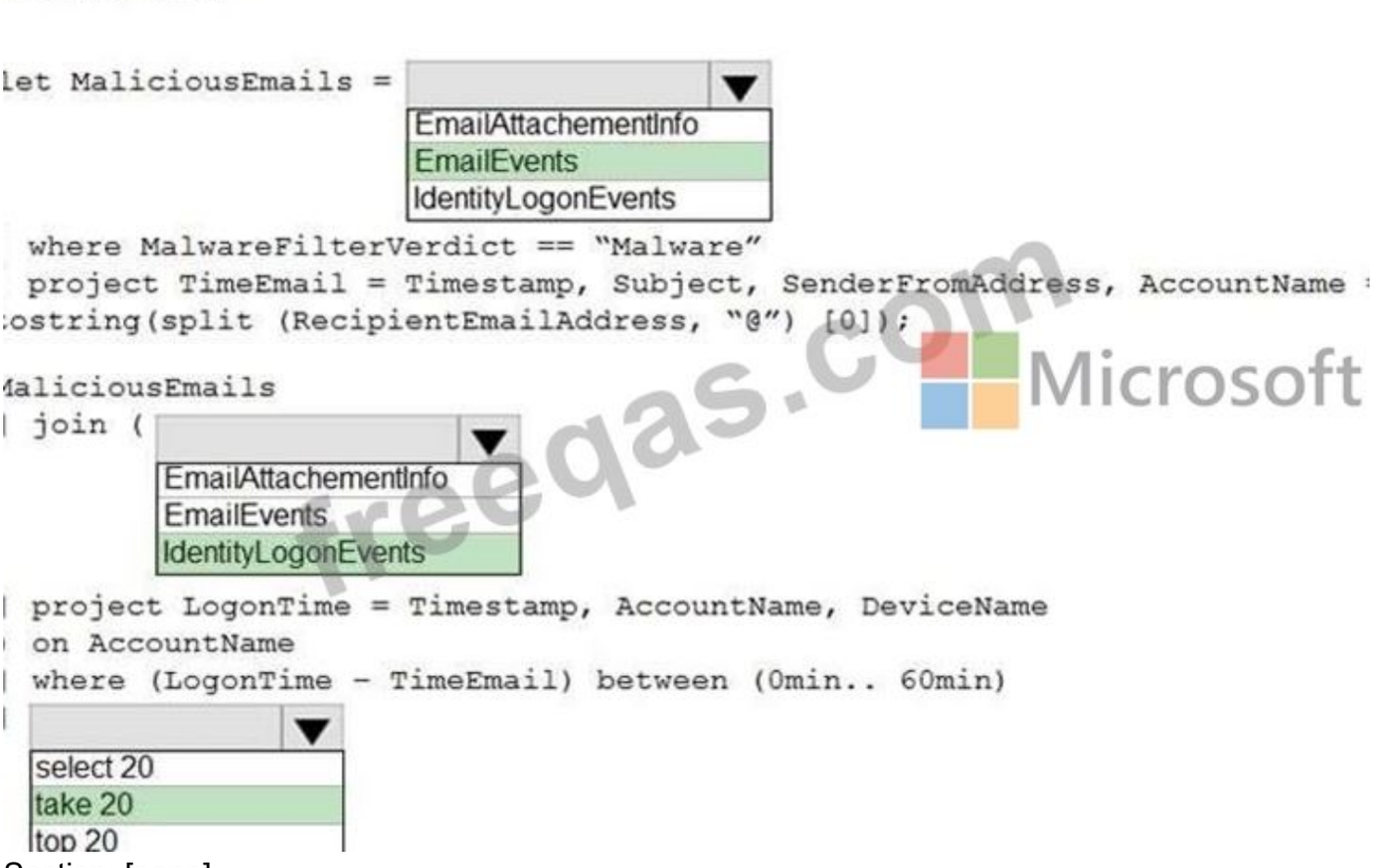
Explanation
You need to resolve the existing alert, not prevent future alerts. Therefore, you need to select the 'Mitigate the threat' option.
Reference:
https://docs.microsoft.com/en-us/azure/security-center/security-center-managing-and-responding-alerts

NEW QUESTION: 56
You are investigating a potential attack that deploys a new ransomware strain.
You plan to perform automated actions on a group of highly valuable machines that contain sensitive information.
You have three custom device groups.
You need to be able to temporarily group the machines to perform actions on the devices. Which three actions should you perform? Each correct answer presents part of the solution. NOTE: Each correct selection is worth one point.
A. Add a tag to the device group.
B. Add the device users to the admin role.
C. Add a tag to the machines.
D. Create a new device group that has a rank of 1.
E. Create a new admin role.
F. Create a new device group that has a rank of 4.
Answer: A,C,D (LEAVE A REPLY)
https://docs.microsoft.com/en-us/learn/modules/deploy-microsoft-defender-for-endpoints-environment/4-manage-access

NEW QUESTION: 57
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:

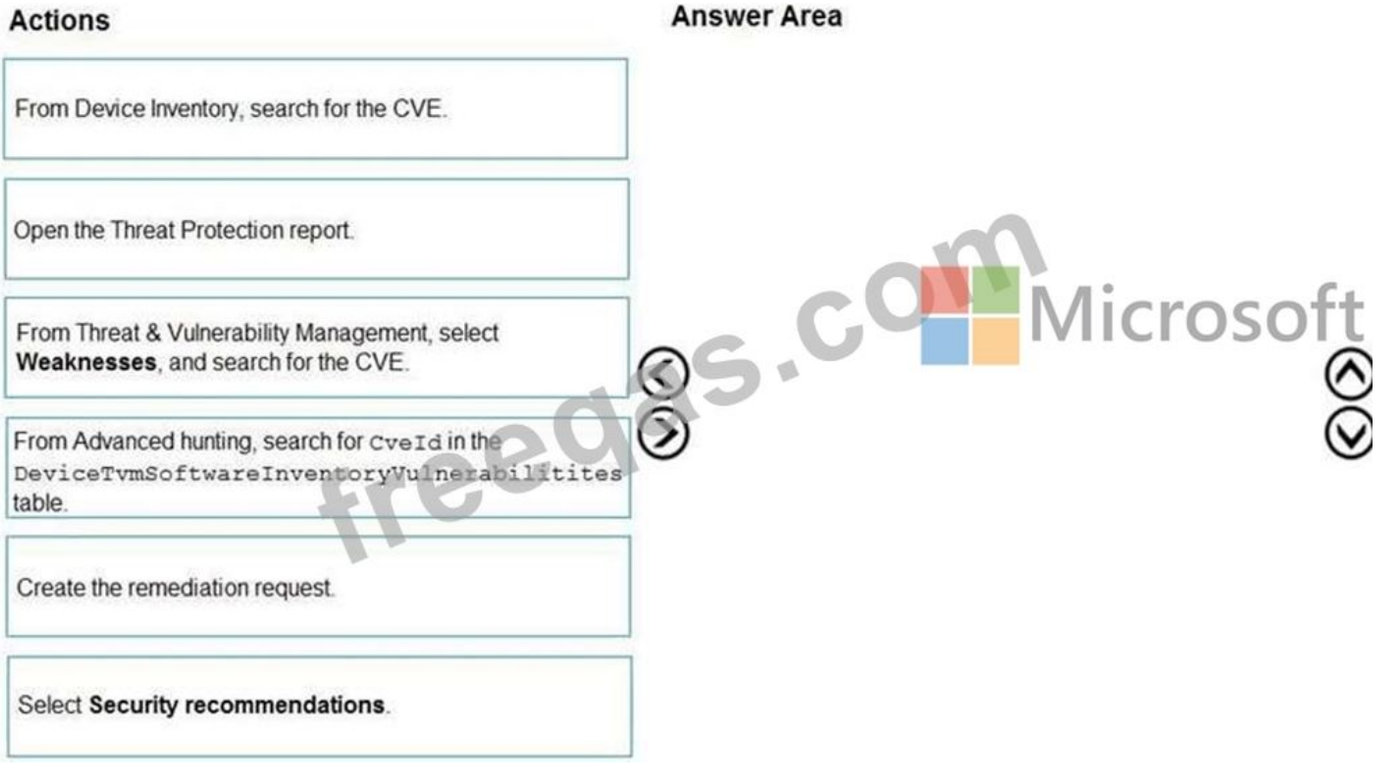


Section: [none]

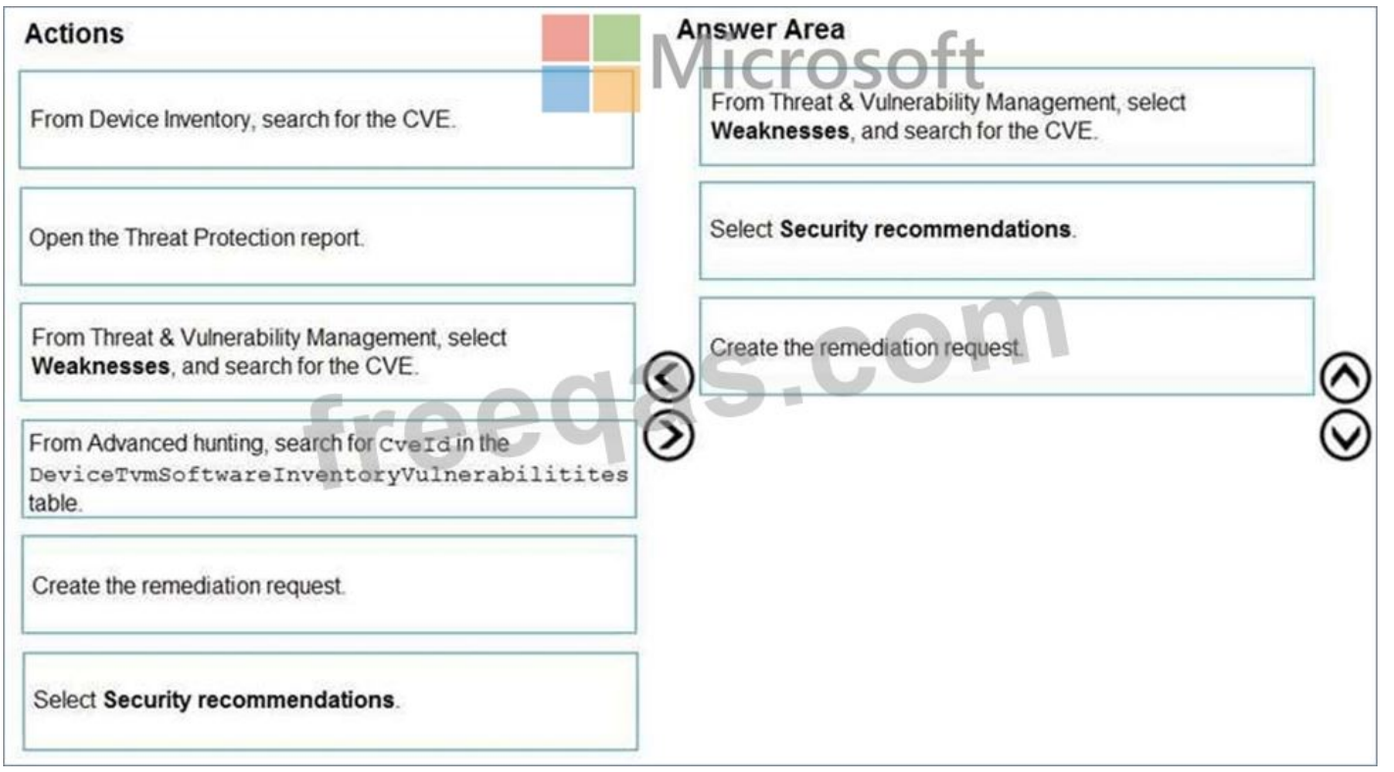
Explanation/Reference:

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

NEW QUESTION: 58
DRAG DROP
You are informed of a new common vulnerabilities and exposures (CVE) vulnerability that affects your environment.
You need to use Microsoft Defender Security Center to request remediation from the team responsible for the affected systems if there is a documented active exploit available.
Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.
Select and Place:



Answer:



Section: [none]
Explanation/Reference:
https://techcommunity.microsoft.com/t5/core-infrastructure-and-security/microsoft-defender-atp-remediate- apps-using-mem/ba-p/1599271

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 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: (SHOW ANSWER)
Section: [none]
Explanation/Reference:
https://docs.microsoft.com/en-us/azure/security-center/security-center-managing-and-responding-alerts

NEW QUESTION: 60

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 (LEAVE A REPLY)
Reference:
https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/overview-attack-surface-reduction?view=o365-worldwide

NEW QUESTION: 61
You have an existing Azure logic app that is used to block Azure Active Directory (Azure AD) users. The logic app is triggered manually.
You deploy Azure Sentinel.
You need to use the existing logic app as a playbook in Azure Sentinel.
What should you do first?
A. And a new scheduled query rule.
B. Add a data connector to Azure Sentinel.
C. Configure a custom Threat Intelligence connector in Azure Sentinel.
D. Modify the trigger in the logic app.
Answer: (SHOW ANSWER)
Section: [none]

NEW QUESTION: 62
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

Answer:

Explanation

Answer Area

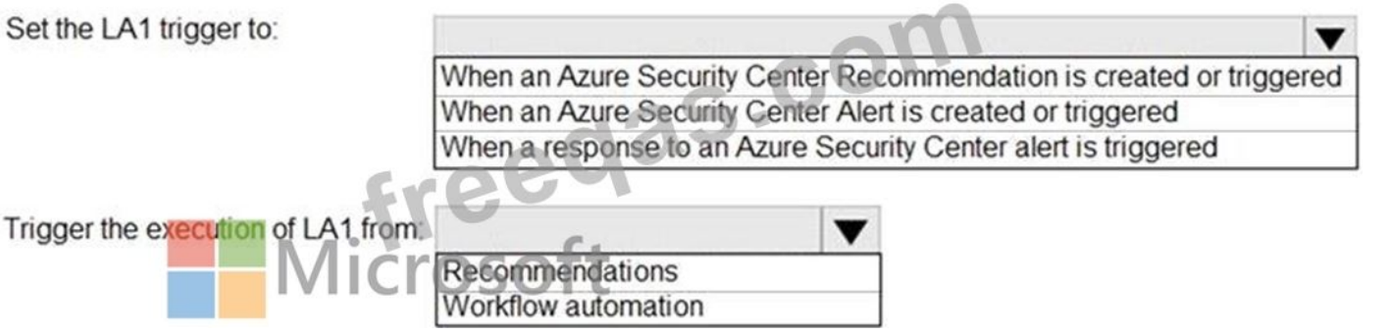
```
EmailAttachmentInfo
| where SenderFromAddress =~ "MaliciousSender@example.com"
| where isnotempty (SHA256)
| [join] (
    DeviceFileEvents
    | [project] FileName, SHA256
) on SHA256
| [project] Timestamp, FileName, SHA256, DeviceName, DeviceId,
    NetworkMessageId, SenderFromAddress, RecipientEmailAddress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

extend / join / project / union

ference:
https://docs.microsoft.com/en-us/microsoft-365/security/mtp/advanced-hunting-query-emails-devices?view=o36

NEW QUESTION: 63
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:

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: 64
You have an Azure Sentinel workspace.
You need to test a playbook manually in the Azure portal. From where can you run the test in Azure Sentinel?
A. Playbooks
B. Analytics
C. Threat intelligence
D. Incidents
Answer: (SHOW ANSWER)
Reference:
https://docs.microsoft.com/en-us/azure/sentinel/tutorial-respond-threats-playbook#run-a-playbook-on-demand

NEW QUESTION: 65
You plan to create a custom Azure Sentinel query that will track anomalous Azure Active Directory (Azure AD) sign-in activity and present the activity as a time chart aggregated by day.
You need to create a query that will be used to display the time chart.
What should you include in the query?
A. extend

B. bin
C. makeset
D. workspace
Answer: B (LEAVE A REPLY)
Section: [none]
Explanation/Reference:
https://docs.microsoft.com/en-us/azure/azure-monitor/logs/get-started-queries

NEW QUESTION: 66
Your company stores the data for every project in a different Azure subscription. All the subscriptions use the same Azure Active Directory (Azure AD) tenant.
Every project consists of multiple Azure virtual machines that run Windows Server. The Windows events of the virtual machines are stored in a Log Analytics workspace in each machine's respective subscription.
You deploy Azure Sentinel to a new Azure subscription.
You need to perform hunting queries in Azure Sentinel to search across all the Log Analytics workspaces of all the subscriptions.
Which two actions should you perform? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.
A. Add the Security Events connector to the Azure Sentinel workspace.
B. Create a query that uses the workspaceexpression and the unionoperator.
C. Use the aliasstatement.
D. Create a query that uses the resourceexpression and the aliasoperator.
E. Add the Azure Sentinel solution to each workspace.
Answer: B,E (LEAVE A REPLY)
Section: [none]
Explanation/Reference:
https://docs.microsoft.com/en-us/azure/sentinel/extend-sentinel-across-workspaces-tenants

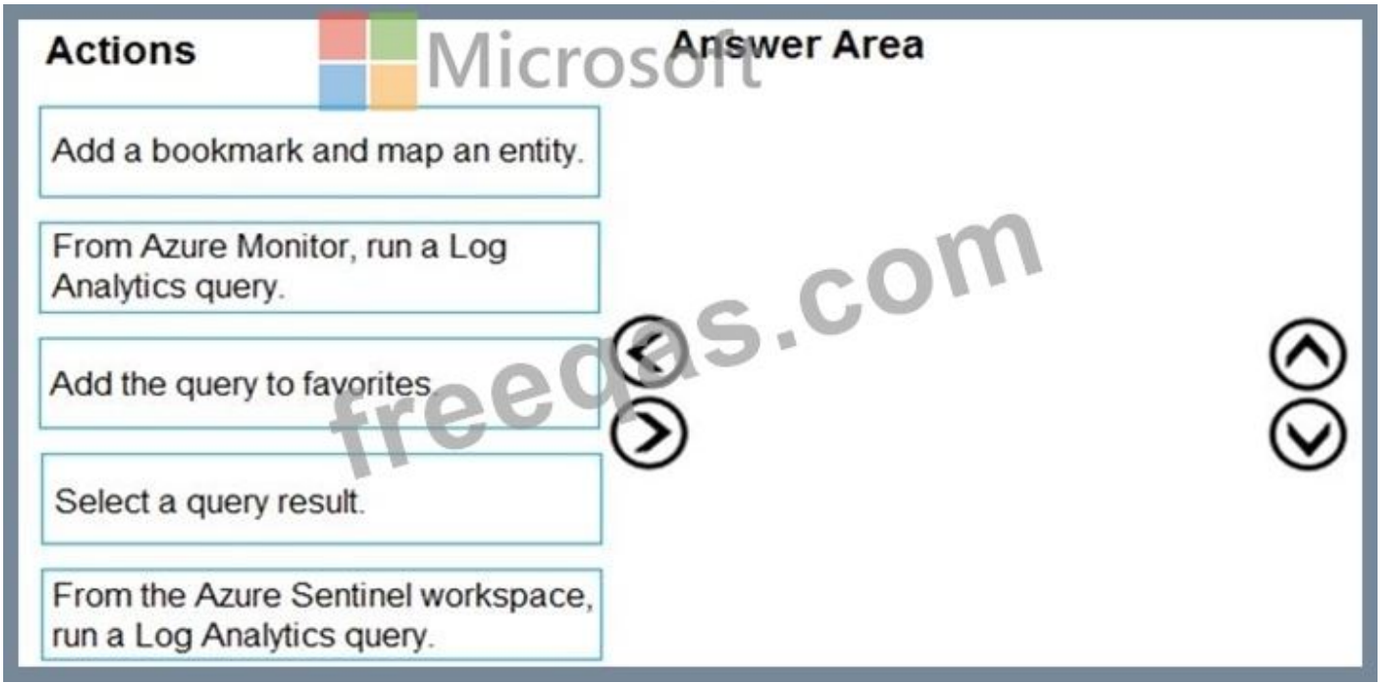
NEW QUESTION: 67
You are investigating a potential attack that deploys a new ransomware strain.
You plan to perform automated actions on a group of highly valuable machines that contain sensitive information.
You have three custom device groups.
You need to be able to temporarily group the machines to perform actions on the devices.
Which three actions should you perform? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.
A. 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: A,C,D (LEAVE A REPLY)
Section: [none]
Explanation/Reference:
https://docs.microsoft.com/en-us/learn/modules/deploy-microsoft-defender-for-endpoints-environment/4- manage-access

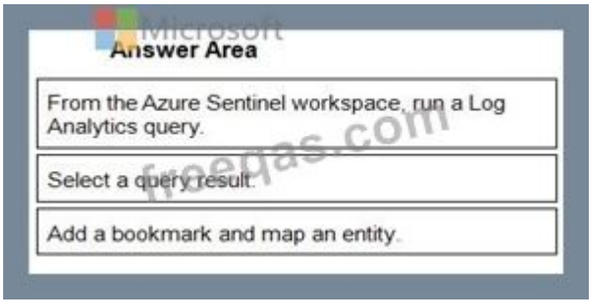
NEW QUESTION: 68
Your company uses Azure Sentinel.
A new security analyst reports that she cannot assign and dismiss incidents in Azure Sentinel.
You need to resolve the issue for the analyst. The solution must use the principle of least privilege. Which role should you assign to the analyst?
A. Azure Sentinel Responder
B. Logic App Contributor
C. Azure Sentinel Contributor
D. Azure Sentinel Reader
Answer: A (LEAVE A REPLY)
Reference:
https://docs.microsoft.com/en-us/azure/sentinel/roles
Topic 2, Contoso Ltd
Existing Environment
End-User Environment
All users at Contoso use Windows 10 devices. Each user is licensed for Microsoft 365. In addition, iOS devices are distributed to the members of the sales team at Contoso.
Cloud and Hybrid Infrastructure
All Contoso applications are deployed to Azure.
You enable Microsoft Cloud App Security.
Contoso and Fabrikam have different Azure Active Directory (Azure AD) tenants. Fabrikam recently purchased an Azure subscription and enabled Azure Defender for all supported resource types.
Current Problems
The security team at Contoso receives a large number of cybersecurity alerts. The security team spends too much time identifying which cybersecurity alerts are legitimate threats, and which are not.
The Contoso sales team uses only iOS devices. The sales team members exchange files with customers by using a variety of third-party tools. In the past, the sales team experienced various attacks on their devices.
The marketing team at Contoso has several Microsoft SharePoint Online sites for collaborating with external vendors. The marketing team has had several incidents in which vendors uploaded files that contain malware.

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

NEW QUESTION: 69
You need to add notes to the events to meet the Azure Sentinel requirements.
Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of action to the answer area and arrange them in the correct order.



Answer:



1 - From the Azure Sentinel workspace, run a Log Analytics query.

2 - Select a query result.

3 - Add a bookmark and map an entity.

Reference:

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

NEW QUESTION: 70

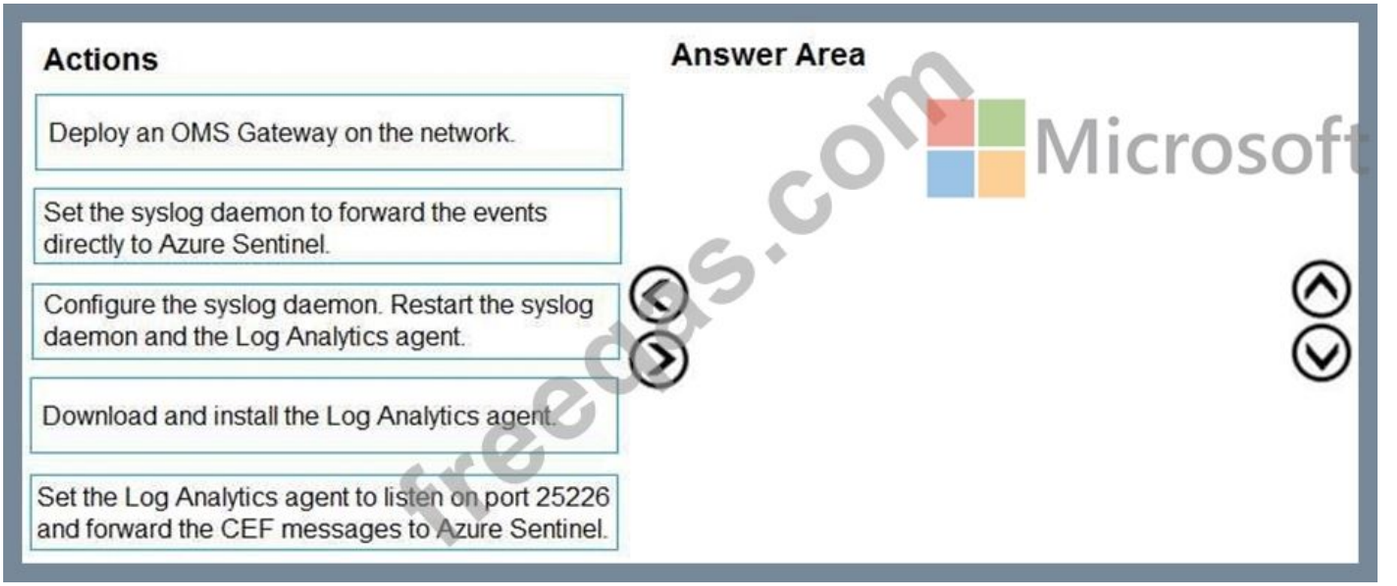
DRAG DROP

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

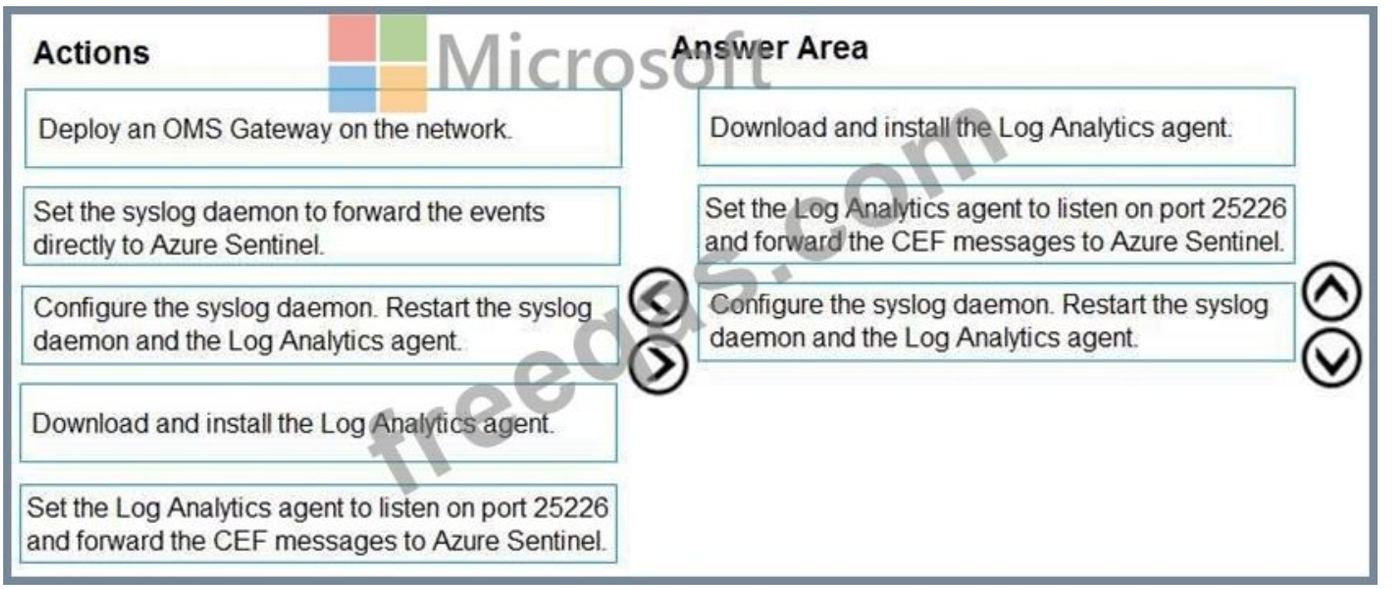
You need to deploy the log forwarder.

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

Select and Place:



Answer:



Section: [none]
Explanation/Reference:
https://docs.microsoft.com/en-us/azure/sentinel/connect-cef-agent?tabs=rsyslog

NEW QUESTION: 71
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 (LEAVE A REPLY)
Reference:
https://docs.microsoft.com/en-us/azure/security-center/security-center-managing-and-responding-alerts

NEW QUESTION: 72
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You are configuring Azure Sentinel.
You need to create an incident in Azure Sentinel when a sign-in to an Azure virtual machine from a malicious IP address is detected.
Solution: You create a Microsoft incident creation rule for a data connector.
Does this meet the goal?
A. Yes
B. No
Answer: A (LEAVE A REPLY)
Section: [none]
Explanation/Reference:
https://docs.microsoft.com/en-us/azure/sentinel/connect-azure-security-center

NEW QUESTION: 73
You have a custom analytics rule to detect threats in Azure Sentinel.
You discover that the analytics rule stopped running. The rule was disabled, and the rule name has a prefix of AUTO DISABLED.
What is a possible cause of the issue?
A. There are connectivity issues between the data sources and Log Analytics.
B. The number of alerts exceeded 10,000 within two minutes.
C. The rule query takes too long to run and times out.
D. Permissions to one of the data sources of the rule query were modified.
Answer: D (LEAVE A REPLY)
Explanation/Reference:
https://docs.microsoft.com/en-us/azure/sentinel/tutorial-detect-threats-custom

NEW QUESTION: 74
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: (SHOW ANSWER)

Explanation/Reference:

https://docs.microsoft.com/en-us/azure/security-center/security-center-managing-and-responding-alerts Mitigate threats using Azure Sentinel Testlet 1 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 company.

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

Existing Environment

Identity Environment

The network contains an Active Directory forest named litware.com that syncs to an Azure Active Directory (Azure AD) tenant named litware.com.

Microsoft 365 Environment

Litware has a Microsoft 365 E5 subscription linked to the litware.com Azure AD tenant. Microsoft Defender for Endpoint is deployed to all computers that run Windows 10. All Microsoft Cloud App Security built-in anomaly detection policies are enabled.

Azure Environment

Litware has an Azure subscription linked to the litware.com Azure AD tenant. The subscription contains resources in the East US Azure region as shown in the following table.

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

Network Environment

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

On-premises Environment

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

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

Planned Changes

Litware plans to implement the following changes:

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

Business Requirements

Litware identifies the following business requirements:

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

Microsoft Defender for Endpoint requirements

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

Microsoft Cloud App Security requirements

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

Azure Defender Requirements

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

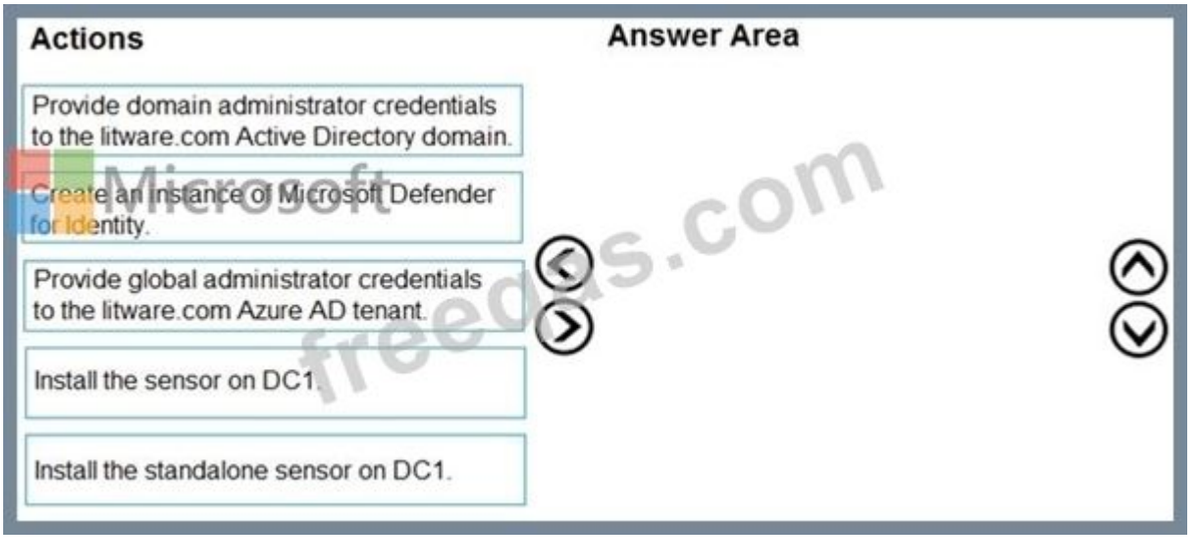
Azure Sentinel Requirements

Litware must meet the following Azure Sentinel requirements:

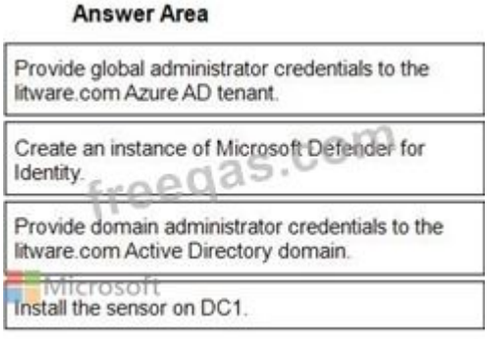
* Integrate Azure Sentinel and Cloud App Security.
* Ensure that a user named admin1 can configure Azure Sentinel playbooks.

* Create an Azure Sentinel analytics rule based on a custom query. The rule must automatically initiate the execution of a playbook.
* Add notes to events that represent data access from a specific IP address to provide the ability to reference the IP address when navigating through an investigation graph while hunting.
* Create a test rule that generates alerts when inbound access to Microsoft Office 365 by the Azure AD test user accounts is detected. Alerts generated by the rule must be grouped into individual incidents, with one incident per test user account.

NEW QUESTION: 75
You need to configure DC1 to meet the business requirements.
Which four actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.



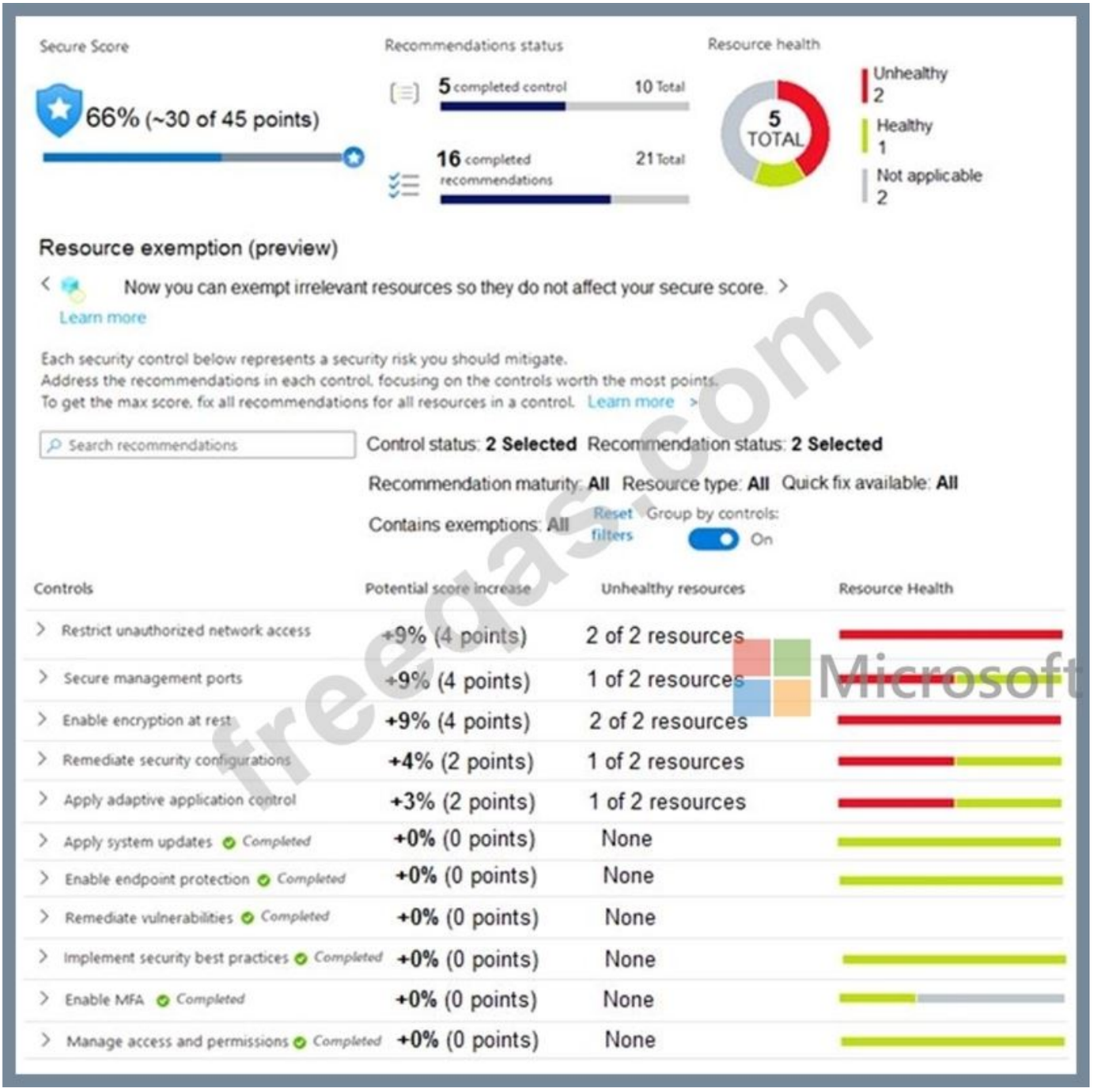
Answer:



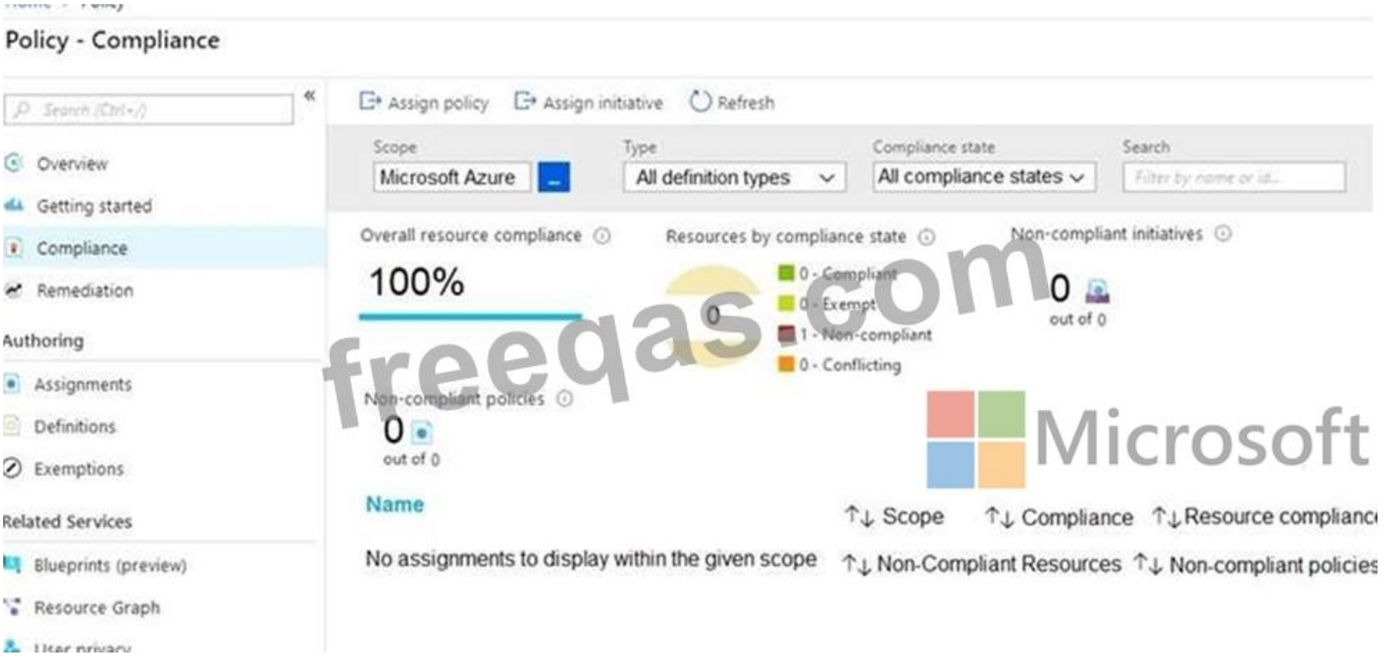
1 - Provide global administrator credentials to the litware.com Azure AD tenant.
2 - Create an instance of Microsoft Defender for Identity.
3 - Provide domain administrator credentials to the litware.com Active Directory domain.
4 - Install the sensor on DC1.
Explanation:
Step 1: log in to https://portal.atp.azure.com as a global admin
Step 2: Create the instance
Step 3. Connect the instance to Active Directory
Step 4. Download and install the sensor.

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

NEW QUESTION: 76
You manage the security posture of an Azure subscription that contains two virtual machines name vm1 and vm2.
