Up-to-date Questions and Answers from authentic resources to improve knowledge and pass the exam at very first attempt. ----- Guaranteed.

KILL EXAMS

SC-200 MCQs
SC-200 TestPrep
SC-200 Study Guide
SC-200 Practice Test
SC-200 Exam Questions

Microsoft

SC-200

Microsoft Security Operations Analyst

Question: 26

You need to complete the query for failed sign-ins to meet the technical requirements.

Where can you find the column name to complete the where clause?
A. Security alerts in Azure Security Center
B. Activity log in Azure
C. Azure Advisor
D. the query windows of the Log Analytics workspace

Answer: D

Question: 27

DRAG DROP

You have 50 on-premises servers.

You have an Azure subscription that uses Microsoft Defender for Cloud. The Defender for Cloud deployment has Microsoft Defender for Servers and automatic provisioning enabled.

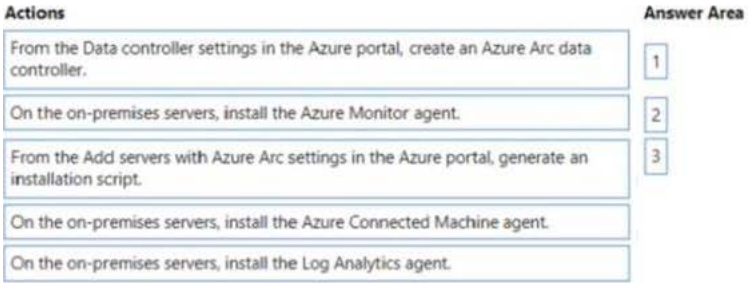
You need to configure Defender for Cloud to support the on-premises servers.

The solution must meet the following requirements:

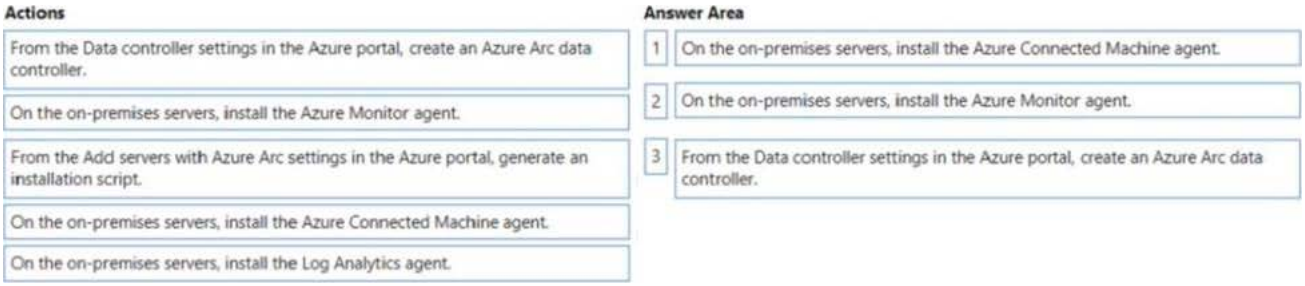
• Provide threat and vulnerability management.

• Support data collection rules.

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



Answer:



Explanation:

To configure Defender for Cloud to support the on-premises servers, you should perform the following three actions in sequence:

On the on-premises servers, install the Azure Connected Machine agent.

On the on-premises servers, install the Log Analytics agent.

From the Data controller settings in the Azure portal, create an Azure Arc data controller.

Once these steps are completed, the on-premises servers will be able to communicate with the Azure Defender for Cloud deployment and will be able to support threat and vulnerability management as well as data collection rules.

Reference: https://docs.microsoft.com/en-us/azure/security-center/deploy-azure-security-center#on-premises-deployment

Question: 28

HOTSPOT

You have an Azure subscription that uses Azure Defender.

You plan to use Azure Security Center workflow automation to respond to Azure Defender threat alerts.

You need to create an Azure policy that will perform threat remediation automatically.

