DUMPSsheet

Free Questions for SC-200 by dumpssheet

Shared by Pittman on 22-07-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

You have a Microsoft Sentinel workspace named Workspace1 and 200 custom Advanced Security Information Model (ASIM) parsers based on the DNS schem

a. You need to make the 200 parsers available in Workspace1. The solution must minimize administrative effort. What should you do first?

Options:

A- Copy the parsers to the Azure Monitor Logs page.

B- Create a JSON file based on the DNS template.

C- Create an XML file based on the DNS template.

D- Create a YAML file based on the DNS template.

Answer:

A

Question 2

Question Type: **MultipleChoice**

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

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

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

What should you install on EC2-1?

Options:

A- the Log Analytics agent

B- the Azure Connected Machine agent

C- the unified Microsoft Defender for Endpoint solution package

D- Microsoft Monitoring Agent

Answer:

A

Question 3

Question Type: MultipleChoice

You have an Azure subscription that contains a user named User1.

User1 is assigned an Azure Active Directory Premium Plan 2 license

You need to identify whether the identity of User1 was compromised during the last 90 days.

What should you use?

Options:

A- the risk detections report

B- the risky users report

C- Identity Secure Score recommendations

D- the risky sign-ins report

Answer:

B

Question 4

Question Type: MultipleChoice

You have an Azure subscription that contains an Azure logic app named app1 and a Microsoft Sentinel workspace that has an Azure AD connector. You need to ensure that app1 launches when Microsoft Sentinel detects an Azure AD-generated alert. What should you create first?

Options:

A- a repository connection

B- awatchlist

C- an analytics rule

D- an automation rule

Answer:

D

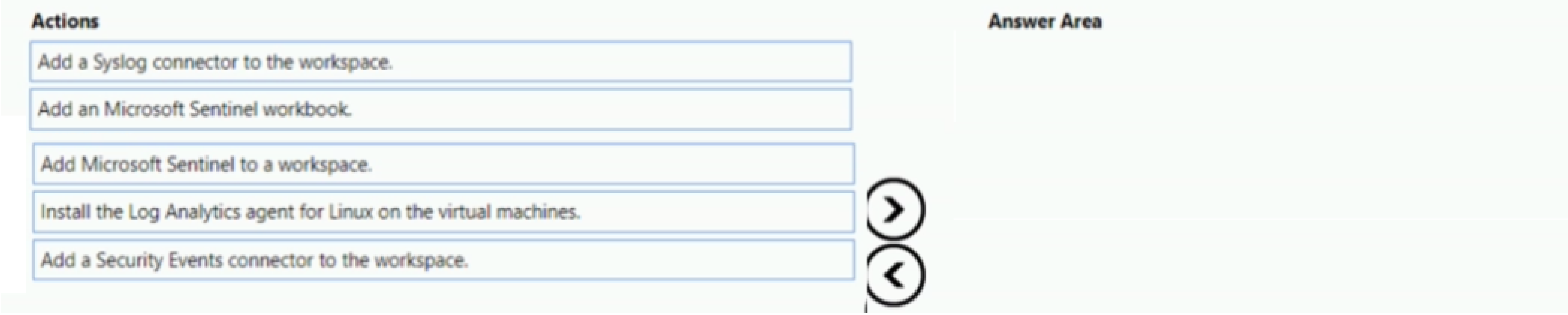
Question 5

Question Type: **OrderList**

You have an Azure subscription that contains 100 Linux virtual machines.

You need to configure Microsoft Sentinel to collect event logs from the virtual machines.

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

- Add a Syslog connector to the workspace.
- Add an Microsoft Sentinel workbook.
- Add Microsoft Sentinel to a workspace.
- Install the Log Analytics agent for Linux on the virtual machines.
- Add a Security Events connector to the workspace.

Answer Area

Answer:

Add Microsoft Sentinel to a workspace.

Add a Security Events connector to the workspace.

Install the Log Analytics agent for Linux on the virtual machines.