The secure score in Azure Security Center is shown in the Security Center exhibit. (Click the Security Center tab.)



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



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

NOTE: Each correct selection is worth one point.

Answer Area

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

Answer:

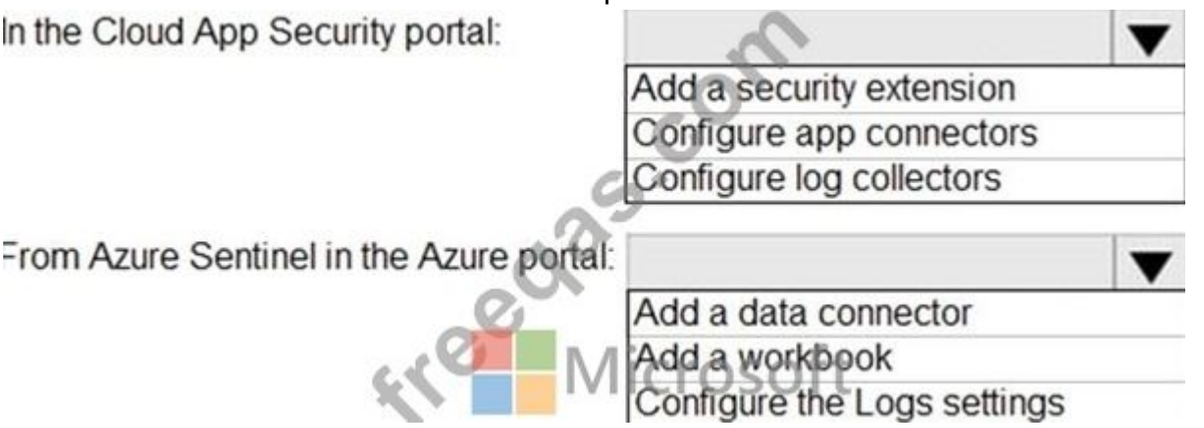
Answer Area

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

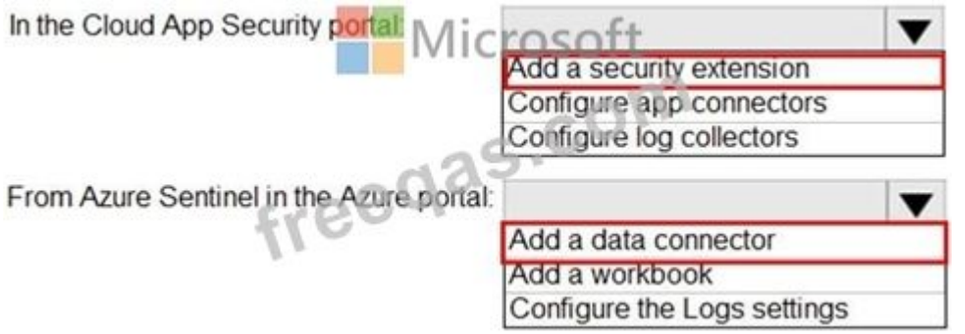
Reference:

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

NEW QUESTION: 77
You need to configure the Azure Sentinel integration to meet the Azure Sentinel requirements.
What should you do? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



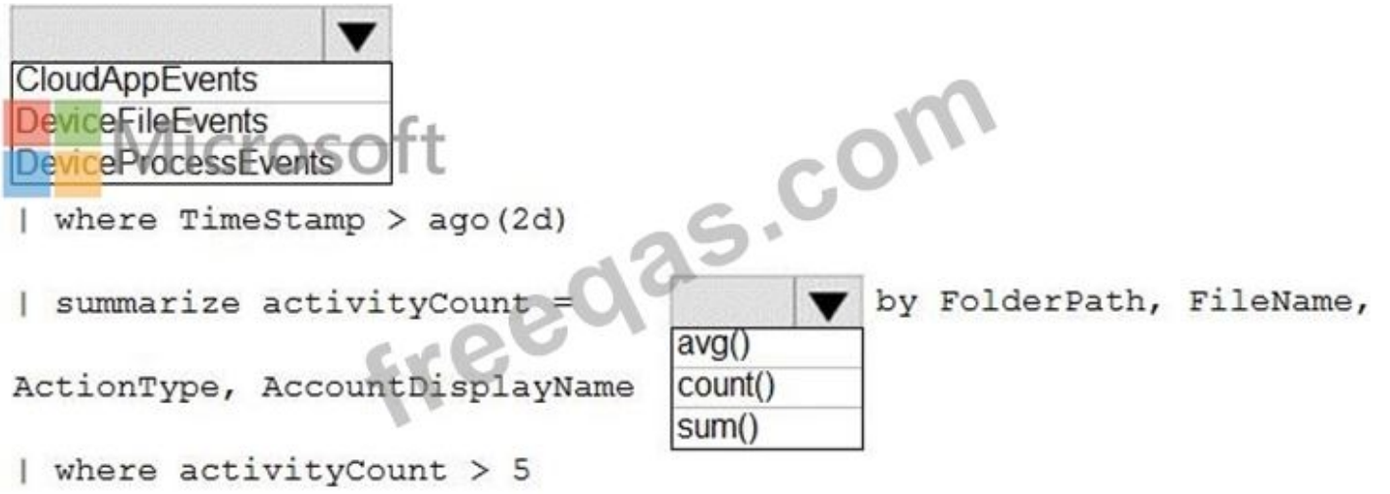
Answer:



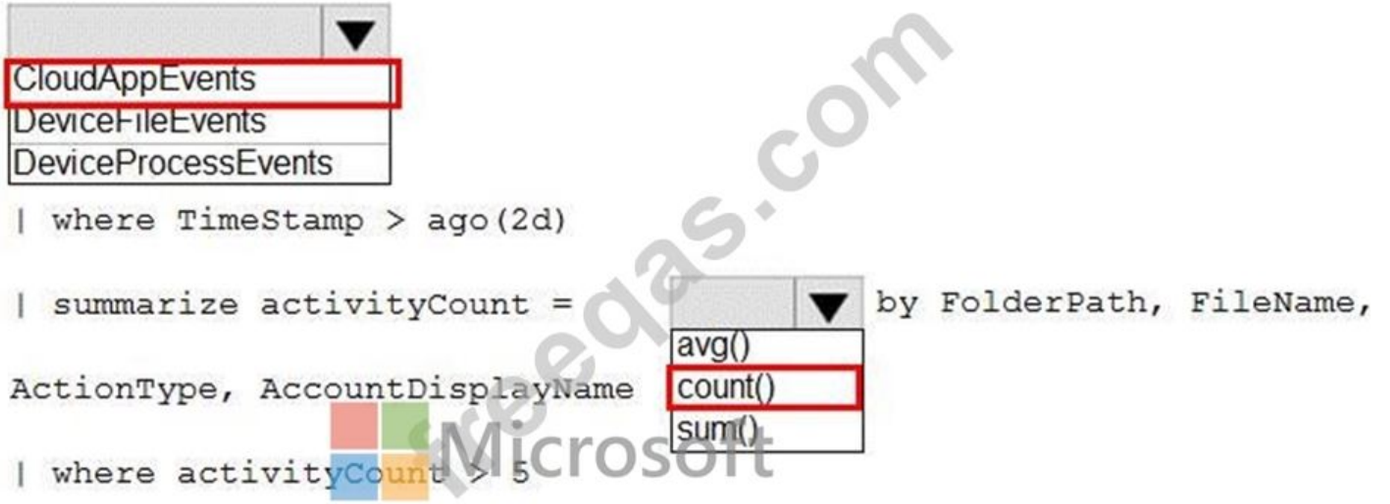
Reference:
https://docs.microsoft.com/en-us/cloud-app-security/siem-sentinel

NEW QUESTION: 78
You need to create an advanced hunting query to investigate the executive team issue.

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



Answer:



NEW QUESTION: 79
You are investigating an incident in Azure Sentinel that contains more than 127 alerts.
You discover eight alerts in the incident that require further investigation.
You need to escalate the alerts to another Azure Sentinel administrator.
What should you do to provide the alerts to the administrator?
A. Create a Microsoft incident creation rule
B. Share the incident URL
C. Create a scheduled query rule
D. Assign the incident
Answer: D (LEAVE A REPLY)
Reference:
https://docs.microsoft.com/en-us/azure/sentinel/investigate-cases

NEW QUESTION: 80

You need to implement the Azure Information Protection requirements.
What should you configure first?
A. Device health and compliance reports settings in Microsoft Defender Security Center
B. scanner clusters in Azure Information Protection from the Azure portal
C. content scan jobs in Azure Information Protection from the Azure portal
D. Advanced features from Settings in Microsoft Defender Security Center
Answer: D (LEAVE A REPLY)
Explanation/Reference:
https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/information- protection-in-windows-overview

NEW QUESTION: 81
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: (SHOW ANSWER)
Section: [none]
Explanation/Reference:
https://docs.microsoft.com/en-us/defender-for-identity/manage-sensitive-honeytoken-accounts

NEW QUESTION: 82
You have the following environment:
Azure Sentinel
A Microsoft 365 subscription
Microsoft Defender for Identity
An Azure Active Directory (Azure AD) tenant
You configure Azure Sentinel to collect security logs from all the Active Directory member servers and domain controllers.
You deploy Microsoft Defender for Identity by using standalone sensors.
You need to ensure that you can detect when sensitive groups are modified in Active Directory.
Which two actions should you perform? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.
A. Configure the Advanced Audit Policy Configuration settings for the domain controllers.
B. Modify the permissions of the Domain Controllers organizational unit (OU).
C. Configure auditing in the Microsoft 365 compliance center.
D. Configure Windows Event Forwarding on the domain controllers.
Answer: A,D (LEAVE A REPLY)
Reference:
https://docs.microsoft.com/en-us/defender-for-identity/configure-windows-event-collection
https://docs.microsoft.com/en-us/defender-for-identity/configure-event-collection

NEW QUESTION: 83
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 (LEAVE A REPLY)
Reference:
https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/safe-attachments?view=o365-worldwide

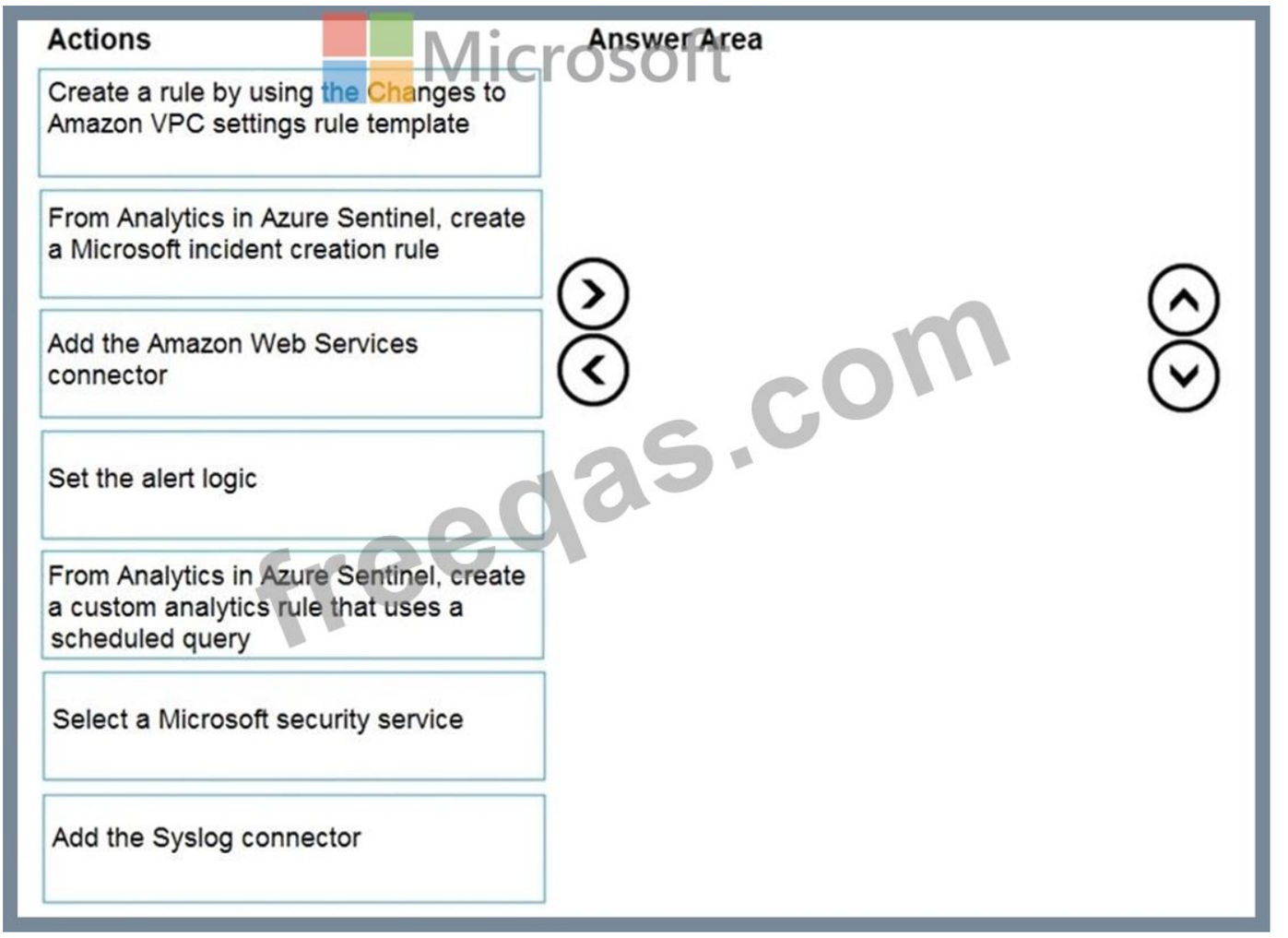
NEW QUESTION: 84
You need to configure Microsoft Cloud App Security to generate alerts and trigger remediation actions in response to external sharing of confidential files.
Which two actions should you perform in the Cloud App Security portal? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.
A. From Settings, select Information Protection, select Azure Information Protection, and then select Only scan files for Azure Information Protection classification labels and content inspection warnings from this tenant
B. Select Investigate files, and then filter App to Office 365.
C. Select Investigate files, and then select New policy from search
D. From Settings, select Information Protection, select Azure Information Protection, and then select Automatically scan new files for Azure Information Protection classification labels and content inspection warnings

E. From Settings, select Information Protection, select Files, and then enable file monitoring.
F. Select Investigate files, and then filter File Type to Document.
Answer: D,E (LEAVE A REPLY)
Reference:
https://docs.microsoft.com/en-us/cloud-app-security/tutorial-dlp
https://docs.microsoft.com/en-us/cloud-app-security/azip-integration

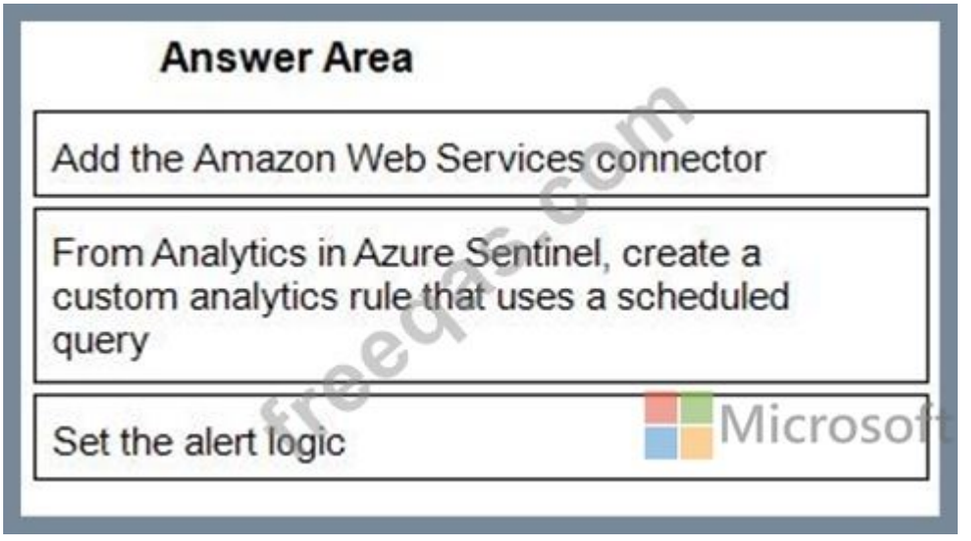
NEW QUESTION: 85
You have an Azure subscription that contains a virtual machine named VM1 and uses Azure Defender. Azure Defender has automatic provisioning enabled.
You need to create a custom alert suppression rule that will supress false positive alerts for suspicious use of PowerShell on VM1.
What should you do first?
A. From Azure Security Center, add a workflow automation.
B. On VM1, run the Get-MPThreatCatalog cmdlet.