What should you include in the solution? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Set available effects to:

Append
DeployIfNotExists
EnforceRegoPolicy

To perform remediation use:

An Azure Automation runbook that has a webhook
An Azure Logic Apps app that has the trigger set to When an Azure Security Center Alert is created or triggered
An Azure Logic Apps app that has the trigger set to When a response to an Azure Security Center alert is triggered

Answer:

Set available effects to:

Append
DeployIfNotExists
EnforceRegoPolicy

To perform remediation use:

An Azure Automation runbook that has a webhook
An Azure Logic Apps app that has the trigger set to When an Azure Security Center Alert is created or triggered
An Azure Logic Apps app that has the trigger set to When a response to an Azure Security Center alert is triggered

Explanation:

Graphical user interface, text, application

Description automatically generated

Question: 29

You need to implement the Azure Information Protection requirements.

What should you configure first?
A. Device health and compliance reports settings in Microsoft Defender Security Center
B. scanner clusters in Azure Information Protection from the Azure portal
C. content scan jobs in Azure Information Protection from the Azure portal
D. Advanced features from Settings in Microsoft Defender Security Center

Answer: D

Explanation:

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

Question: 30

You have a Microsoft 365 tenant that uses Microsoft Exchange Online and Microsoft Defender for Office 365.

What should you use to identify whether zero-hour auto purge (ZAP) moved an email message from the mailbox of a user?
A. the Threat Protection Status report in Microsoft Defender for Office 365
B. the mailbox audit log in Exchange
C. the Safe Attachments file types report in Microsoft Defender for Office 365
D. the mail flow report in Exchange

Answer: A

Explanation:

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

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

Question: 31

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

You discover that the rule fails intermittently.

What are two possible causes of the failures? Each correct answer presents part of the solution. NOTE: Each correct selection is worth one point.
A. The rule query takes too long to run and times out.
B. The target workspace was deleted.
C. Permissions to the data sources of the rule query were modified.
D. There are connectivity issues between the data sources and Log Analytics

Answer: A,D

Question: 32

HOTSPOT

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

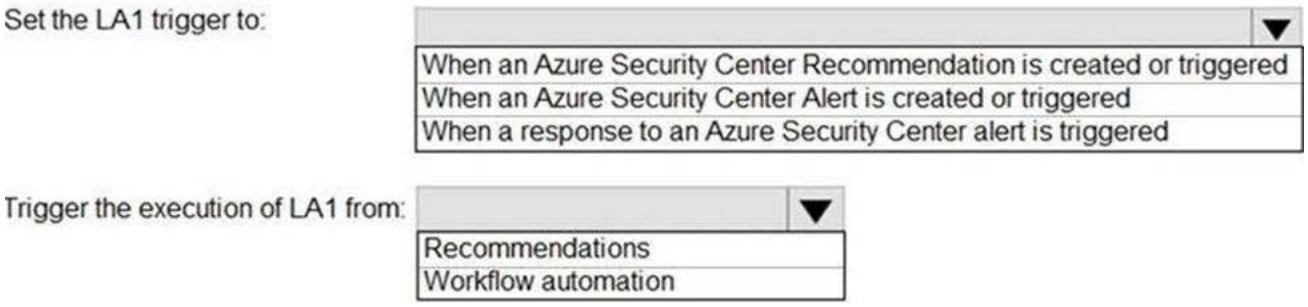
You create an Azure logic app named LA1.

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

You need to test LA1 in Security Center.

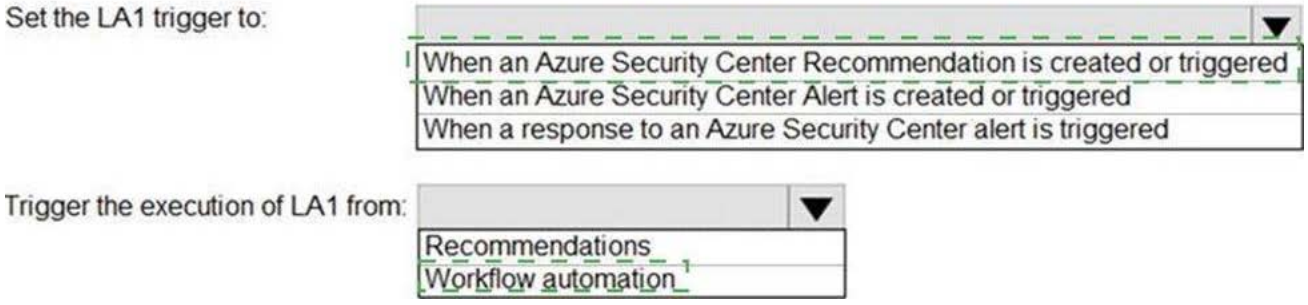
What should you do? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Answer Area



Answer:

Answer Area



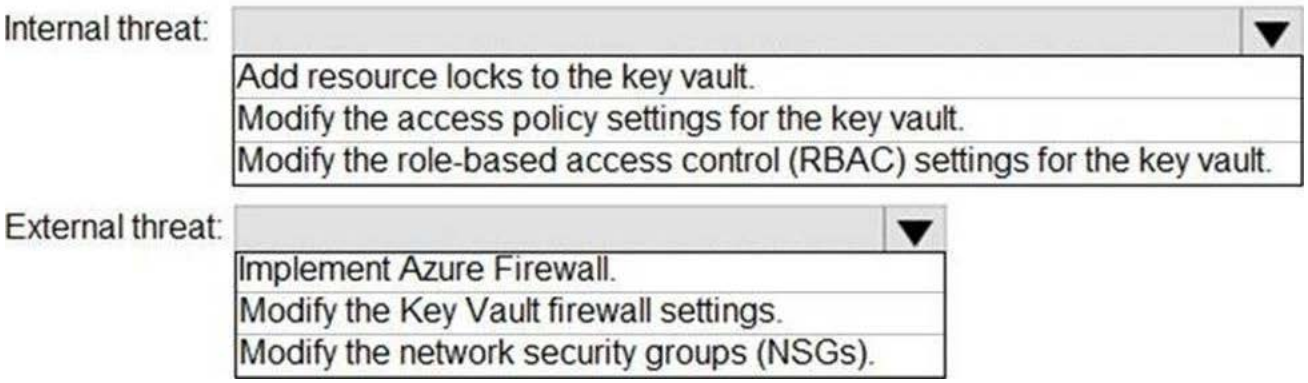
Question: 33

HOTSPOT

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

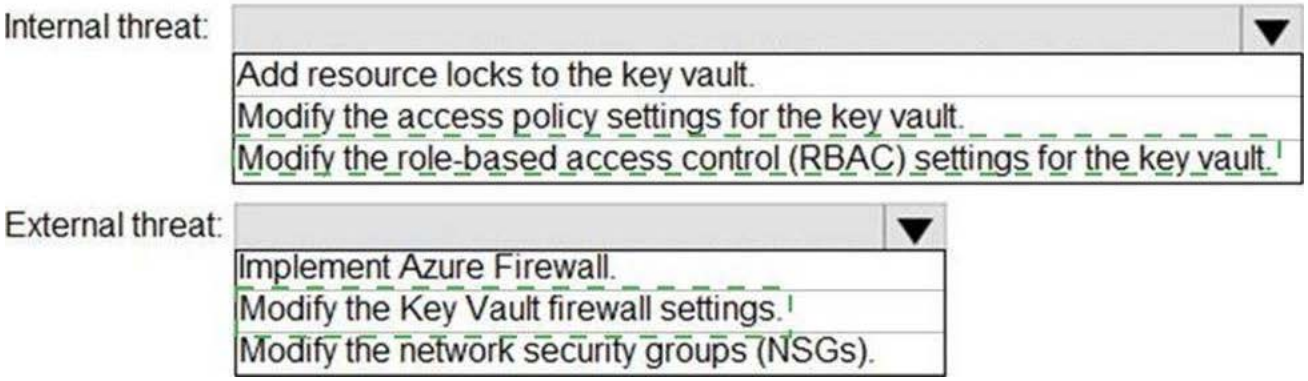
What should you recommend for each threat? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Answer Area



Answer:

Answer Area



Question: 34

Topic 2, Litware inc.

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 C 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.

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.

Actions	Answer Area
Provide domain administrator credentials to the litware.com Active Directory domain.	
Create an instance of Microsoft Defender for Identity.	
Provide global administrator credentials to the litware.com Azure AD tenant.	
Install the sensor on DC1.	
Install the standalone sensor on DC1.	

Answer:

Actions	Answer Area
Provide domain administrator credentials to the litware.com Active Directory domain.	Provide global administrator credentials to the litware.com Azure AD tenant.
Create an instance of Microsoft Defender for Identity.	Create an instance of Microsoft Defender for Identity.
Provide global administrator credentials to the litware.com Azure AD tenant.	Provide domain administrator credentials to the litware.com Active Directory domain.
Install the sensor on DC1.	Install the sensor on DC1.
Install the standalone sensor on DC1.	

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.

Question: 35

HOTSPOT

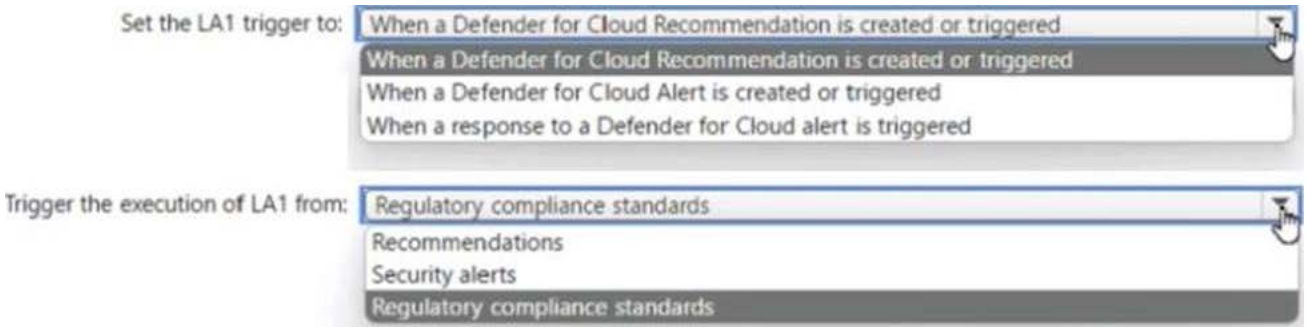
You have an Azure subscription that has Azure Defender enabled for all supported resource types.

You create an Azure logic app named LA1.

You plan to use LA1 to automatically remediate security risks detected in Defenders for Cloud.

You need to test LA1 in Defender for Cloud.

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



Answer:

Question: 36

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.

[▼]
CloudAppEvents
DeviceFileEvents
DeviceProcessEvents

```
| where TimeStamp > ago(2d)
| summarize activityCount = [ ▼ ] by FolderPath, FileName,
ActionType, AccountDisplayName
| where activityCount > 5
```

avg()
count()
sum()

Answer:

[▼]
CloudAppEvents
DeviceFileEvents
DeviceProcessEvents

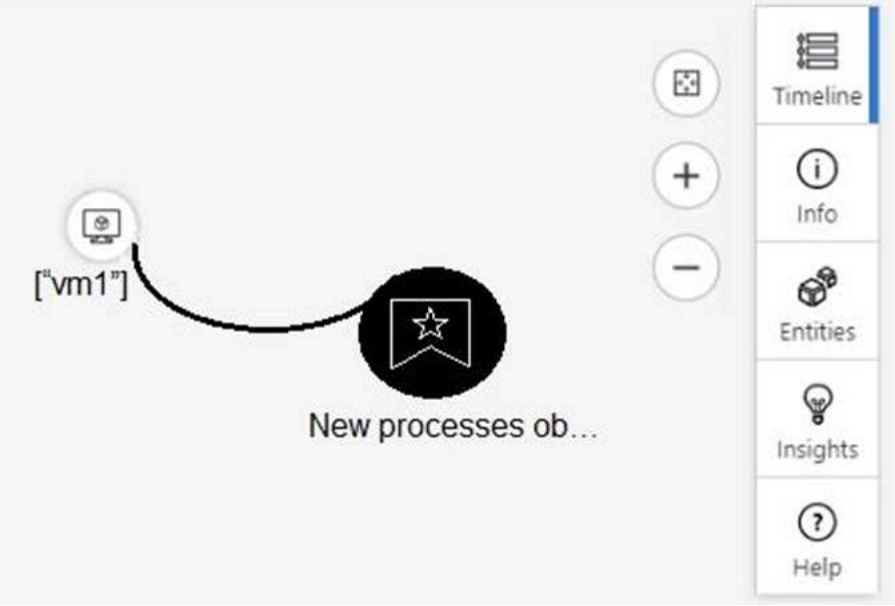
```
| where TimeStamp > ago(2d)
| summarize activityCount = [ ▼ ] by FolderPath, FileName,
ActionType, AccountDisplayName
| where activityCount > 5
```

avg()
count()
sum()

