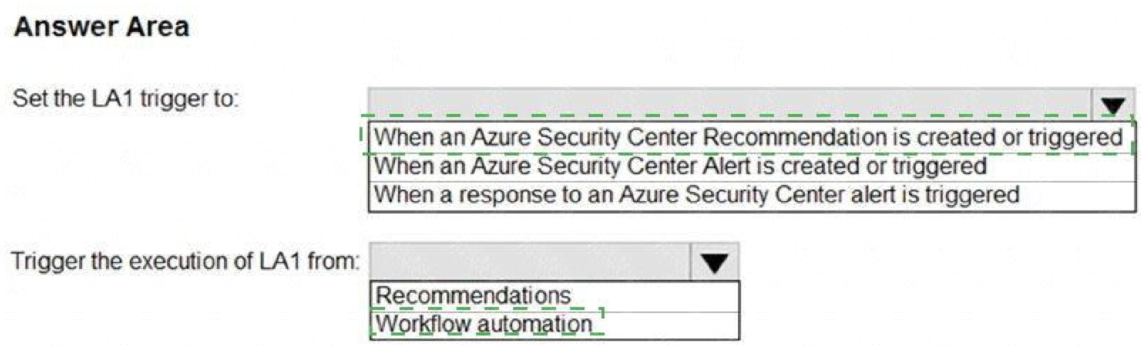


Answer Area

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

QUESTION 22
You have a Microsoft Sentinel workspace.

You need to prevent a built-in Advance Security information Model (ASIM) parse from being updated automatically.

What are two ways to achieve this goal? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

A. Redeploy the built-in parse and specify a CallerContext parameter of any and a SourceSpecificParse parameter of any.
B. Create a hunting query that references the built-in parse.
C. Redeploy the built-in parse and specify a CallerContext parameter of built-in.
D. Build a custom unify parse and include the build- parse version
E. Create an analytics rule that includes the built-in parse

Correct Answer: AD

QUESTION 23
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.

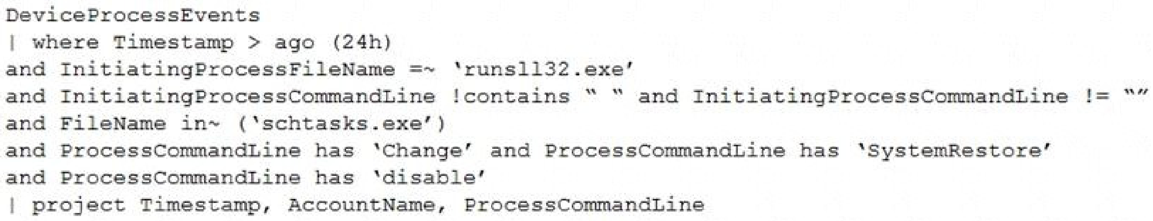
What is a possible cause of the issue?

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.

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

QUESTION 24

You have the following advanced hunting query in Microsoft 365 Defender.



```
DeviceProcessEvents
| where Timestamp > ago (24h)
and InitiatingProcessFileName =~ 'runsll32.exe'
and InitiatingProcessCommandLine !contains " " and InitiatingProcessCommandLine != ""
and FileName in~ ('schtasks.exe')
and ProcessCommandLine has 'Change' and ProcessCommandLine has 'SystemRestore'
and ProcessCommandLine has 'disable'
| project Timestamp, AccountName, ProcessCommandLine
```

You need to receive an alert when any process disables System Restore on a device managed by Microsoft Defender during the last 24 hours.

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 detection rule.
B. Create a suppression rule.
C. Add | order by Timestamp to the query.
D. Replace DeviceProcessEvents with DeviceNetworkEvents.
E. Add DeviceId and ReportId to the output of the query.

Correct Answer: AE
Explanation:
https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/custom-detection- rules

QUESTION 25
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

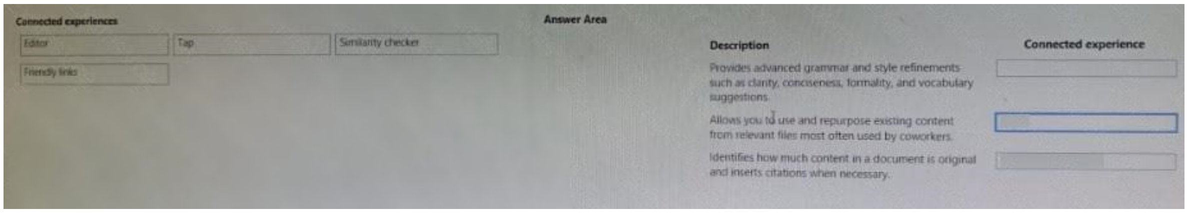
Correct Answer: B
Explanation:
https://docs.microsoft.com/en-us/azure/defender-for-cloud/quickstart-onboard-machines?pivots=azure-arc

QUESTION 26
DRAG DROP
A company wants to analyze by using Microsoft 365 Apps.

You need to describe the connected experiences the company can use.

Which connected experiences should you describe? To answer, drag the appropriate connected experiences to the correct description. Each connected experience may be used once, more than once, or not at all. You may need to drag the split between panes or scroll to view content.

NOTE: Each correct selection is worth one point.



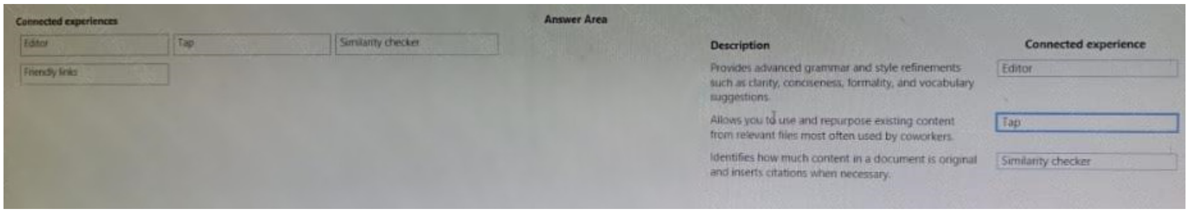
Connected experiences

Editor
Tap
Similarity checker
Friendly links

Answer Area

Description	Connected experience
Provides advanced grammar and style refinements such as clarity, conciseness, formality, and vocabulary suggestions.	
Allows you to use and repurpose existing content from relevant files most often used by coworkers.	
Identifies how much content in a document is original and inserts citations when necessary.	

Correct Answer:



Connected experiences

Editor
Tap
Similarity checker
Friendly links

Answer Area

Description	Connected experience
Provides advanced grammar and style refinements such as clarity, conciseness, formality, and vocabulary suggestions.	Editor
Allows you to use and repurpose existing content from relevant files most often used by coworkers.	Tap
Identifies how much content in a document is original and inserts citations when necessary.	Similarity checker

QUESTION 27
You have a Microsoft Sentinel workspace that contains the following incident.

Brute force attack against Azure Portal analytics rule has been triggered.

You need to identify the geolocation information that corresponds to the incident.

What should you do?

A. From Overview, review the Potential malicious events map.
B. From Incidents, review the details of the iPCustomEntity entity associated with the incident.
C. From Incidents, review the details of the AccouncCuscomEntity entity associated with the incident.
D. From Investigation, review insights on the incident entity.

Correct Answer: A
Explanation:
Potential malicious events: When traffic is detected from sources that are known to be malicious, Microsoft Sentinel alerts you on the map. If you see orange, it is inbound traffic: someone is trying to access your organization from a known malicious IP address. If you see Outbound (red) activity, it means that data from your network is being streamed out of your organization to a known malicious IP address.

QUESTION 28
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

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

QUESTION 29
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?

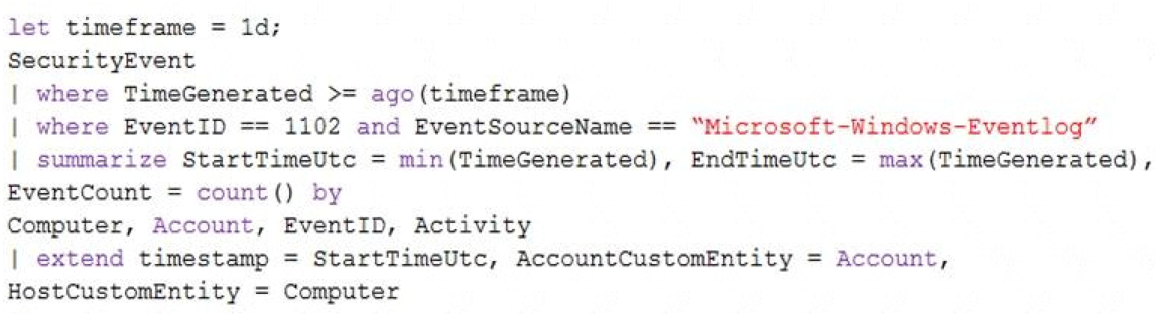
A. SharePoint search
B. a hunting query in Microsoft 365 Defender
C. Azure Information Protection
D. RegEx pattern matching

Correct Answer: C
Explanation:
https://docs.microsoft.com/en-us/azure/information-protection/what-is-information-protection

QUESTION 30
You provision Azure Sentinel for a new Azure subscription. You are configuring the Security Events connector.

While creating a new rule from a template in the connector, you decide to generate a new alert for every event.

You create the following rule query.



```
let timeframe = 1d;
SecurityEvent
| where TimeGenerated >= ago(timeframe)
| where EventID == 1102 and EventSourceName == "Microsoft-Windows-Eventlog"
| summarize StartTimeUtc = min(TimeGenerated), EndTimeUtc = max(TimeGenerated),
EventCount = count() by
Computer, Account, EventID, Activity
| extend timestamp = StartTimeUtc, AccountCustomEntity = Account,
HostCustomEntity = Computer
```

By which two components can you group alerts into incidents? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

A. user
B. resource group
C. IP address
D. computer

Correct Answer: AD

QUESTION 31
You receive an alert from Azure Defender for Key Vault.

You discover that the alert is generated from multiple suspicious IP addresses.

You need to reduce the potential of Key Vault secrets being leaked while you investigate the issue. The solution must be implemented as soon as possible and must minimize the impact on legitimate users.

What should you do first?

A. Modify the access control settings for the key vault.
B. Enable the Key Vault firewall.
C. Create an application security group.
D. Modify the access policy for the key vault.

Correct Answer: B
Explanation:
https://docs.microsoft.com/en-us/azure/security-center/defender-for-key-vault-usage

QUESTION 32
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

Correct Answer: B
Explanation:
https://docs.microsoft.com/en-us/azure/security-center/security-center-managing-and-responding-