C. On VM1 trigger a PowerShell alert.
D. From Azure Security Center, export the alerts to a Log Analytics workspace.
Answer: C (LEAVE A REPLY)
Reference:
https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/manage-alerts?view=o365-worldwide

NEW QUESTION: 86
You plan to create a custom Azure Sentinel query that will provide a visual representation of the security alerts generated by Azure Security Center.
You need to create a query that will be used to display a bar graph. What should you include in the query?
A. bin
B. workspace
C. extend
D. count
Answer: D (LEAVE A REPLY)

NEW QUESTION: 87
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:



1 - Add the Amazon Web Services connector

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

3 - Set the alert logic

Reference:

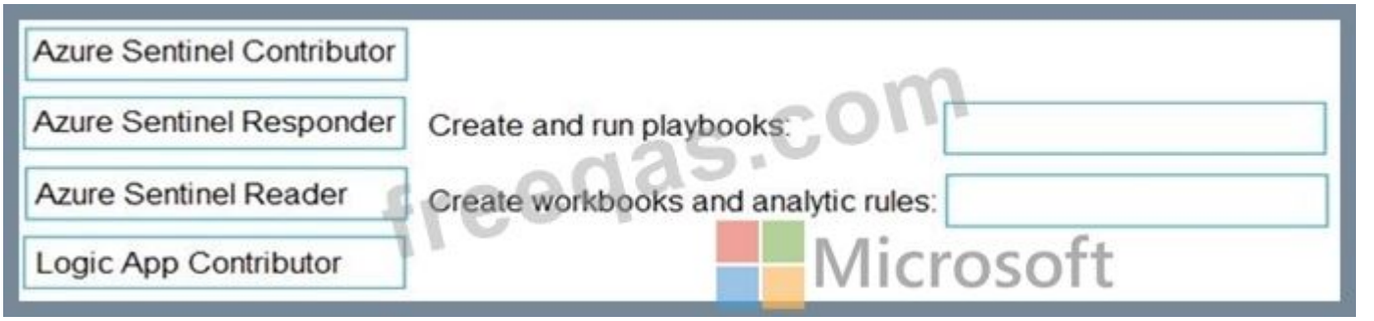
https://docs.microsoft.com/en-us/azure/sentinel/detect-threats-custom

Topic 2, Contoso Ltd

Existing Environment

End-User Environment
All users at Contoso use Windows 10 devices. Each user is licensed for Microsoft 365. In addition, iOS devices are distributed to the members of the sales team at Contoso.
Cloud and Hybrid Infrastructure
All Contoso applications are deployed to Azure.
You enable Microsoft Cloud App Security.
Contoso and Fabrikam have different Azure Active Directory (Azure AD) tenants. Fabrikam recently purchased an Azure subscription and enabled Azure Defender for all supported resource types.
Current Problems
The security team at Contoso receives a large number of cybersecurity alerts. The security team spends too much time identifying which cybersecurity alerts are legitimate threats, and which are not.
The Contoso sales team uses only iOS devices. The sales team members exchange files with customers by using a variety of third-party tools. In the past, the sales team experienced various attacks on their devices.
The marketing team at Contoso has several Microsoft SharePoint Online sites for collaborating with external vendors. The marketing team has had several incidents in which vendors uploaded files that contain malware.
The executive team at Contoso suspects a security breach. The executive team requests that you identify which files had more than five activities during the past 48 hours, including data access, download, or deletion for Microsoft Cloud App Security-protected applications.
Requirements
Planned Changes
Contoso plans to integrate the security operations of both companies and manage all security operations centrally.
Technical Requirements
Contoso identifies the following technical requirements:
Receive alerts if an Azure virtual machine is under brute force attack.
Use Azure Sentinel to reduce organizational risk by rapidly remediating active attacks on the environment.
Implement Azure Sentinel queries that correlate data across the Azure AD tenants of Contoso and Fabrikam.
Develop a procedure to remediate Azure Defender for Key Vault alerts for Fabrikam in case of external attackers and a potential compromise of its own Azure AD applications.
Identify all cases of users who failed to sign in to an Azure resource for the first time from a given country. A junior security administrator provides you with the following incomplete query.
BehaviorAnalytics
| where ActivityType == "FailedLogOn"
| where _____ == True

NEW QUESTION: 88
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.



Answer:

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

NEW QUESTION: 89
You have a playbook in Azure Sentinel.
When you trigger the playbook, it sends an email to a distribution group.
You need to modify the playbook to send the email to the owner of the resource instead of the distribution group.
What should you do?
A. Add a parameter and modify the trigger.
B. Add a custom data connector and modify the trigger.
C. Add a condition and modify the action.
D. Add a parameter and modify the action.
Answer: D (LEAVE A REPLY)
Section: [none]
Explanation/Reference:

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

NEW QUESTION: 90

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.

Answer:

1 - Configure 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.

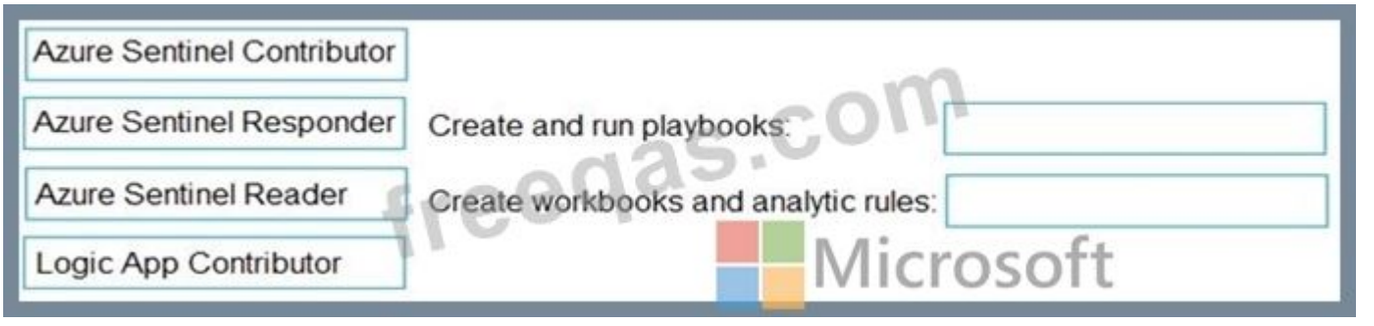
5 - From Azure Security Center, add cloud connectors.
Reference:
https://docs.microsoft.com/en-us/azure/security-center/quickstart-onboard-gcp

NEW QUESTION: 91
You need to remediate active attacks to meet the technical requirements.
What should you include in the solution?
A. Azure Automation runbooks
B. Azure Logic Apps
C. Azure Functions
D. Azure Sentinel livestreams
Answer: (SHOW ANSWER)
Reference:
https://docs.microsoft.com/en-us/azure/sentinel/automate-responses-with-playbooks

NEW QUESTION: 92
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 (LEAVE A REPLY)
Reference:
https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/safe-attachments?view=o365-world

NEW QUESTION: 93
You recently deployed Azure Sentinel.
You discover that the default Fusion rule does not generate any alerts. You verify that the rule is enabled.
You need to ensure that the Fusion rule can generate alerts.
What should you do?
A. Disable, and then enable the rule.
B. Add data connectors
C. Create a new machine learning analytics rule.
D. Add a hunting bookmark.
Answer: (SHOW ANSWER)
Section: [none]
Explanation/Reference:
https://docs.microsoft.com/en-us/azure/sentinel/connect-data-sources

NEW QUESTION: 94
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.



Answer:

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

NEW QUESTION: 95

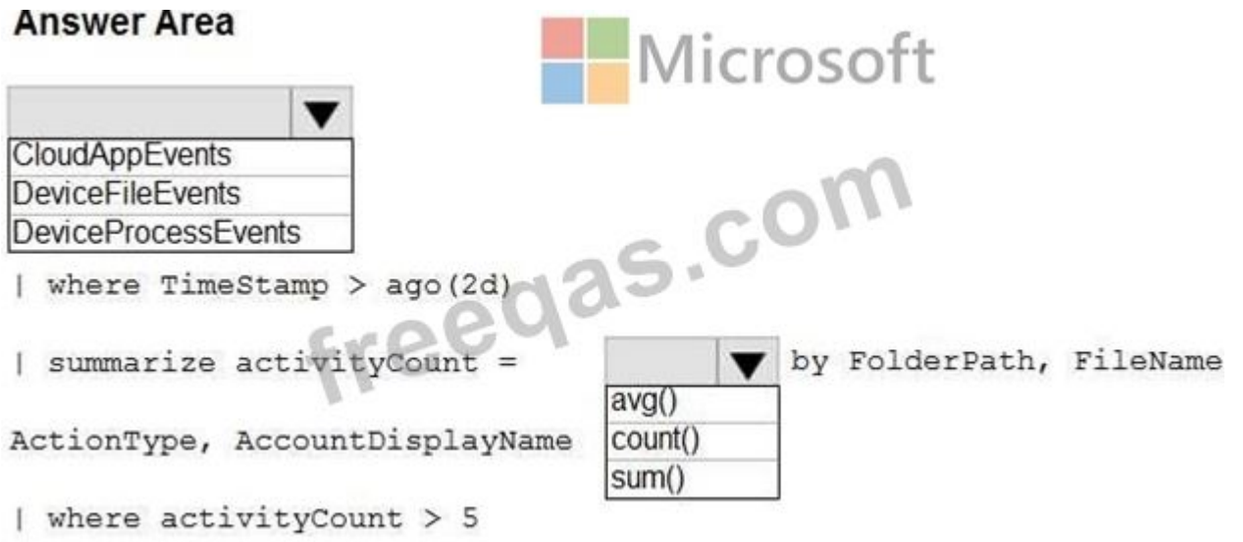
HOTSPOT

You need to create an advanced hunting query to investigate the executive team issue.

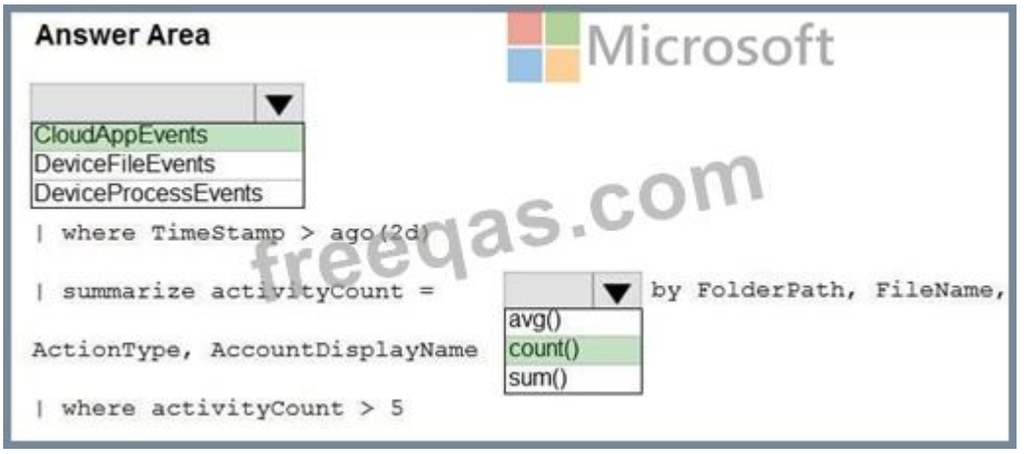
How should you complete the query? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:



Answer:



Section: [none]

Explanation/Reference:

Testlet 2

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 company.
Litware has offices in Boston and Seattle. Litware also has remote users located across the United States. To access Litware resources, including cloud resources, the remote users establish a VPN connection to either office.
Existing Environment
Identity Environment
The network contains an Active Directory forest named litware.com that syncs to an Azure Active Directory (Azure AD) tenant named litware.com.
Microsoft 365 Environment
Litware has a Microsoft 365 E5 subscription linked to the litware.com Azure AD tenant. Microsoft Defender for Endpoint is deployed to all computers that run Windows 10. All Microsoft Cloud App Security built-in anomaly detection policies are enabled.
Azure Environment
Litware has an Azure subscription linked to the litware.com Azure AD tenant. The subscription contains resources in the East US Azure region as shown in the following table.

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

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

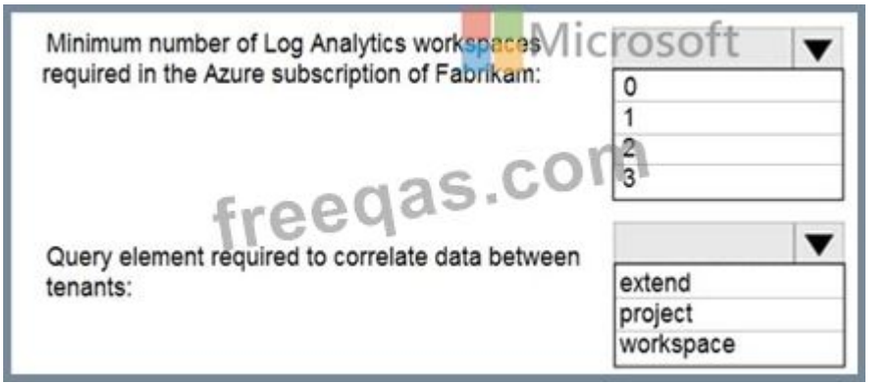
Current problems
Cloud App Security frequently generates false positive alerts when users connect to both offices simultaneously.
Planned Changes
Litware plans to implement the following changes:
* Create and configure Azure Sentinel in the Azure subscription.
* Validate Azure Sentinel functionality by using Azure AD test user accounts.
Business Requirements
Litware identifies the following business requirements:
* 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 security labels and are stored on the Windows 10 computers must be available from the Azure Information Protection - Data discovery dashboard.
Microsoft Defender for Endpoint requirements
All Cloud App Security unsanctioned apps must be blocked on the Windows 10 computers by using Microsoft Defender for Endpoint.
Microsoft Cloud App Security requirements
Cloud App Security must identify whether a user connection is anomalous based on tenant-level data.
Azure Defender Requirements
All servers must send logs to the same Log Analytics workspace.
Azure Sentinel Requirements
Litware must meet the following Azure Sentinel requirements:
* Integrate Azure Sentinel and Cloud App Security.
* Ensure that a user named admin1 can configure Azure Sentinel playbooks.
* Create an Azure Sentinel analytics rule based on a custom query. The rule must automatically initiate the execution of a playbook.
* Add notes to events that represent data access from a specific IP address to provide the ability to reference the IP address when navigating through an investigation graph while hunting.
* Create a test rule that generates alerts when inbound access to Microsoft Office 365 by the Azure AD test user accounts is detected. Alerts generated by the rule must be grouped into individual incidents, with one incident per test user account.

NEW QUESTION: 96
You need to modify the anomaly detection policy settings to meet the Cloud App Security requirements. Which policy should you modify?
A. Activity from suspicious IP addresses
B. Activity from anonymous IP addresses

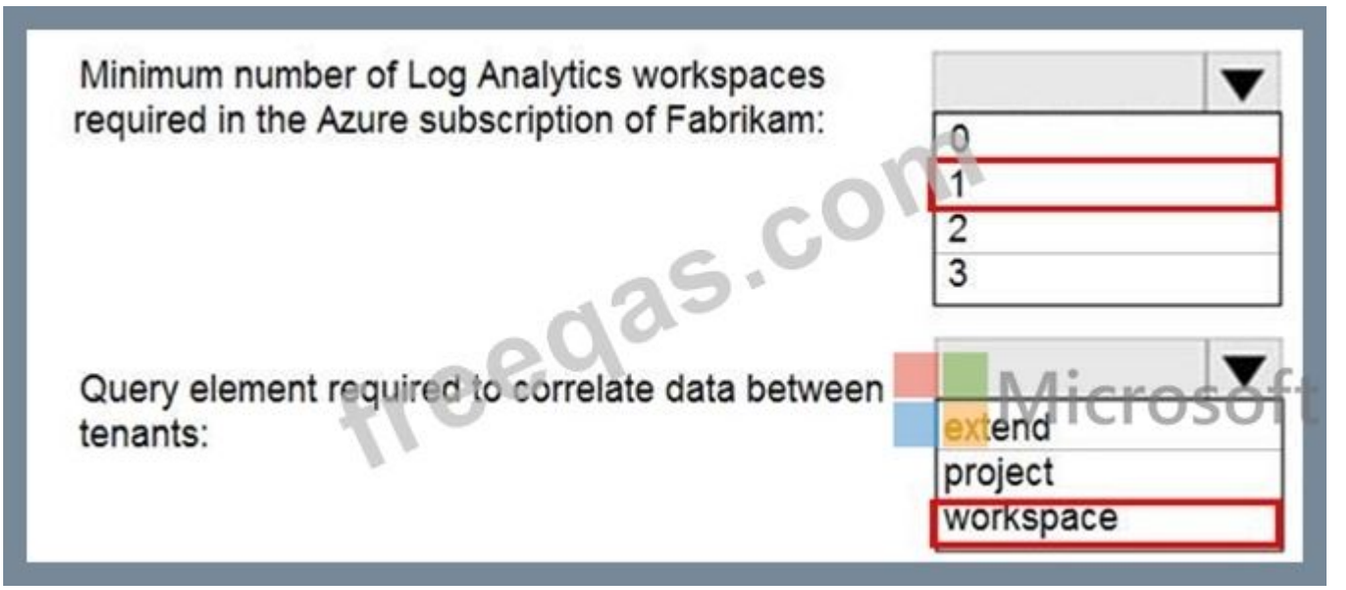
C. Impossible travel
D. Risky sign-in
Answer: (SHOW ANSWER)
Reference:
https://docs.microsoft.com/en-us/cloud-app-security/anomaly-detection-policy

NEW QUESTION: 97
A security administrator receives email alerts from Azure Defender for activities such as potential malware uploaded to a storage account and potential successful brute force attacks.
The security administrator does NOT receive email alerts for activities such as antimalware action failed and suspicious network activity. The alerts appear in Azure Security Center.
You need to ensure that the security administrator receives email alerts for all the activities.
What should you configure in the Security Center settings?
A. the severity level of email notifications
B. a cloud connector
C. the Azure Defender plans
D. the integration settings for Threat detection
Answer: (SHOW ANSWER)
Reference:
https://techcommunity.microsoft.com/t5/microsoft-365-defender/get-email-notifications-on-new-incidents-from-microsoft-365/ba-p/2012518

NEW QUESTION: 98
You need to implement Azure Sentinel queries for Contoso and Fabrikam to meet the technical requirements.
What should you include in the solution? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



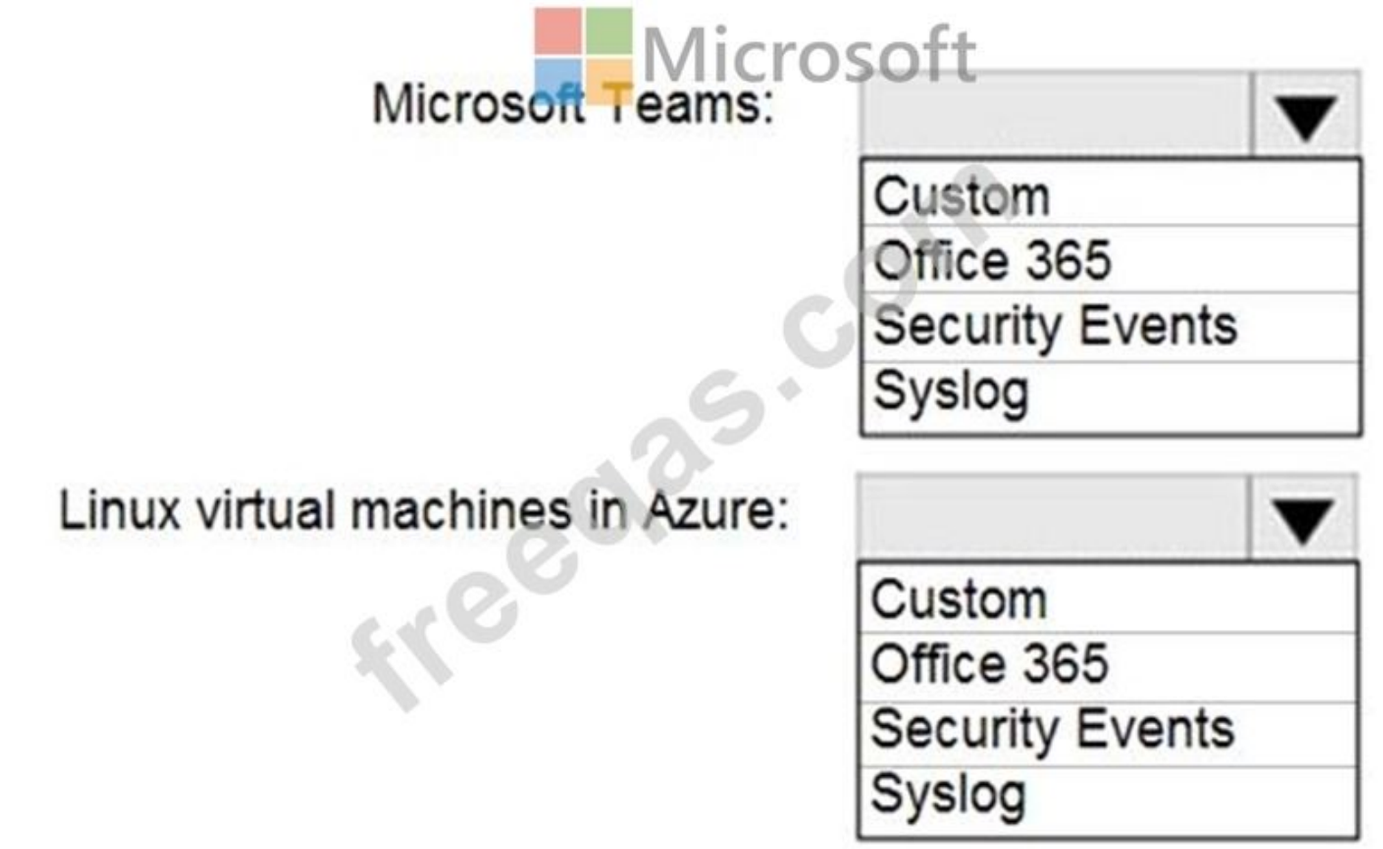
Answer:



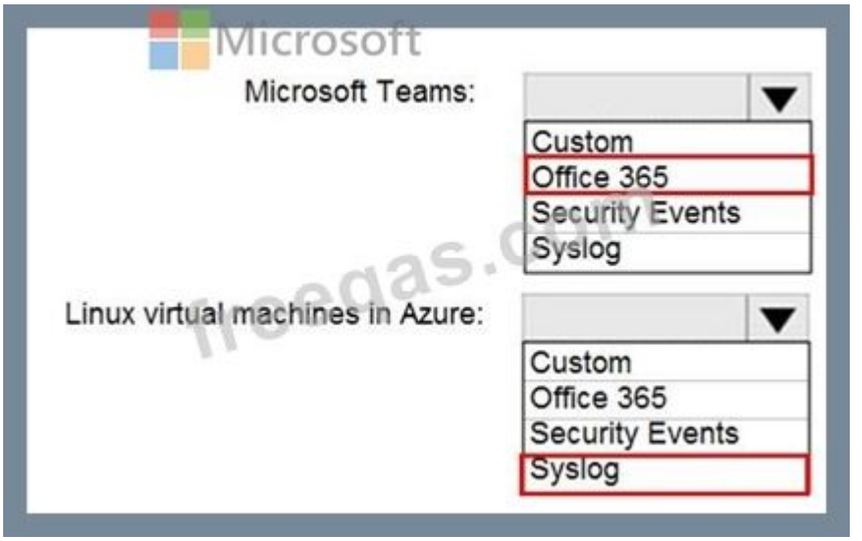
Reference:
https://docs.microsoft.com/en-us/azure/sentinel/extend-sentinel-across-workspaces-tenants

NEW QUESTION: 99
You need to implement the Azure Information Protection requirements. What should you configure first?
A. Device health and compliance reports settings in Microsoft Defender Security Center
B. scanner clusters in Azure Information Protection from the Azure portal
C. content scan jobs in Azure Information Protection from the Azure portal
D. Advanced features from Settings in Microsoft Defender Security Center