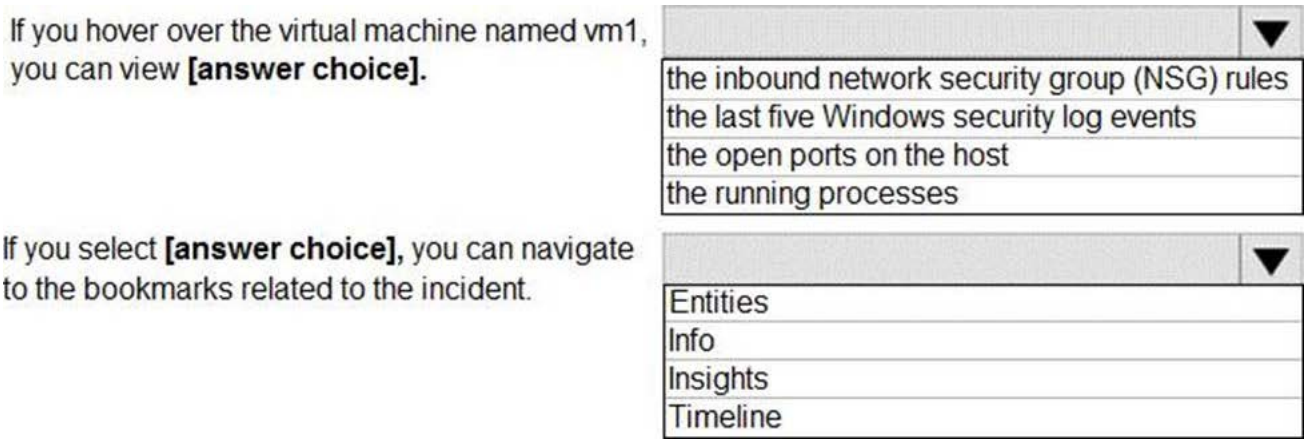
Question: 37

HOTSPOT

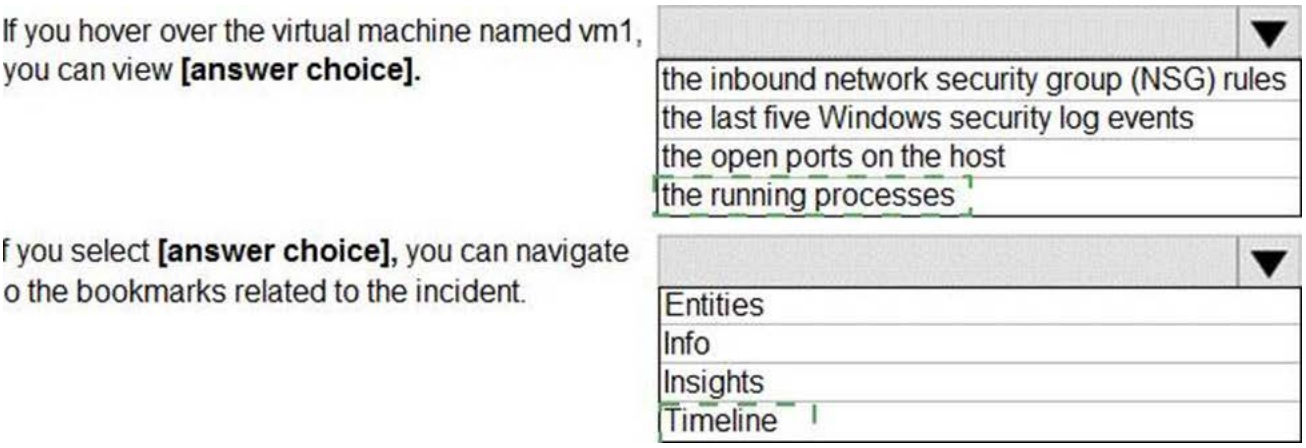
From Azure Sentinel, you open the Investigation pane for a high-severity incident as shown in the following exhibit.



Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic. NOTE: Each correct selection is worth one point.



Answer:



Question: 38

Topic 3, Misc. Questions

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

Which anomaly detection policy should you use?
A. Impossible travel
B. Activity from anonymous IP addresses
C. Activity from infrequent country
D. Malware detection

Answer: C

Explanation:

Activity from a country/region that could indicate malicious activity. This policy profiles your environment and triggers alerts when activity is detected from a location that was not recently or was never visited by any user in the organization. Activity from the same user in different locations within a time period that is shorter than the expected

travel time between the two locations. This can indicate a credential breach, however, it's also possible that the user's actual location is masked, for example, by using a VPN.