Question 6

Question Type: **MultipleChoice**

You have an Azure subscription that use Microsoft Defender for Cloud and contains a user named User1.

You need to ensure that User1 can modify Microsoft Defender for Cloud security policies. The solution must use the principle of least privilege.

Which role should you assign to User1?

Options:

A- Security operator

B- Security Admin

C- Owner

D- Contributor

Answer:

B

Question 7

Question Type: **MultipleChoice**

You have an Azure subscription that uses Microsoft Defender for Cloud and contains 100 virtual machines that run Windows Server.

You need to configure Defender for Cloud to collect event data from the virtual machines. The solution must minimize administrative effort and costs.

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

NOTE: Each correct selection is worth one point.

Options:

A- From the workspace created by Defender for Cloud, set the data collection level to Common

B- From the Microsoft Endpoint Manager admin center, enable automatic enrollment.

C- From the Azure portal, create an Azure Event Grid subscription.

D- From the workspace created by Defender for Cloud, set the data collection level to All Events

E- From Defender for Cloud in the Azure portal, enable automatic provisioning for the virtual machines.

Answer:

D, E

Question 8

Question Type: Hotspot

You have a Microsoft Sentinel workspace that has User and Entity Behavior Analytics (UEBA) enabled.

You need to identify all the log entries that relate to security-sensitive user actions performed on a server named Server1. The solution must meet the following requirements:

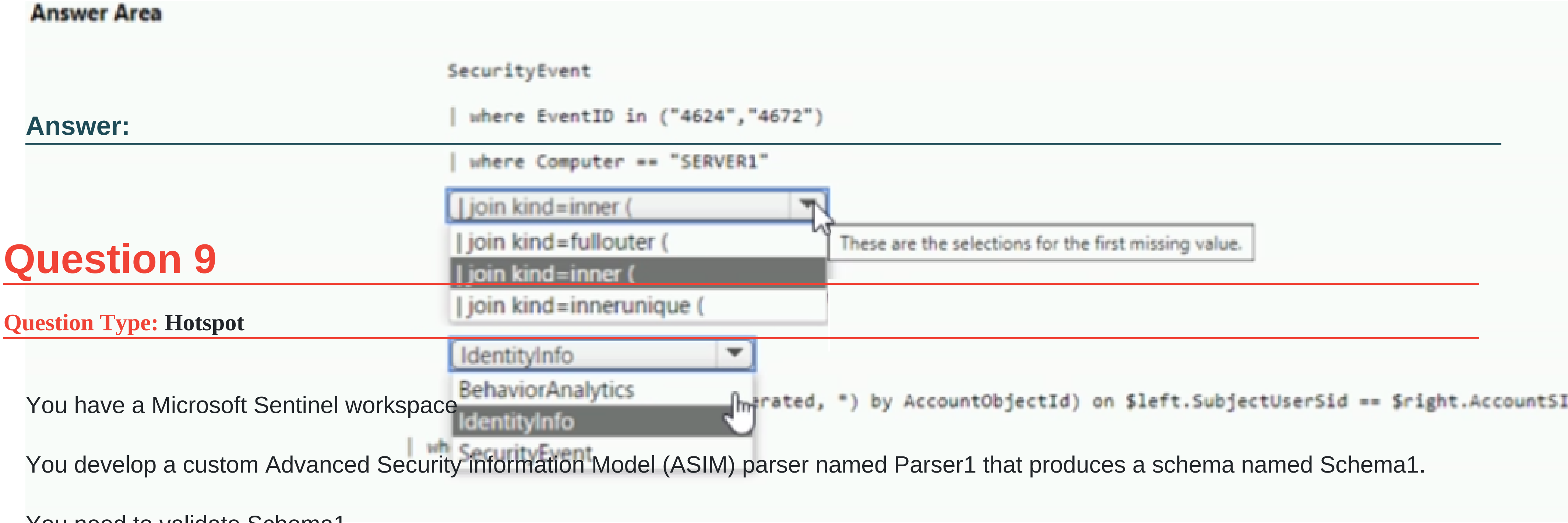
* Only include security-sensitive actions by users that are NOT members of the IT department.