Answer: D (LEAVE A REPLY)
Explanation
https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/information- protection-in-windows-overview

NEW QUESTION: 100
You deploy Azure Sentinel.
You need to implement connectors in Azure Sentinel to monitor Microsoft Teams and Linux virtual machines in Azure. The solution must minimize administrative effort.
Which data connector type should you use for each workload? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



Answer:

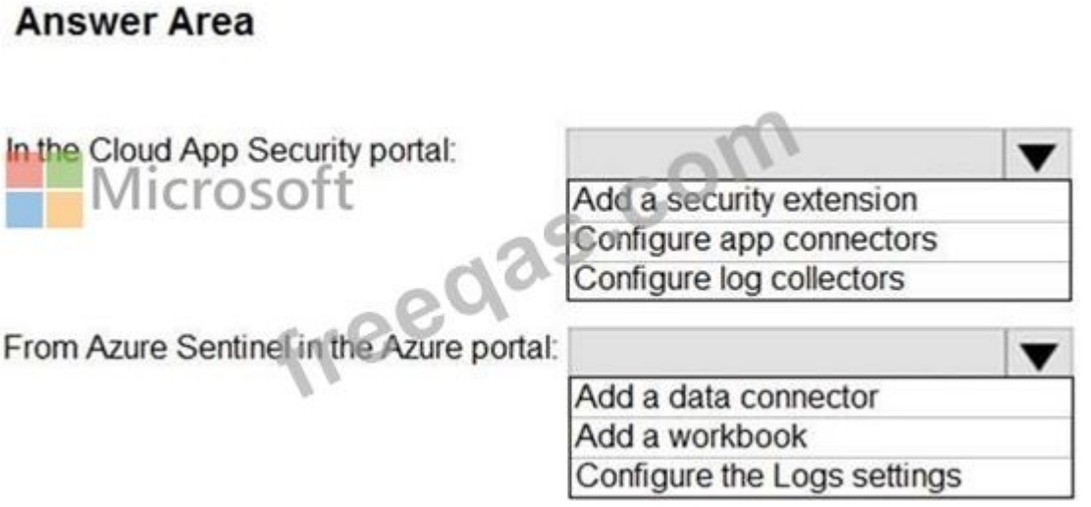


Reference:
https://docs.microsoft.com/en-us/azure/sentinel/connect-office-365
https://docs.microsoft.com/en-us/azure/sentinel/connect-syslog

NEW QUESTION: 101
You create a hunting query in Azure Sentinel.
You need to receive a notification in the Azure portal as soon as the hunting query detects a match on the query. The solution must minimize effort.
What should you use?
A. a playbook

B. a notebook
C. a livestream
D. a bookmark
Answer: C (LEAVE A REPLY)
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: 102
HOTSPOT
You need to configure the Azure Sentinel integration to meet the Azure Sentinel requirements.
What should you do? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.
Hot Area:



Answer:

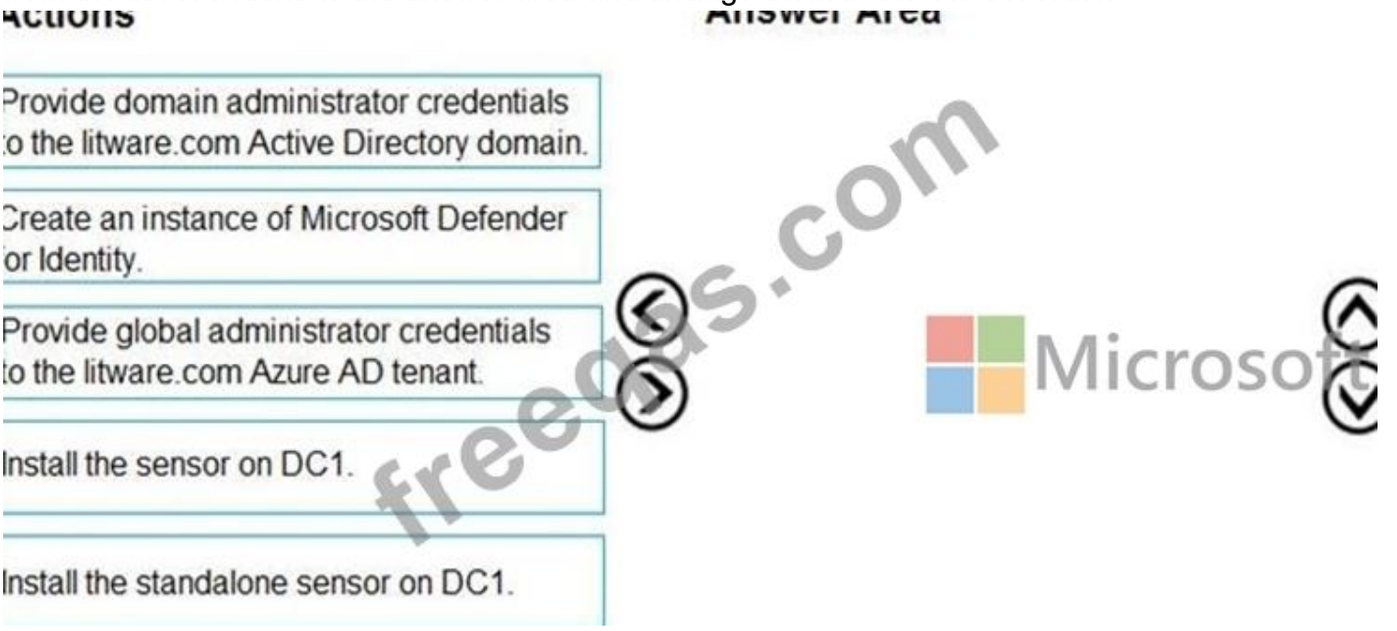
Section: [none]
Explanation/Reference:

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

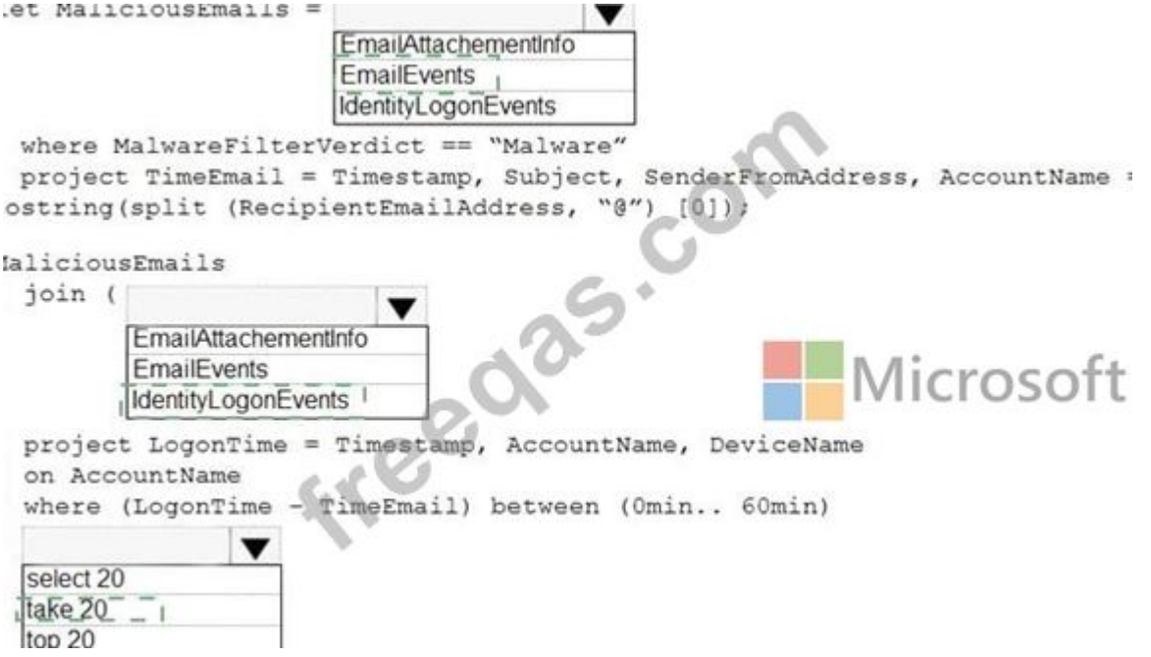
NEW QUESTION: 103

You need to configure DC1 to meet the business requirements.

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

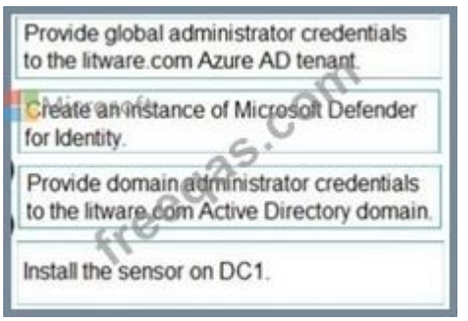


Answer:



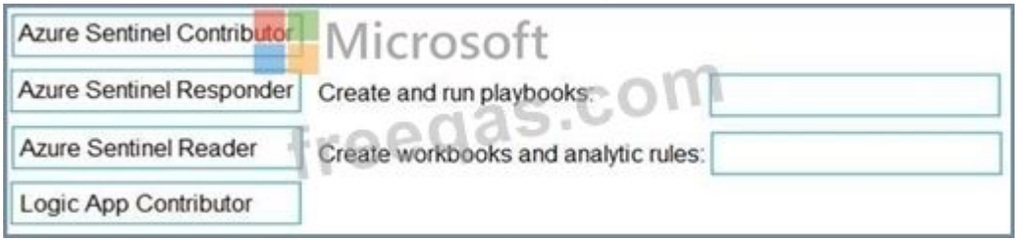
Explanation

Text Description automatically generated with medium confidence

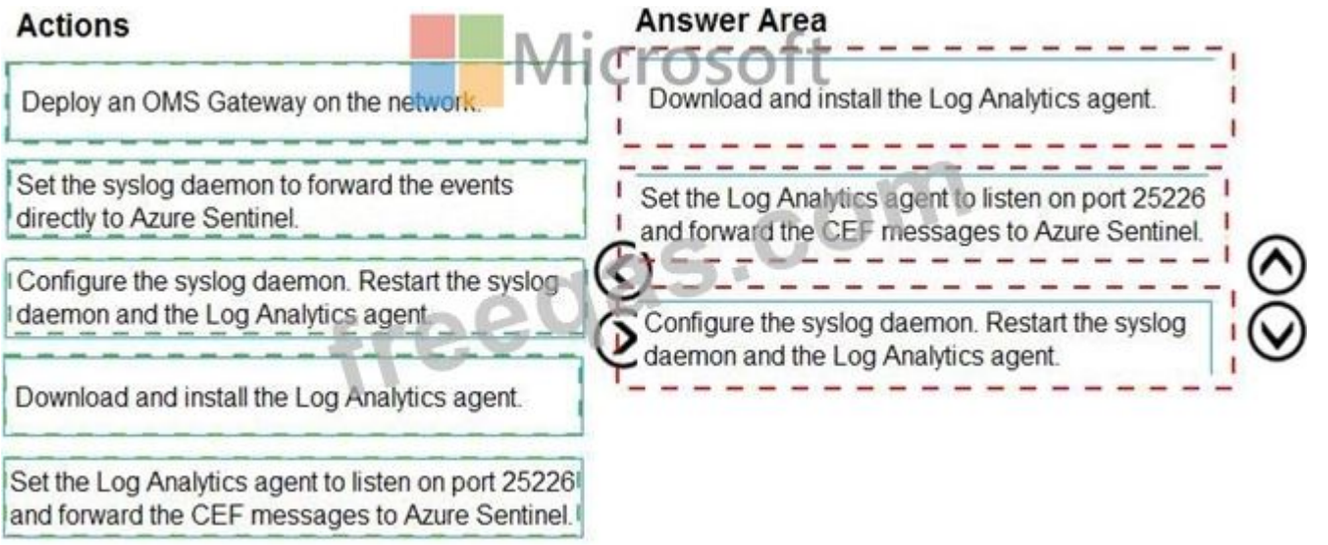


Step 1: log in to https://portal.atp.azure.com as a global admin
Step 2: Create the instance
Step 3. Connect the instance to Active Directory
Step 4. Download and install the sensor.
Reference:
https://docs.microsoft.com/en-us/defender-for-identity/install-step1
https://docs.microsoft.com/en-us/defender-for-identity/install-step4

NEW QUESTION: 104
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.



Answer:



Explanation

A picture containing graphical user interface Description automatically generated

Reference:

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

NEW QUESTION: 105

You are responsible for responding to Azure Defender for Key Vault alerts.

During an investigation of an alert, you discover unauthorized attempts to access a key vault from a Tor exit node.

What should you configure to mitigate the threat?

A. Key Vault firewalls and virtual networks

B. Azure Active Directory (Azure AD) permissions

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

D. the access policy settings of the key vault

Answer: A (LEAVE A REPLY)

Section: [none]

Explanation/Reference:

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

NEW QUESTION: 106

You use Azure Sentinel to monitor irregular Azure activity.

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

Home > Azure Sentinel workspaces > Azure Sentinel

Analytics rule wizard – Edit existing rule

DeployVM

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

Define the logic for your new analytics rule.

Rule query

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

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

View query results >

Map entities

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

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

Query scheduling

Run query every *

5 | Minutes

Lookup data from the last *

5 | Hours

Alert threshold

Generate alert when number of query results *

Is greater than | 2

Event grouping

Configure how rule query results are grouped into alerts

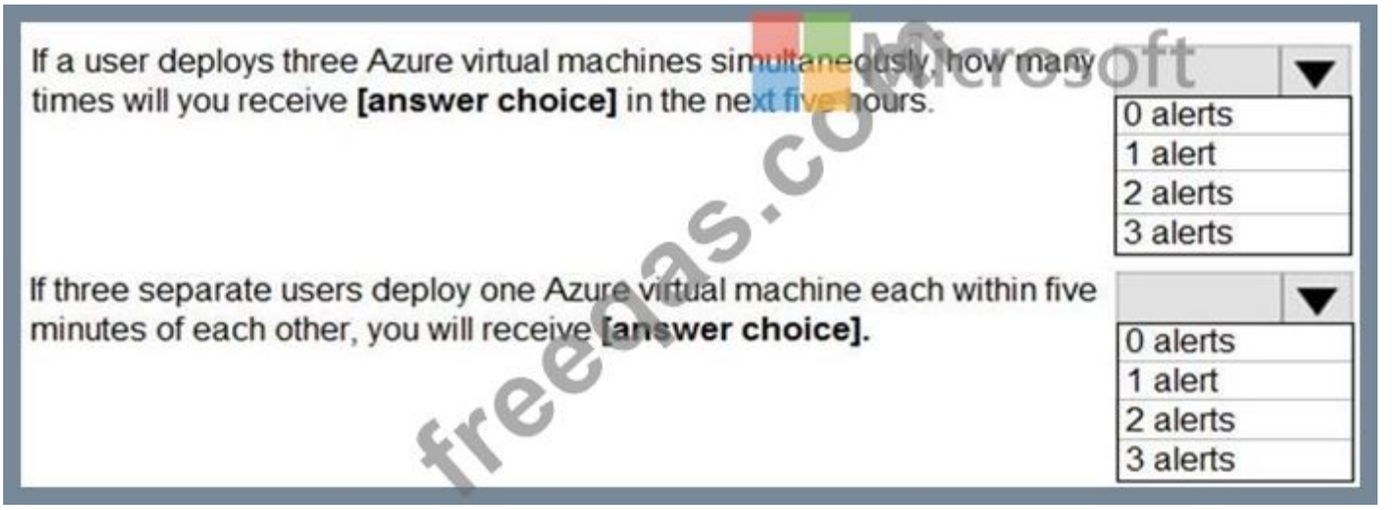
- (•) Group all events into a single alert
- ( ) Trigger an alert for each event

Suppression

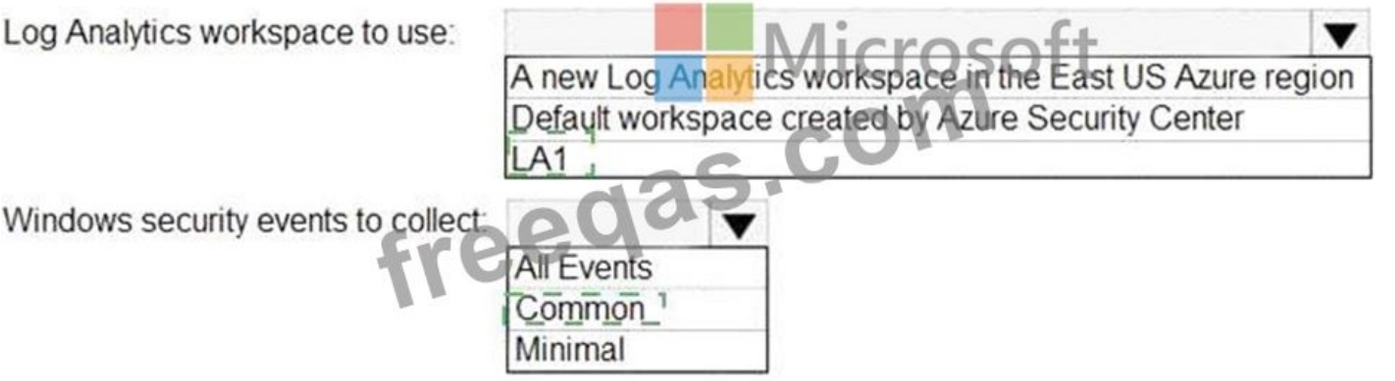
You do NOT define any incident settings as part of the rule definition.

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

NOTE: Each correct selection is worth one point.

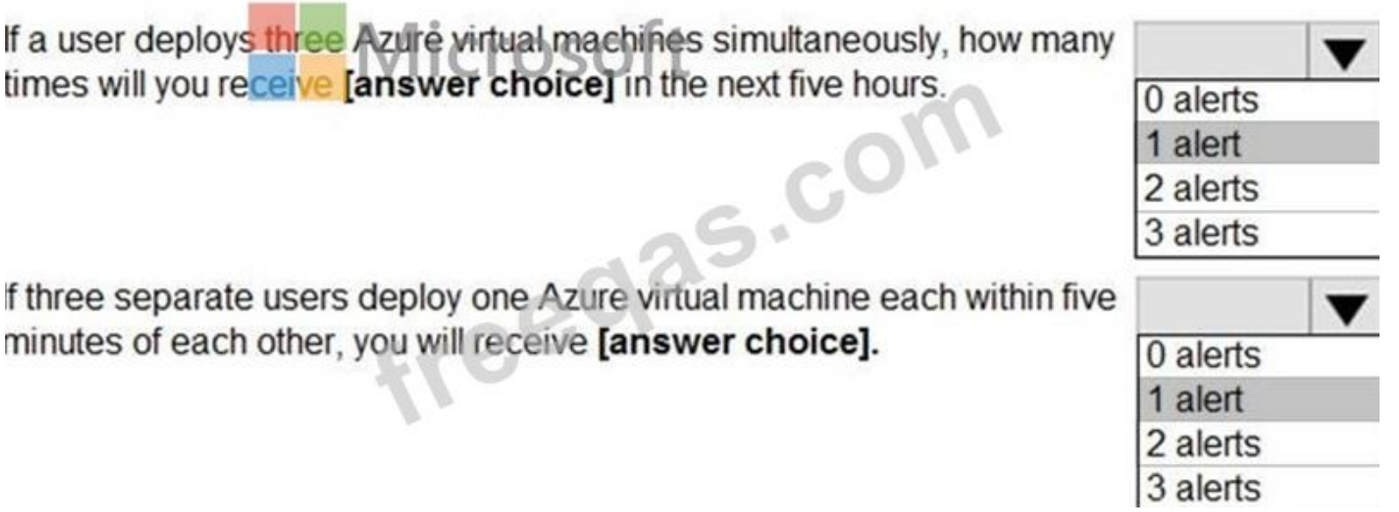


Answer:



Explanation

Graphical user interface, text, application, email Description automatically generated



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

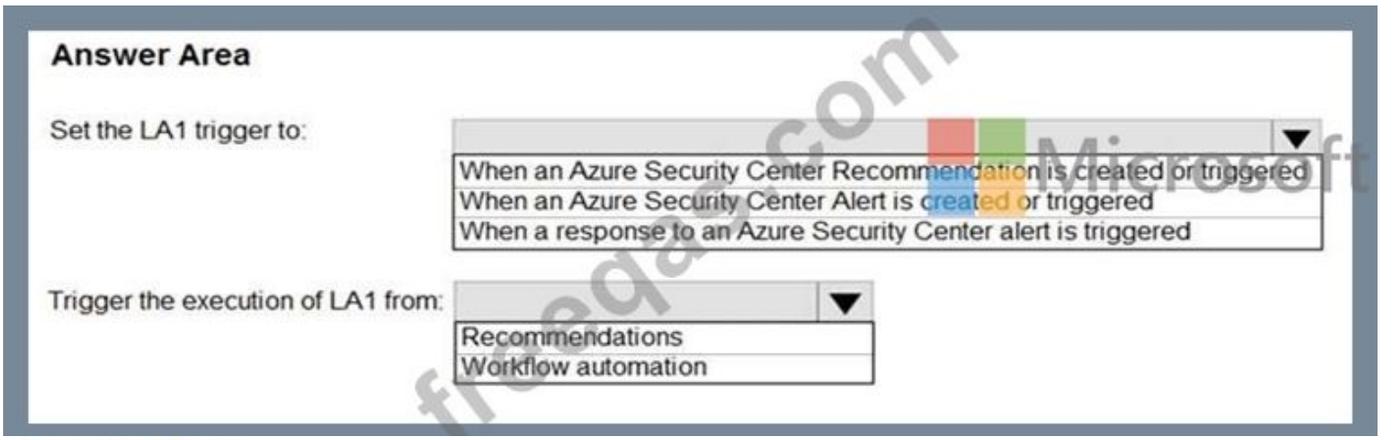
NEW QUESTION: 107
You need to implement the Azure Information Protection requirements. What should you configure first?
A. Device health and compliance reports settings in Microsoft Defender Security Center
B. scanner clusters in Azure Information Protection from the Azure portal
C. content scan jobs in Azure Information Protection from the Azure portal
D. Advanced features from Settings in Microsoft Defender Security Center
Answer: D (LEAVE A REPLY)
https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/information- protection-in-windows-overview

NEW QUESTION: 108
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 (LEAVE A REPLY)
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: 109
You need to create the test rule to meet the Azure Sentinel requirements.
What should you do when you create the rule?
A. From Set rule logic, turn off suppression.
B. From Analytics rule details, configure the tactics.
C. From Set rule logic, map the entities.
D. From Analytics rule details, configure the severity.
Answer: C (LEAVE A REPLY)
Section: [none]