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

Question: 39

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

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

To which service should you export the alerts?
A. Azure Cosmos DB
B. Azure Event Grid
C. Azure Event Hubs
D. Azure Data Lake

Answer: C

Explanation:

Reference: https://docsmicrosoftcom/en-us/azure/security-center/continuous-export?tabs=azure-portal

Question: 40

HOTSPOT

You have a Microsoft 365 E5 subscription that uses Microsoft Defender and an Azure subscription that uses Azure Sentinel.

You need to identify all the devices that contain files in emails sent by a known malicious email sender. The query will be based on the match of the SHA256 hash.

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

```
EmailAttachmentInfo
| where SenderFromAddress =~ "MaliciousSender@example.com"
where isnotempty [ ▼ ]
```

- (DeviceId)
- (RecipientEmailAddress)
- (SenderFromAddress)
- (SHA256)

```
| join (
DeviceFileEvents
| project FileName, SHA256
) on [ ▼ ]
```

- (DeviceId)
- (RecipientEmailAddress)
- (SenderFromAddress)
- (SHA256)

```
| project Timestamp, FileName, SHA256, DeviceName, DeviceId,
NetworkMessageId, SenderFromAddress, RecipientEmailAddress
```

Answer:

```
EmailAttachmentInfo
| where SenderFromAddress =~ "MaliciousSender@example.com"
where isnotempty [ ▼ ]
```

- (DeviceId)
- (RecipientEmailAddress)
- (SenderFromAddress)
- (SHA256)

```
| join (
DeviceFileEvents
| project FileName, SHA256
) on [ ▼ ]
```

- (DeviceId)
- (RecipientEmailAddress)
- (SenderFromAddress)
- (SHA256)

```
| project Timestamp, FileName, SHA256, DeviceName, DeviceId,
NetworkMessageId, SenderFromAddress, RecipientEmailAddress
```

Explanation:

Graphical user interface, text, application

Description automatically generated

Question: 41

You have an Azure subscription that uses Microsoft Sentinel.

You detect a new threat by using a hunting query.

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

What should you do?
A. Create a playbook.
B. Create a watchlist.
C. Create an analytics rule.
D. Add the query to a workbook.

Answer: C

Explanation:

By creating an analytics rule, you can set up a query that will automatically run and alert you when the threat is detected, without having to manually run the query. This will help minimize administrative effort, as you can set up the rule once and it will run on a schedule, alerting you when the threat is detected.

Reference: https://docs.microsoft.com/en-us/azure/sentinel/analytics-create-rule

KILLEXAMS.COM

Killexams.com is a leading online platform specializing in high-quality certification exam preparation. Offering a robust suite of tools, including MCQs, practice tests, and advanced test engines, Killexams.com empowers candidates to excel in their certification exams. Discover the key features that make Killexams.com the go-to choice for exam success.

Exam Questions:

Killexams.com provides exam questions that are experienced in test centers. These questions are updated regularly to ensure they are up-to-date and relevant to the latest exam syllabus. By studying these questions, candidates can familiarize themselves with the content and format of the real exam.

Exam MCQs:

Killexams.com offers exam MCQs in PDF format. These questions contain a comprehensive collection of questions and answers that cover the exam topics. By using these MCQs, candidate can enhance their knowledge and improve their chances of success in the certification exam.

Practice Test:

Killexams.com provides practice test through their desktop test engine and online test engine. These practice tests simulate the real exam environment and help candidates assess their readiness for the actual exam. The practice test cover a wide range of questions and enable candidates to identify their strengths and weaknesses.

Guaranteed Success:

Killexams.com offers a success guarantee with the exam MCQs. Killexams claim that by using this materials, candidates will pass their exams on the first attempt or they will get refund for the purchase price. This guarantee provides assurance and confidence to individuals preparing for certification exam.

Updated Contents:

Killexams.com regularly updates its question bank of MCQs to ensure that they are current and reflect the latest changes in the exam syllabus. This helps candidates stay up-to-date with the exam content and increases their chances of success.