* Minimize the number of false positives.

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

a. NOTE: Each correct selection is worth one point.

Answer:



Answer Area

```
SecurityEvent
| where EventID in ("4624","4672")
| where Computer == "SERVER1"
| join kind=inner (
IdentityInfo
...rated, *) by AccountObjectId) on $left.SubjectUserSid == $right.AccountSI
| wh
```

Question 9

Question Type: **Hotspot**

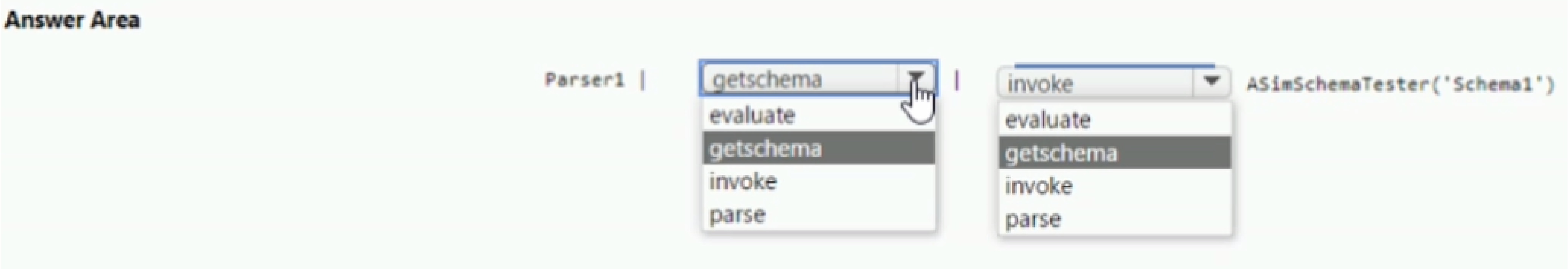
You have a Microsoft Sentinel workspace.

You develop a custom Advanced Security information Model (ASIM) parser named Parser1 that produces a schema named Schema1.

You need to validate Schema1.

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

NOTE: Each correct selection is worth one point.



Answer Area

```
Parser1 | getschema | invoke ASimSchemaTester('Schema1')
```

Answer:

Question 10

Question Type: Hotspot

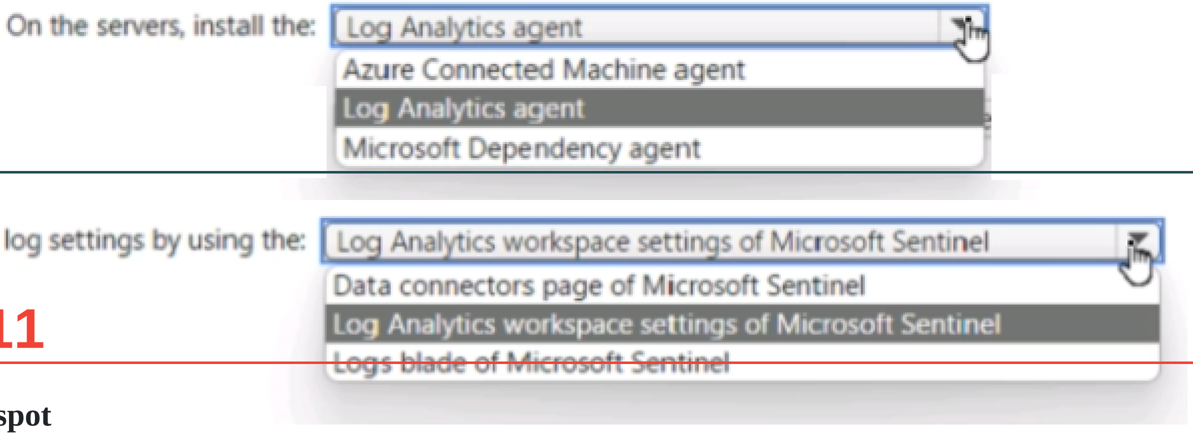
Your on-premises network contains 100 servers that run Windows Server.

You have an Azure subscription that uses Microsoft Sentinel.

You need to upload custom logs from the on-premises servers to Microsoft Sentinel.

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

Answer:



On the servers, install the: Log Analytics agent

Azure Connected Machine agent
Log Analytics agent
Microsoft Dependency agent

Configure custom log settings by using the: Log Analytics workspace settings of Microsoft Sentinel

Data connectors page of Microsoft Sentinel
Log Analytics workspace settings of Microsoft Sentinel
Logs blade of Microsoft Sentinel

Question 11

Question Type: Hotspot

You have an Azure subscription.

You plan to implement an Microsoft Sentinel workspace. You anticipate that you will ingest 20 GB of security log data per day.

You need to configure storage for the workspace. The solution must meet the following requirements:

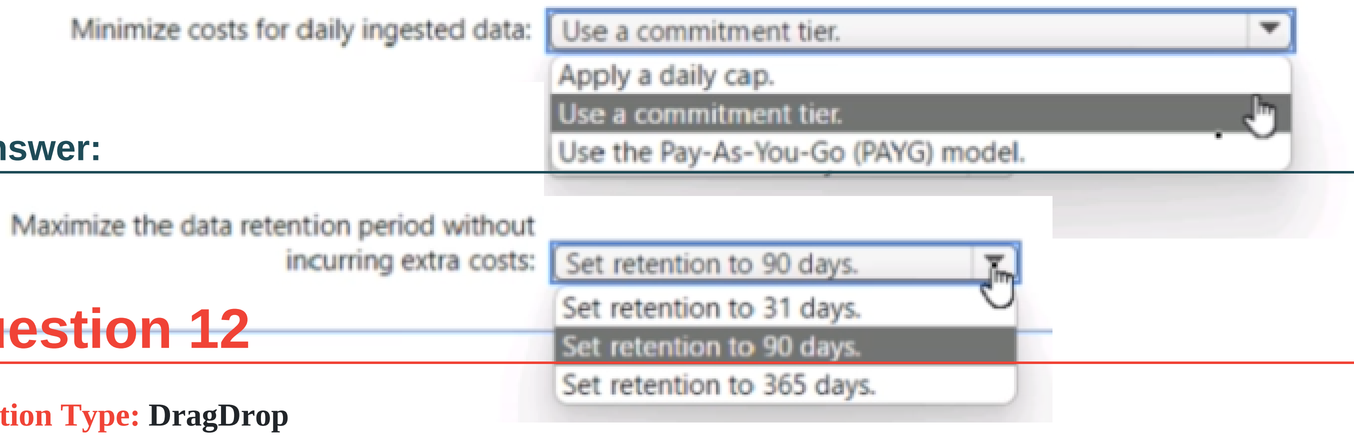
* Minimize costs for daily ingested data.

* Maximize the data retention period without incurring extra costs.

What should you do for each requirement? To answer, select the appropriate options in the answer are

a. NOTE Each correct selection is worth one point.

Answer:



Minimize costs for daily ingested data: Use a commitment tier.

- Apply a daily cap.
- Use a commitment tier.
- Use the Pay-As-You-Go (PAYG) model.

Maximize the data retention period without incurring extra costs: Set retention to 90 days.

- Set retention to 31 days.
- Set retention to 90 days.
- Set retention to 365 days.

Question 12

Question Type: **DragDrop**

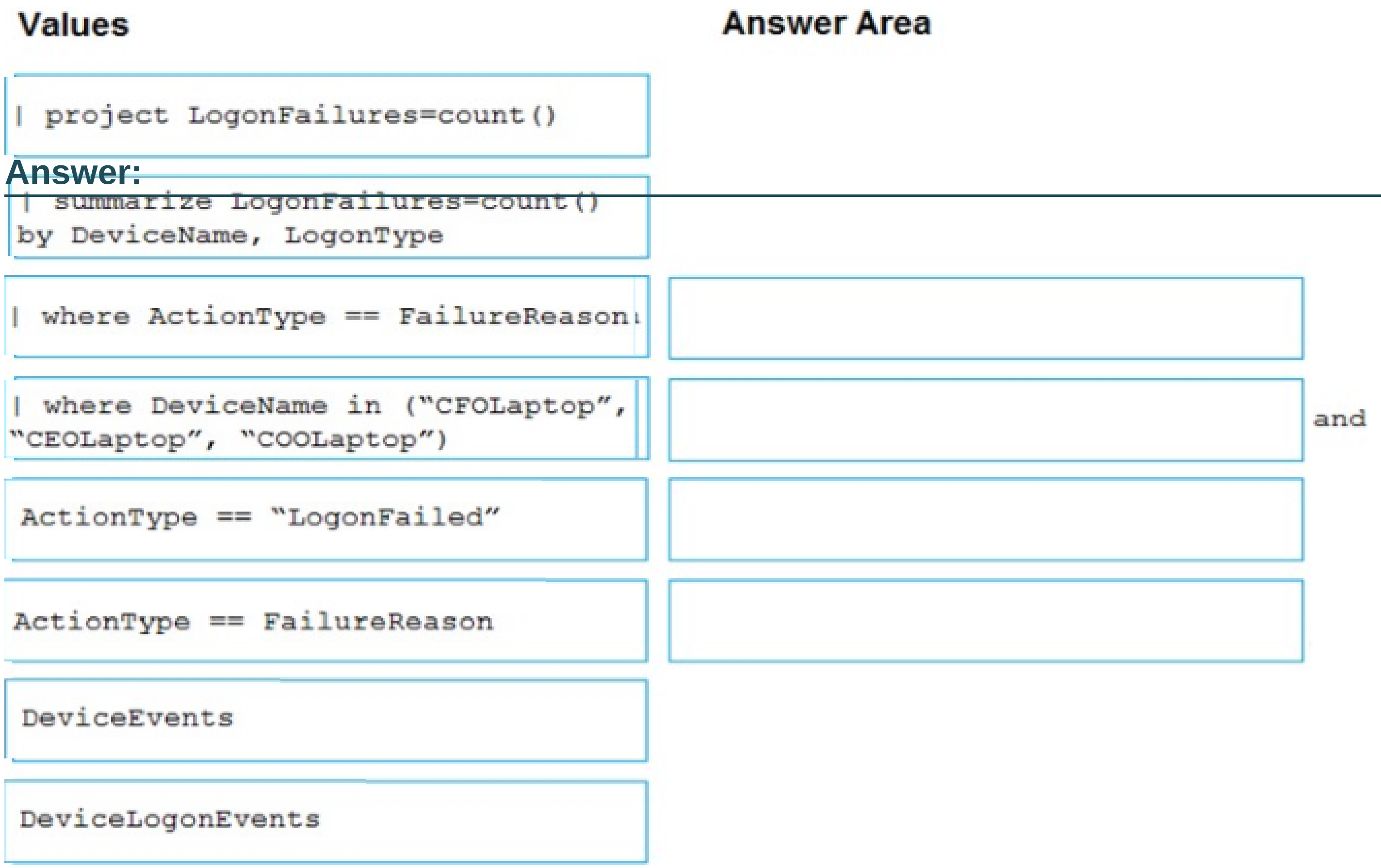
You are investigating an incident by using Microsoft 365 Defender.

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

Answer:



Values

```
| project LogonFailures=count()
```

```
| summarize LogonFailures=count()
by DeviceName, LogonType
```

```
| where ActionType == FailureReason
```

```
| where DeviceName in ("CFOLaptop",
"CEOLaptop", "COOLaptop")
```

```
ActionType == "LogonFailed"
```

```
ActionType == FailureReason
```

```
DeviceEvents
```

```
DeviceLogonEvents
```

Answer Area

and