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

Correct Answer: AD

QUESTION 16
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

Correct Answer: B
Explanation:
https://docs.microsoft.com/en-us/azure/sentinel/connect-azure-security-center

QUESTION 17
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.

```
let MaliciousEmails =
    [ EmailAttachementInfo ]
    [ EmailEvents         ]
    [ IdentityLogonEvents ]
| where MalwareFilterVerdict == "Malware"
| project TimeEmail = Timestamp, Subject, SenderFromAddress, AccountName =
tostring(split (RecipientEmailAddress, "@") [0]);

MaliciousEmails
| join (
    [ EmailAttachementInfo ]
    [ EmailEvents         ]
    [ IdentityLogonEvents ]
| project LogonTime = Timestamp, AccountName, DeviceName
) on AccountName
| where (LogonTime - TimeEmail) between (0min.. 60min)
|
    [ select 20 ]
    [ take 20   ]
    [ top 20    ]
```

Correct Answer:

```
let MaliciousEmails =
    [ EmailAttachementInfo ]
    [ EmailEvents         ]
    [ IdentityLogonEvents ]
| where MalwareFilterVerdict == "Malware"
| project TimeEmail = Timestamp, Subject, SenderFromAddress, AccountName =
tostring(split (RecipientEmailAddress, "@") [0]);

MaliciousEmails
| join (
    [ EmailAttachementInfo ]
    [ EmailEvents         ]
    [ IdentityLogonEvents ]
| project LogonTime = Timestamp, AccountName, DeviceName
) on AccountName
| where (LogonTime - TimeEmail) between (0min.. 60min)
|
    [ select 20 ]
    [ take 20   ]
    [ top 20    ]
```

QUESTION 18
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.

Correct Answer: BD
Explanation:

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

QUESTION 19
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.

Correct Answer: A
Explanation:
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.
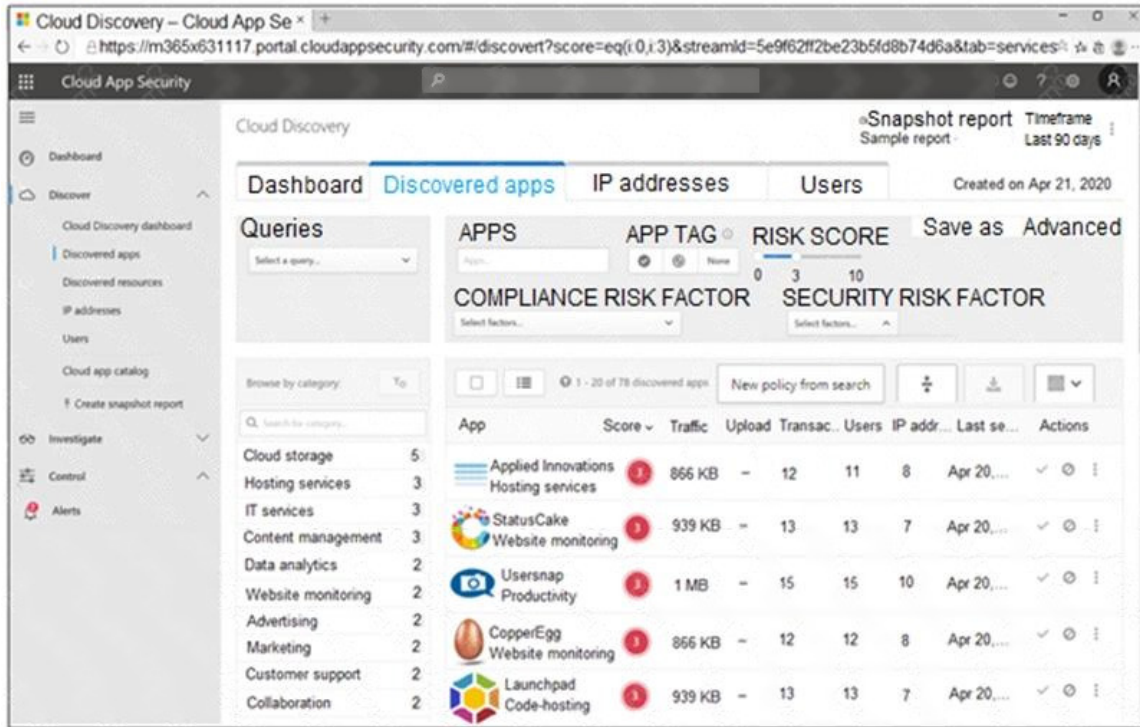
Reference:
https://docs.microsoft.com/en-us/azure/security-center/security-center-enable-data-collection

QUESTION 20
DRAG DROP
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

Correct Answer:

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

Select the app.

Tag the app as **Unsanctioned.**

Generate a block script.

Run the script on the source appliance.

QUESTION 21
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

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 |

Correct Answer: