Experience 24/7 Support And Real Microsoft SC-200 Exam Questions With Pass4Test

Download Free PDF Demo for Microsoft-SC-200 Exam from PassExam4Sure

PassExam4Sure provides a totally free demo version to try the product out with sample features before purchasing it. This demonstrates our concern for your best possible experience. You may obtain the Microsoft-SC-200 braindumps Questions immediately after you have thoroughly tested the demo.

Download Free Demo Q&A

BTW, DOWNLOAD part of Pass4Test SC-200 dumps from Cloud Storage: https://drive.google.com/open?id=1iZTVhOWxATZyUz3PylZcnaxtmWSDlN2d

Our Microsoft Certified: Security Operations Analyst Associate exam question is widely known throughout the education market. Almost all the candidates who are ready for the qualifying examination know our products. Even when they find that their classmates or colleagues are preparing a SC-200 exam, they will introduce our study materials to you. So, our learning materials help users to be assured of the SC-200 exam. Currently, my company has introduced a variety of learning materials, covering almost all the official certification of qualification exams, and each SC-200 practice dump in our online store before the listing, are subject to stringent quality checks within the company. Thus, users do not have to worry about such trivial issues as typesetting and proofreading, just focus on spending the most practice to use our Microsoft Certified: Security Operations Analyst Associate test materials. After careful preparation, I believe you will be able to pass the exam.

Microsoft SC-200 Certification is an excellent way for cybersecurity professionals to demonstrate their expertise in managing and responding to security incidents. Microsoft Security Operations Analyst certification covers a broad range of security topics and validates the candidate's ability to use Microsoft security technologies to maintain a secure network environment. Microsoft Security Operations Analyst certification is ideal for individuals who want to advance their careers in the cybersecurity industry and demonstrate their expertise in Microsoft security technologies.

Skills measured

- Mitigate threats using Azure Defender (25-30%)
- Mitigate threats using Azure Sentinel (40-45%)
- Mitigate threats using Microsoft 365 Defender (25-30%)

>> SC-200 Test Book <<

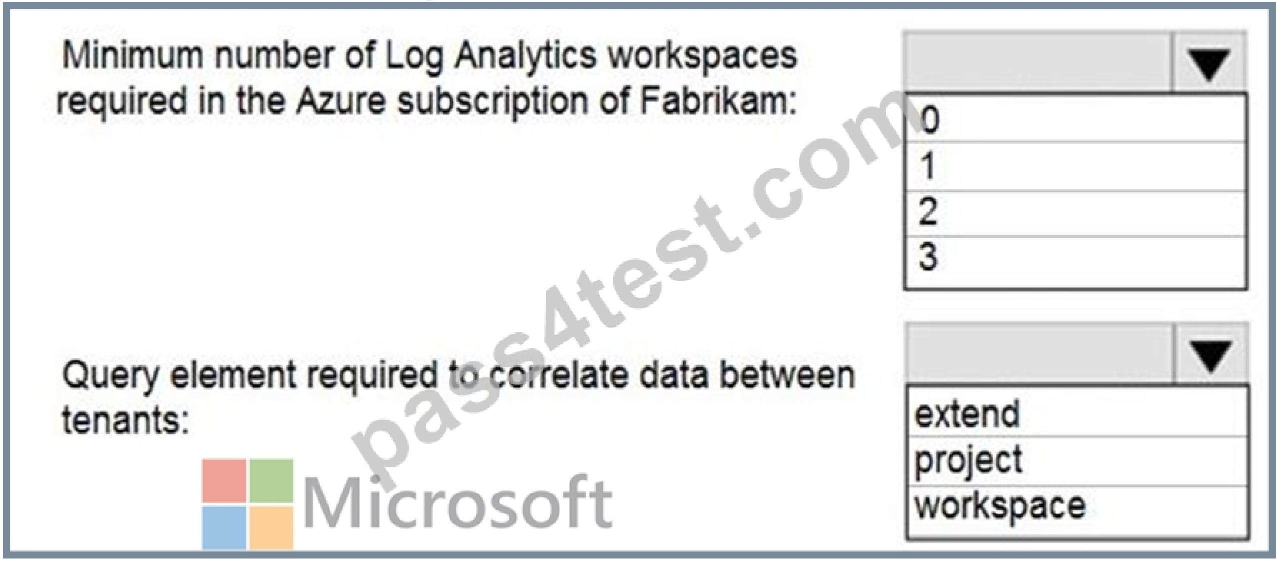
Microsoft Security Operations Analyst exam dumps & SC-200 practice torrent & Microsoft Security Operations Analyst training vces

The Microsoft Security Operations Analyst exam dumps are designed efficiently and pointedly, so that users can check their learning effects in a timely manner after completing a section. Good practice on the success rate of SC-200 quiz guide is not fully indicate that you have mastered knowledge is skilled, therefore, the SC-200 test material let the user consolidate learning content as many times as possible, although the practice seems very boring, but it can achieve the result of good consolidate knowledge.

Passing the Microsoft SC-200 Exam validates the candidate's ability to identify, investigate, and respond to security threats in a Microsoft environment. Microsoft Security Operations Analyst certification demonstrates that the candidate has the skills and knowledge required to manage security incidents and protect Microsoft environments against cyber threats. Microsoft Security Operations Analyst certification is highly valued in the industry and can open up new career opportunities for security operations analysts.

Microsoft Security Operations Analyst Sample Questions (Q225-Q230):

NEW QUESTION # 225
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.



Minimum number of Log Analytics workspaces required in the Azure subscription of Fabrikam: ▼

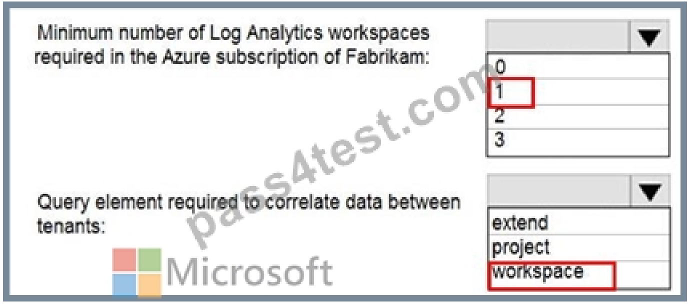
0
1
2
3

Query element required to correlate data between tenants: ▼

extend
project
workspace

Answer:

Explanation:



Minimum number of Log Analytics workspaces required in the Azure subscription of Fabrikam: ▼

0
[✓ 1]
2
3

Query element required to correlate data between tenants: ▼

extend
project
[✓ workspace]

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

NEW QUESTION # 226
You have a Microsoft 365 E5 subscription that uses Microsoft Defender for Endpoint. You need to create a detection rule that

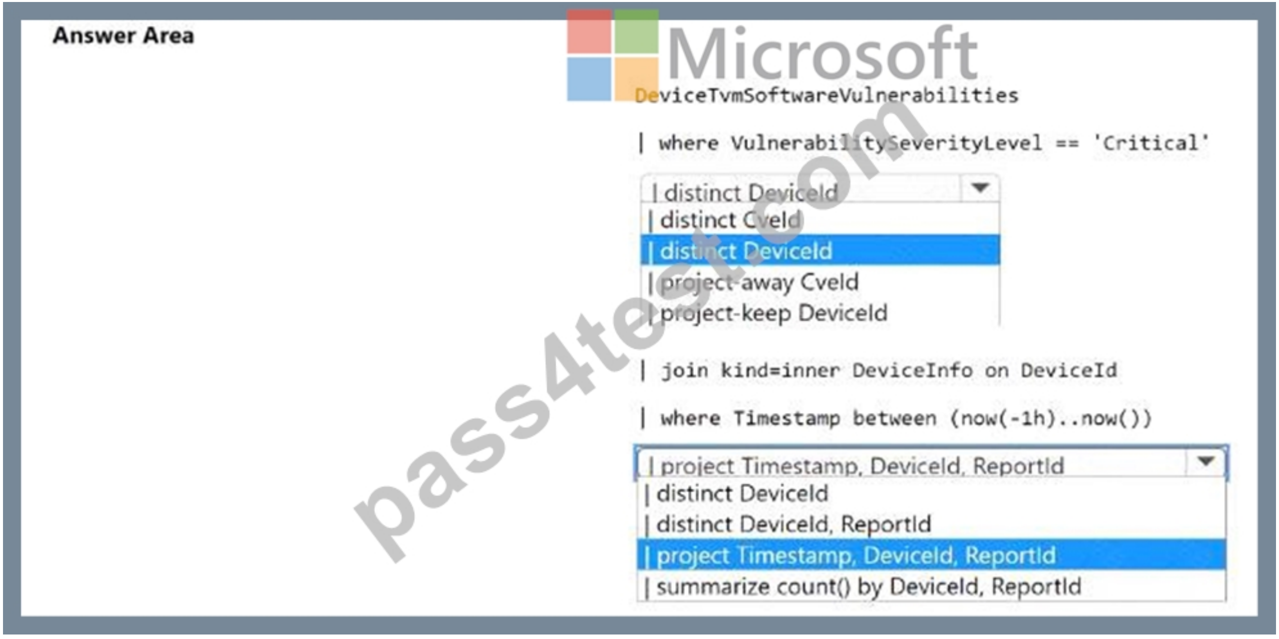
meets the following requirements:

* Is triggered when a device that has critical software vulnerabilities was active during the last hour

* Limits the number of duplicate results

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

NOTE: Each correct selection is worth one point.



Answer Area

```
DeviceTvmSoftwareVulnerabilities
| where VulnerabilitySeverityLevel == 'Critical'
```

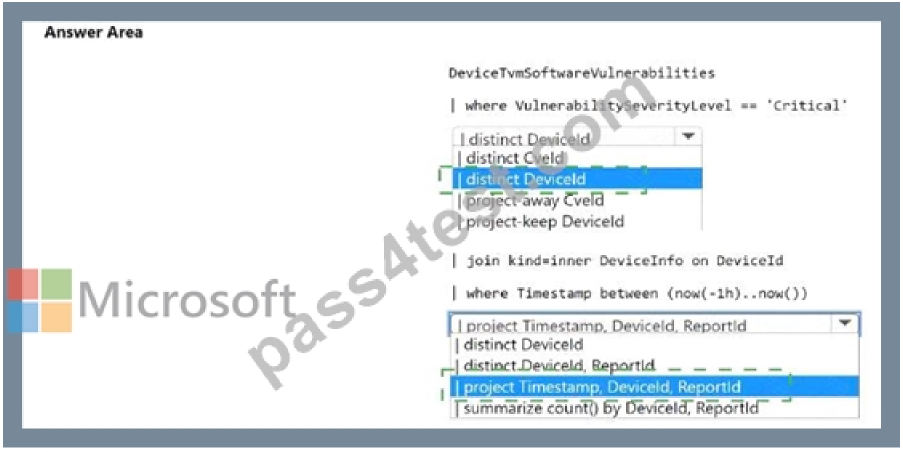
| distinct DeviceId ▼
- | distinct CveId
- | distinct DeviceId
- | project-away CveId
- | project-keep DeviceId

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

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

Answer:

Explanation:



Answer Area

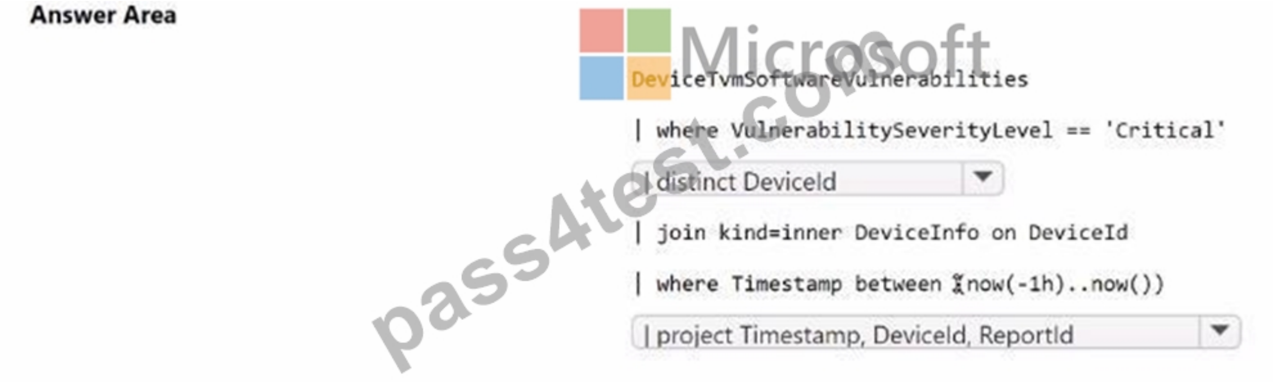
```
DeviceTvmSoftwareVulnerabilities
| where VulnerabilitySeverityLevel == 'Critical'
```

| distinct DeviceId ▼
- | distinct CveId
- | distinct DeviceId
- | project-away CveId
- | project-keep DeviceId