Explanation/Reference:
https://docs.microsoft.com/en-us/azure/sentinel/tutorial-detect-threats-custom

NEW QUESTION: 110
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:

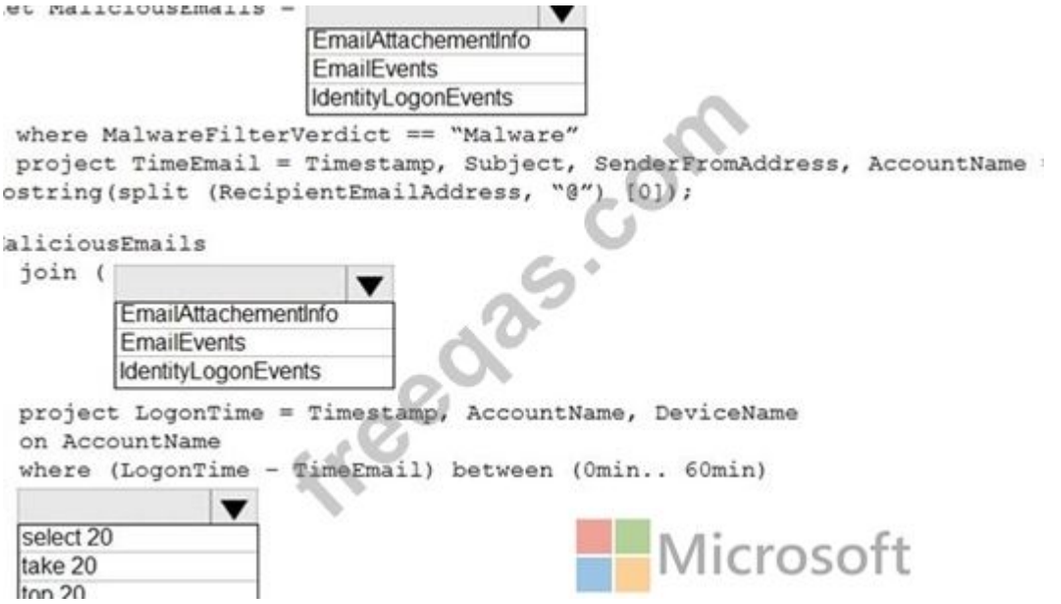
When an Azure Security Center Recommendation is created or triggered
When an Azure Security Center Alert is created or triggered
When a response to an Azure Security Center alert is triggered

Trigger the execution of LA1 from:

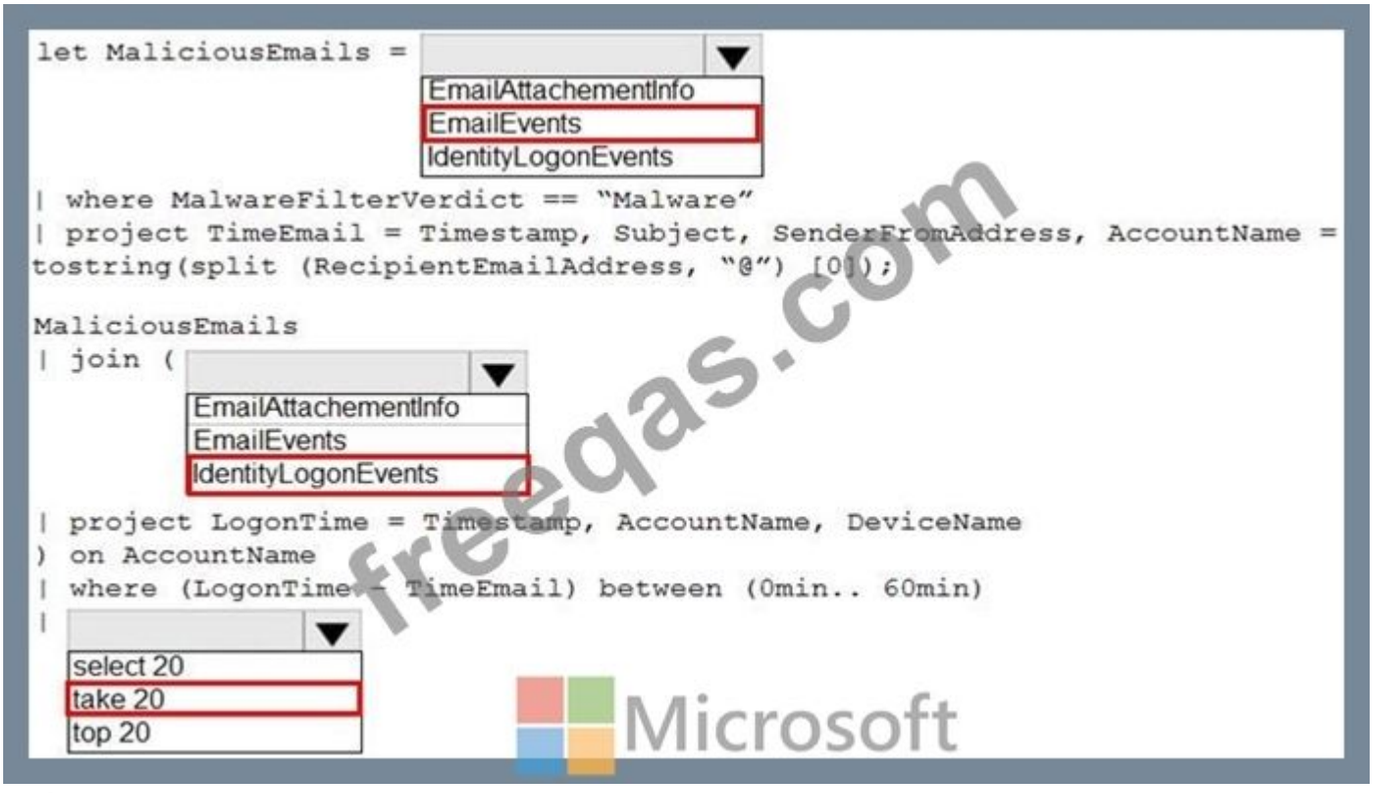
Recommendations
Workflow automation

Section: [none]
Explanation/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: 111
You are informed of an increase in malicious email being received by users.
You need to create an advanced hunting query in Microsoft 365 Defender to identify whether the accounts of the email recipients were compromised. The query must return the most recent 20 sign-ins performed by the recipients within an hour of receiving the known malicious email.
How should you complete the query? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



Answer:



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

NEW QUESTION: 112

You use Azure Sentinel.

You need to receive an immediate alert whenever Azure Storage account keys are enumerated.

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

NOTE: Each correct selection is worth one point.

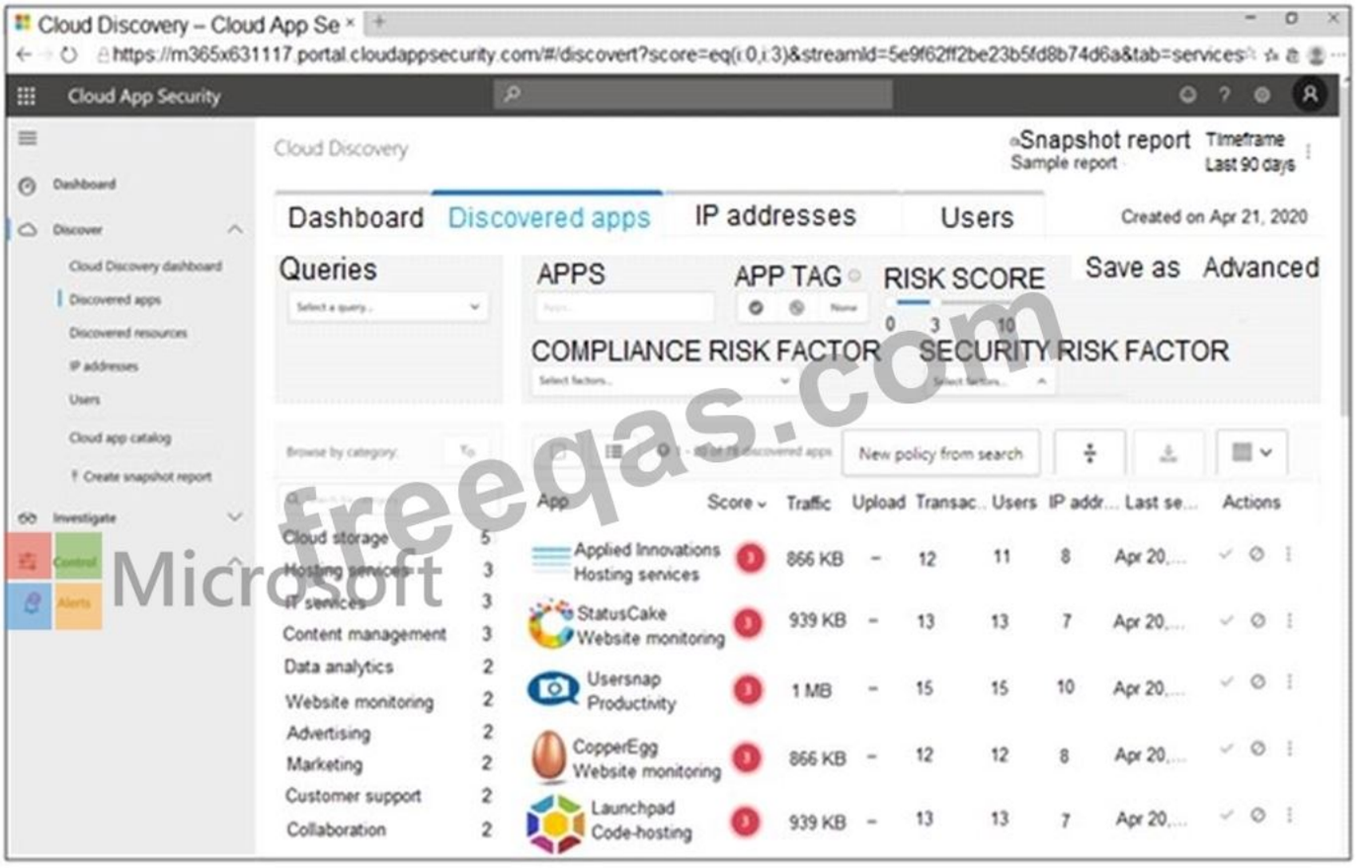
A. Create a livestream

B. Add a data connector

C. Create an analytics rule
D. Create a hunting query.
E. Create a bookmark.
Answer: B,D (LEAVE A REPLY)
Reference:
https://docs.microsoft.com/en-us/azure/sentinel/livestream

NEW QUESTION: 113
Your company uses Azure Security Center and Azure Defender.
The security operations team at the company informs you that it does NOT receive email notifications for security alerts.
What should you configure in Security Center to enable the email notifications?
A. Security solutions
B. Security policy
C. Pricing & settings
D. Security alerts
E. Azure Defender
Answer: C (LEAVE A REPLY)
Section: [none]
Explanation/Reference:
https://docs.microsoft.com/en-us/azure/security-center/security-center-provide-security-contact-details

NEW QUESTION: 114
You open the Cloud App Security portal as shown in the following exhibit.



You need to remediate the risk for the Launchpad app.

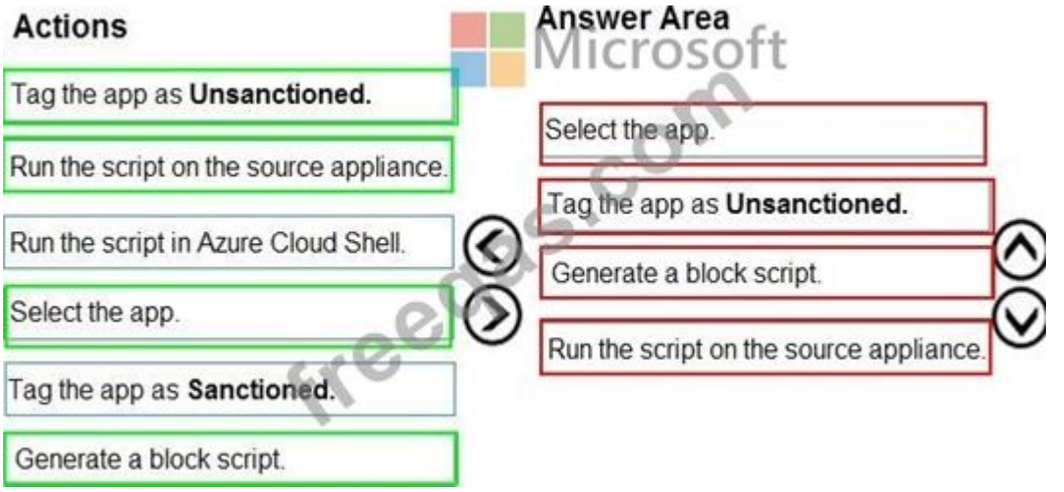
Which four actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

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

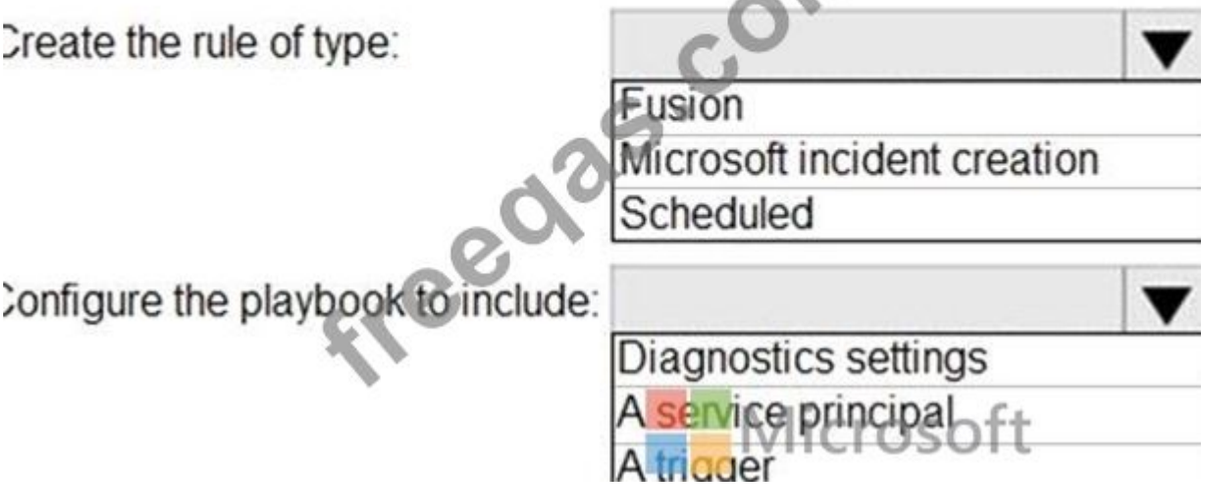
Answer:



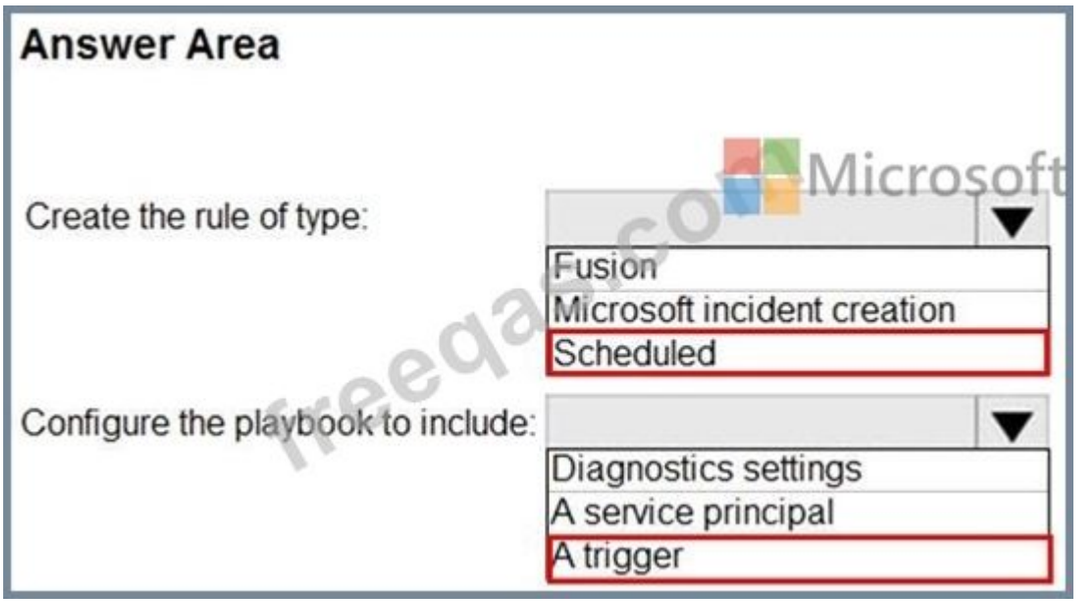
Reference:
https://docs.microsoft.com/en-us/cloud-app-security/governance-discovery

NEW QUESTION: 115
You need to create the analytics rule to meet the Azure Sentinel requirements.
What should you do? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Answer Area



Answer:



NEW QUESTION: 116

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 (LEAVE A REPLY)

Reference:

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

NEW QUESTION: 117

Your company uses Microsoft Defender for Endpoint.

The company has Microsoft Word documents that contain macros. The documents are used frequently on the devices of the company's accounting team.

You need to hide false positive in the Alerts queue, while maintaining the existing security posture. Which three actions should you perform? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

A. Resolve the alert automatically.

B. Hide the alert.
C. Create a suppression rule scoped to any device.
D. Create a suppression rule scoped to a device group.
E. Generate the alert.
Answer: B,C,E (LEAVE A REPLY)
Reference:
https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/manage-alerts

NEW QUESTION: 118
You have a suppression rule in Azure Security Center for 10 virtual machines that are used for testing. The virtual machines run Windows Server.
You are troubleshooting an issue on the virtual machines.
In Security Center, you need to view the alerts generated by the virtual machines during the last five days.
What should you do?
A. Change the rule expiration date of the suppression rule.
B. Change the state of the suppression rule to Disabled.
C. Modify the filter for the Security alerts page.
D. View the Windows event logs on the virtual machines.
Answer: (SHOW ANSWER)
Reference:
https://docs.microsoft.com/en-us/azure/security-center/alerts-suppression-rules

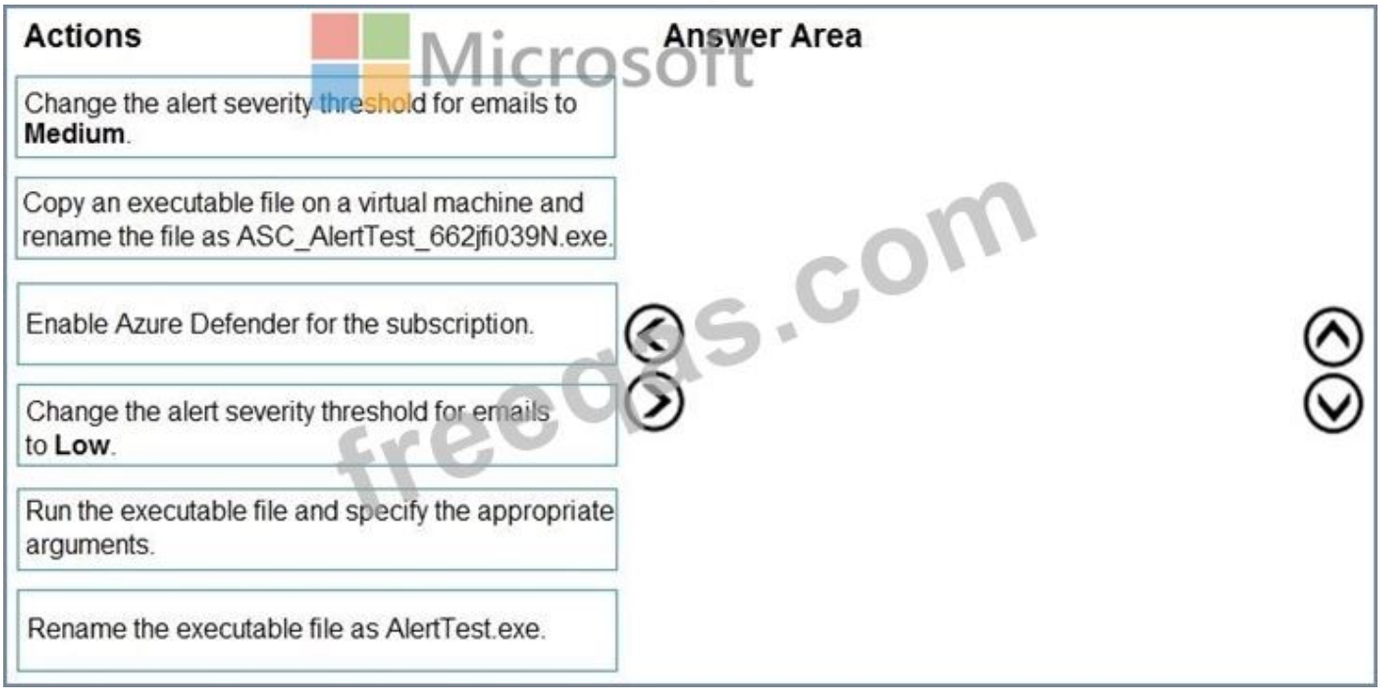
NEW QUESTION: 119
You are investigating a potential attack that deploys a new ransomware strain.
You plan to perform automated actions on a group of highly valuable machines that contain sensitive information.
You have three custom device groups.
You need to be able to temporarily group the machines to perform actions on the devices.
Which three actions should you perform? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.
A. Add a tag to the device group.
B. Add the device users to the admin role.
C. Add a tag to the machines.
D. Create a new device group that has a rank of 1.
E. Create a new admin role.
F. Create a new device group that has a rank of 4.
Answer: B,D,E (LEAVE A REPLY)
Explanation/Reference:
https://www.drware.com/how-to-use-tagging-effectively-in-microsoft-defender-for-endpoint-part-1/

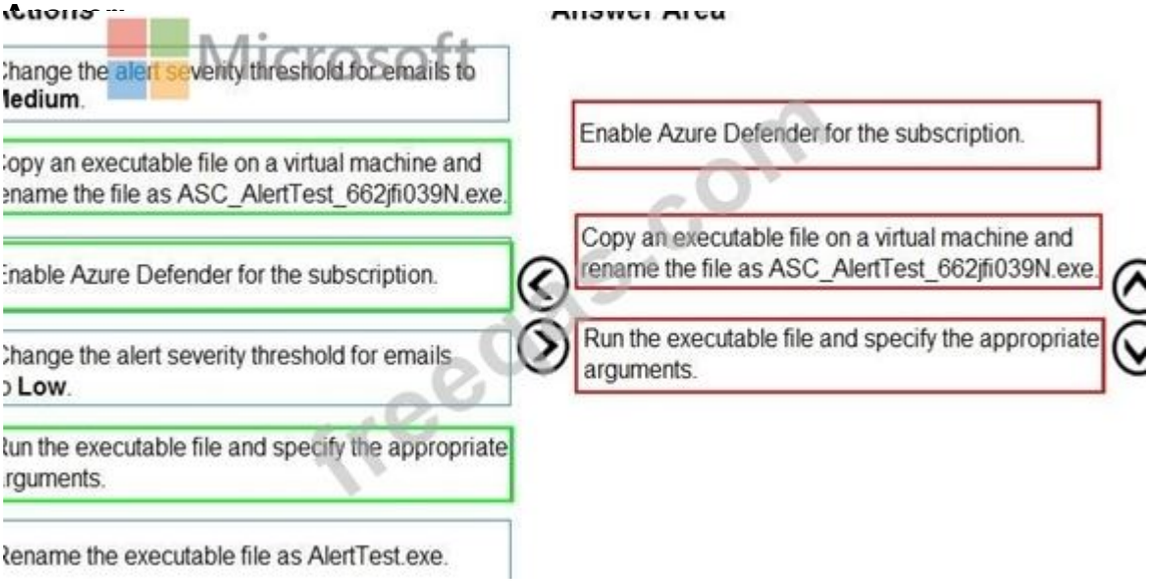
NEW QUESTION: 120

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.





Reference:

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