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

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

Explanation:



Answer Area

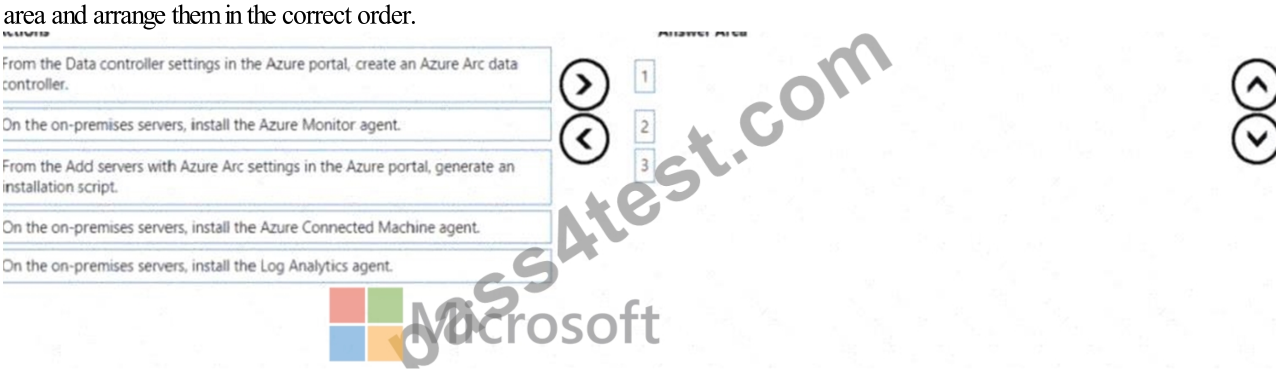
```
DeviceTvmSoftwareVulnerabilities
| where VulnerabilitySeverityLevel == 'Critical'
| distinct DeviceId
| join kind=inner DeviceInfo on DeviceId
| where Timestamp between (now(-1h)..now())
| project Timestamp, DeviceId, ReportId
```

NEW QUESTION # 227

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.



Actions

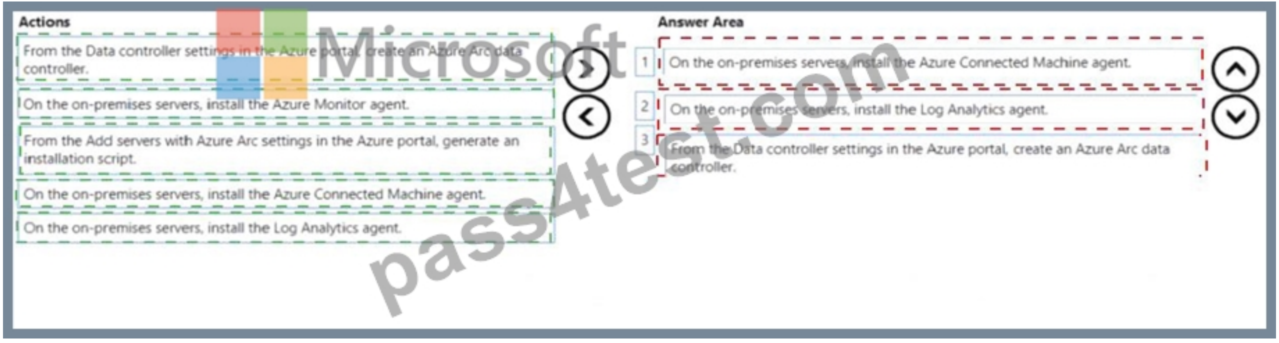
- From the Data controller settings in the Azure portal, create an Azure Arc data controller.
- On the on-premises servers, install the Azure Monitor agent.
- From the Add servers with Azure Arc settings in the Azure portal, generate an installation script.
- On the on-premises servers, install the Azure Connected Machine agent.
- On the on-premises servers, install the Log Analytics agent.

Answer Area

1
2
3

Answer:

Explanation:



Actions

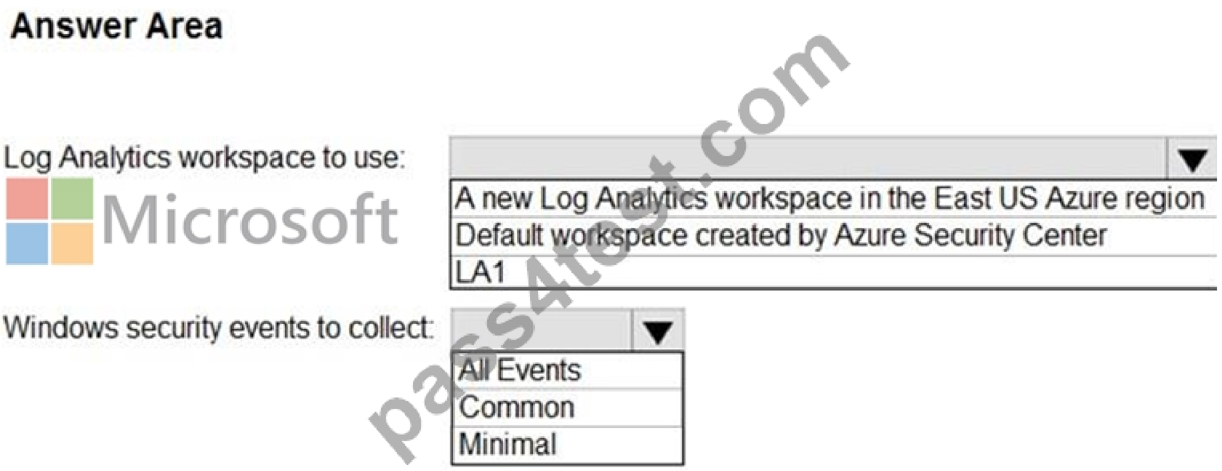
- From the Data controller settings in the Azure portal, create an Azure Arc data controller.
- On the on-premises servers, install the Azure Monitor agent.
- From the Add servers with Azure Arc settings in the Azure portal, generate an installation script.
- On the on-premises servers, install the Azure Connected Machine agent.
- On the on-premises servers, install the Log Analytics agent.

Answer Area

1. On the on-premises servers, install the Azure Connected Machine agent.
2. On the on-premises servers, install the Log Analytics agent.
3. From the Data controller settings in the Azure portal, create an Azure Arc data controller.

Explanation:
To integrate on-premises servers into Microsoft Defender for Cloud and support features such as Threat and Vulnerability Management (TVM) and data collection rules, the servers must first be connected to Azure Arc. Azure Arc allows non-Azure servers to be managed as Azure resources and enables Defender for Cloud capabilities such as endpoint protection, vulnerability management, and compliance assessment.
The correct sequence of steps is:
1## Generate the installation script:
In the Azure portal, navigate to Azure Arc # Servers # Add. From there, select the appropriate subscription and resource group, then generate the Azure Arc onboarding script. This script includes registration commands and configuration for the machine to connect to Azure.
2## Install the Azure Connected Machine agent:
On each on-premises server, run the generated script. This installs the Azure Connected Machine agent (Azure Arc agent), which establishes communication between the on-premises server and Azure. After installation, the server appears as an Arc-enabled machine in the Azure portal.
3## Create an Azure Arc Data Controller (if data services are required):
Once the machines are connected, you can configure data services or additional Defender for Cloud features (such as data collection and TVM). The Azure Arc Data Controller provides hybrid data capabilities for managing and monitoring on-premises workloads.
This sequence aligns with Microsoft's Defender for Cloud documentation and Arc onboarding best practices, ensuring minimal administrative overhead while enabling full SecOps visibility across hybrid environments.

NEW QUESTION # 228
You need to implement Microsoft Defender for Cloud to meet the Microsoft Defender for Cloud requirements and the business requirements. What should you include in the solution? To answer, select the appropriate options in the answer are a. NOTE: Each correct selection is worth one point.



Answer Area

Log Analytics workspace to use:

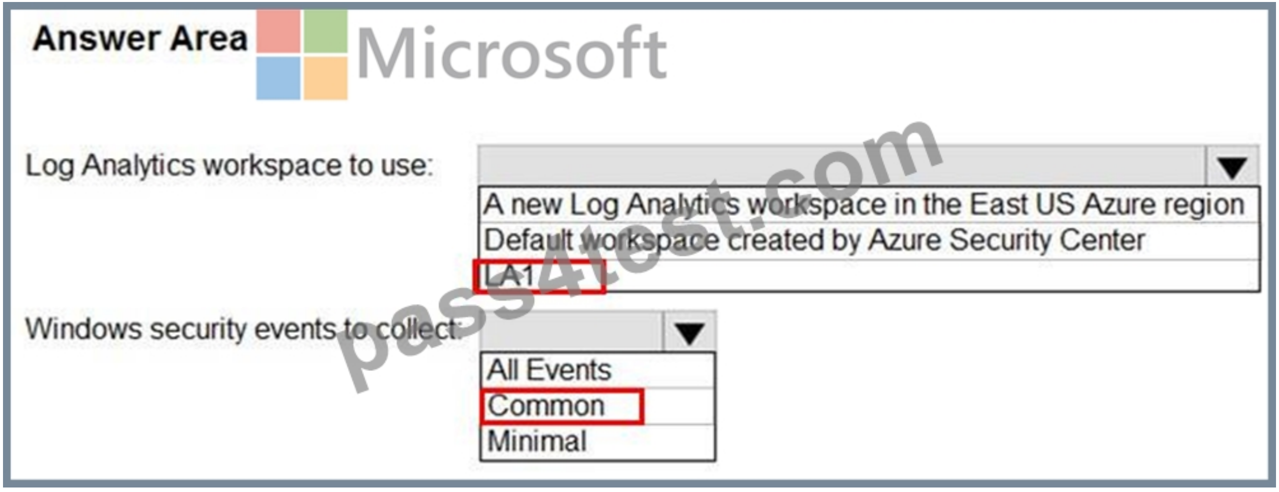
- A new Log Analytics workspace in the East US Azure region
- Default workspace created by Azure Security Center
- LA1

Windows security events to collect:

- All Events
- Common
- Minimal

Answer:

Explanation:



Answer Area

Log Analytics workspace to use:

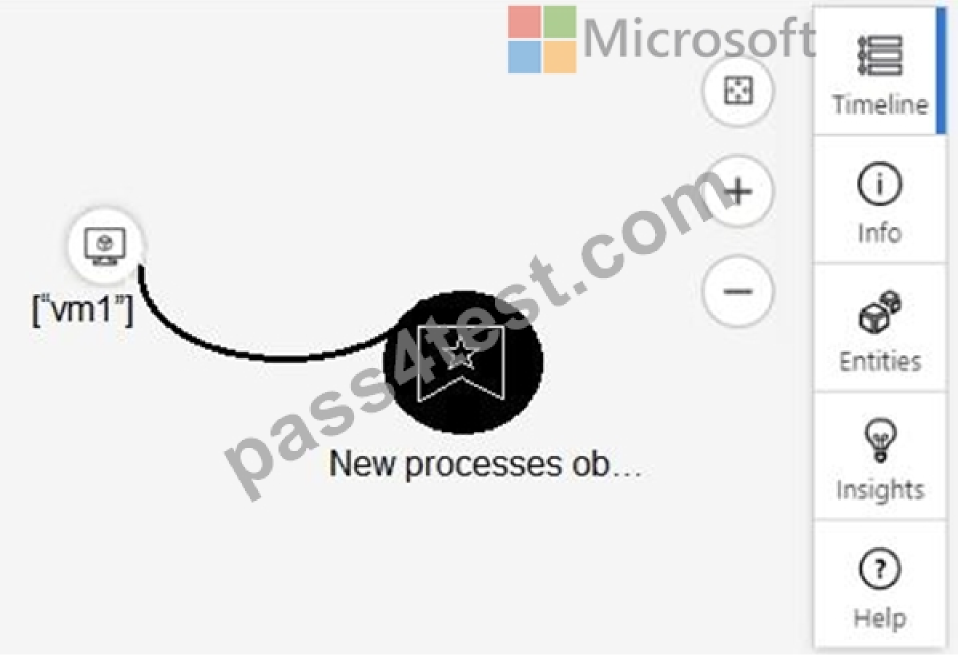
- A new Log Analytics workspace in the East US Azure region
- Default workspace created by Azure Security Center
- [✓ LA1]

Windows security events to collect:

- All Events
- [✓ Common]
- Minimal

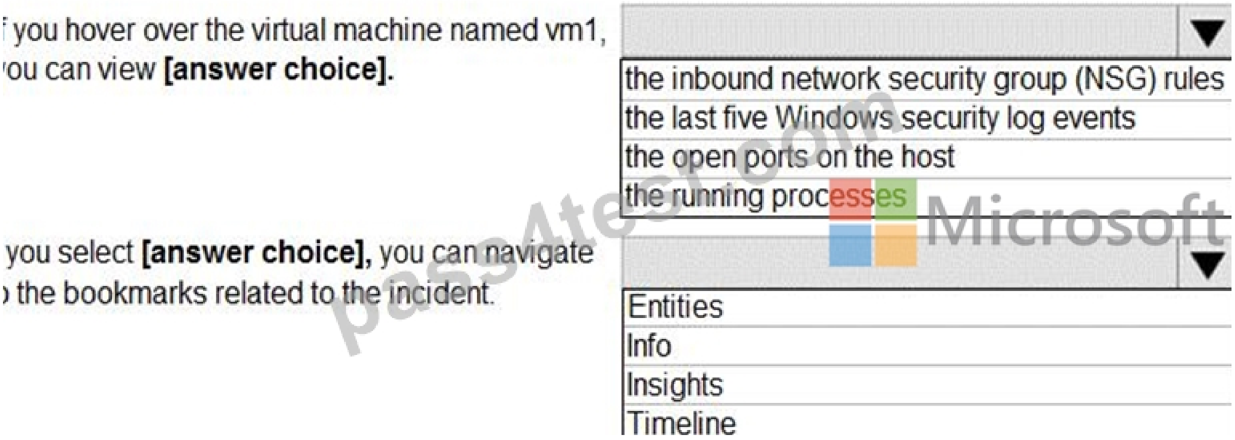
NEW QUESTION # 229

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.



f you hover over the virtual machine named vm1, 'ou can view [answer choice].

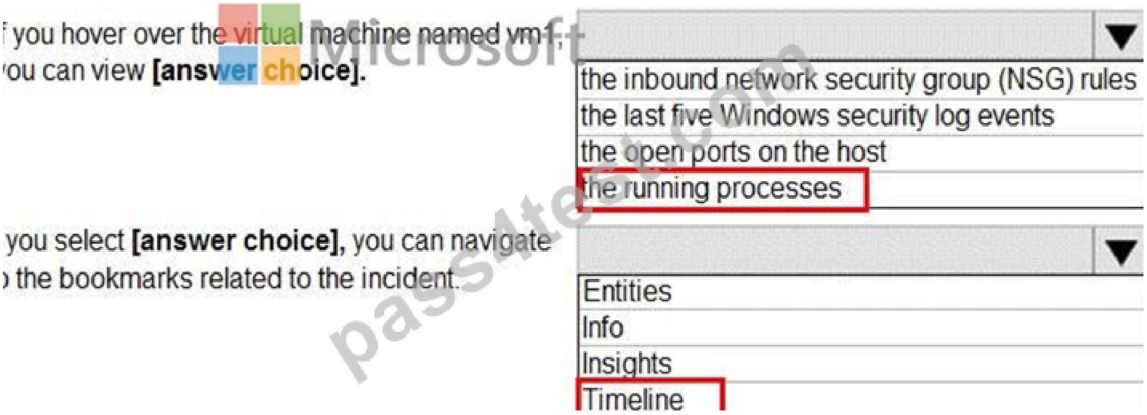
- the inbound network security group (NSG) rules
- the last five Windows security log events
- the open ports on the host
- the running processes

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

- Entities
- Info
- Insights
- Timeline

Answer:

Explanation:



f you hover over the virtual machine named vm1, 'ou can view [answer choice].

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

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

- Entities
- Info
- Insights
- [✓ Timeline]

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

NEW QUESTION # 230

......

PDF SC-200 Cram Exam: https://www.pass4test.com/SC-200.html

- Pass Guaranteed 2026 Microsoft Pass-Sure SC-200 Test Book □ Search for □ SC-200 □ and easily obtain a free download on ▹ www.torrentvce.com ◃ □Test SC-200 Topics Pdf
- www.stes.tyc.edu.tw, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, www.stes.tyc.edu.tw, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, www.stes.tyc.edu.tw, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, www.stes.tyc.edu.tw, daotao.wisebusiness.edu.vn, www.stes.tyc.edu.tw, dorahacks.io, Disposable vapes

BONUS!!! Download part of Pass4Test SC-200 dumps for free: https://drive.google.com/open?id=1iZTVhOWxATZyUz3PylZcnaxtmWSDlN2d