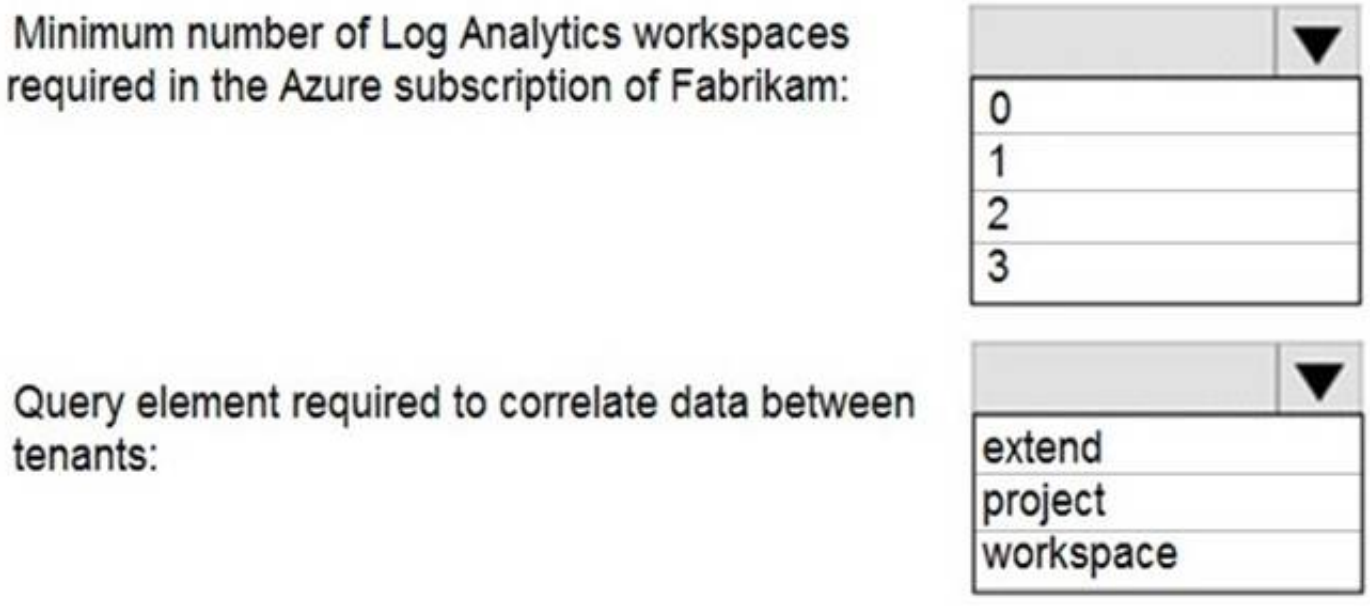
# Exam Questions SC-200

Microsoft Security Operations Analyst

**https://www.2passeasy.com/dumps/SC-200/**

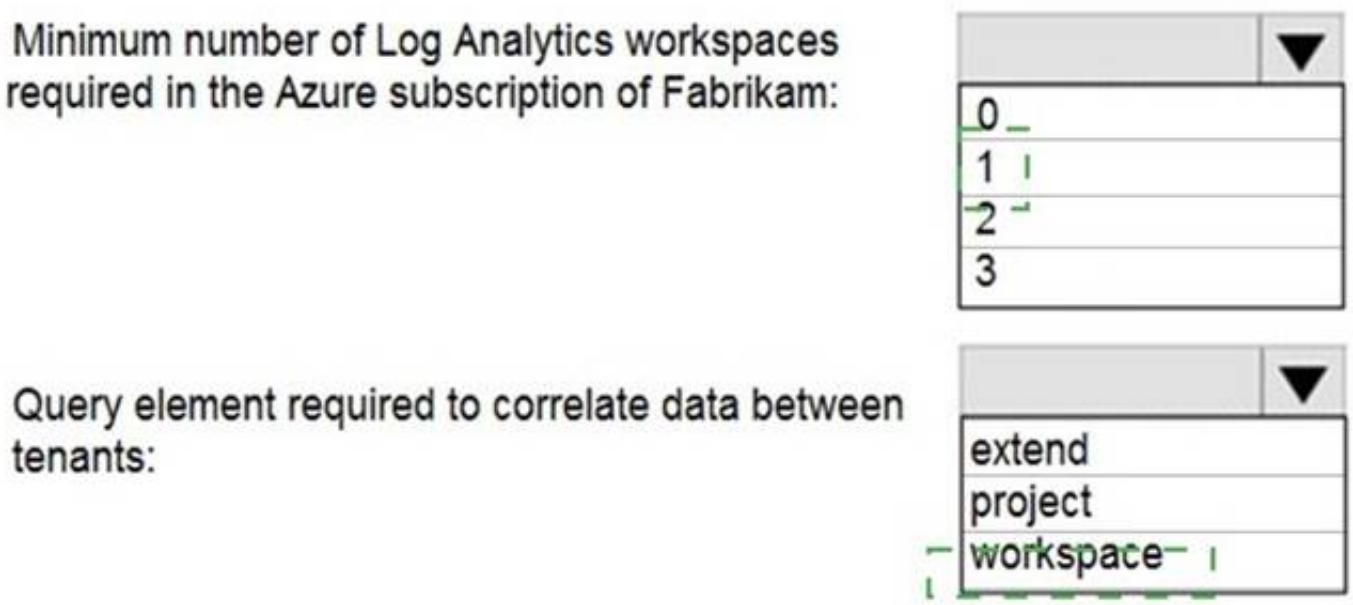
**NEW QUESTION 1**
HOTSPOT - (Topic 1)
You need to implement Azure Sentinel queries for Contoso and Fabrikam to meet the technical requirements.
What should you include in the solution? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.




A. Mastered
B. Not Mastered

**Answer:** A

**Explanation:**




**NEW QUESTION 2**
- (Topic 1)
You need to remediate active attacks to meet the technical requirements. What should you include in the solution?

A. Azure Automation runbooks
B. Azure Logic Apps
C. Azure FunctionsD Azure Sentinel livestreams

**Answer:** B

**Explanation:**
Reference:
https://docs.microsoft.com/en-us/azure/sentinel/automate-responses-with-playbooks

**NEW QUESTION 3**
- (Topic 1)
The issue for which team can be resolved by using Microsoft Defender for Office 365?

A. executive
B. marketing
C. security
D. sales

**Answer:** B

**Explanation:**
Reference:
https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/atp-for-spo-odb- and-teams? view=o365-worldwide

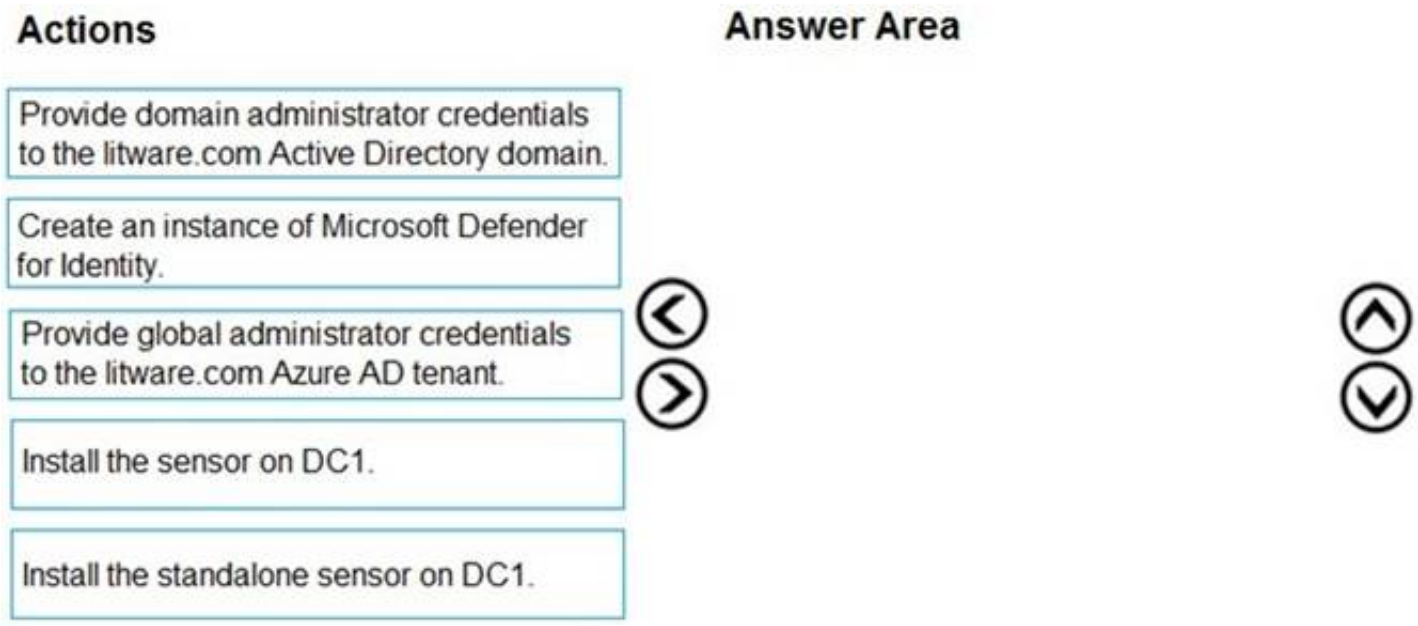
**NEW QUESTION 4**
- (Topic 1)
You need to recommend a solution to meet the technical requirements for the Azure virtual machines. What should you include in the recommendation?

A. just-in-time (JIT) access
B. Azure Defender
C. Azure Firewall
D. Azure Application Gateway

**Answer:** B

**Explanation:**
Reference:
https://docs.microsoft.com/en-us/azure/security-center/azure-defender

**NEW QUESTION 5**
DRAG DROP - (Topic 2)
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.




A. Mastered
B. Not Mastered

**Answer:** A

**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.

**NEW QUESTION 6**
- (Topic 2)
You need to assign a role-based access control (RBAC) role to admin1 to meet the Azure Sentinel requirements and the business requirements.
Which role should you assign?

A. Automation Operator
B. Automation Runbook Operator
C. Azure Sentinel Contributor
D. Logic App Contributor

**Answer:** C

**Explanation:**
Reference:
https://docs.microsoft.com/en-us/azure/sentinel/roles

**NEW QUESTION 7**
- (Topic 3)
You need to ensure that the Group1 members can meet the Microsoft Sentinel requirements.
Which role should you assign to Group1?

A. Microsoft Sentinel Automation Contributor
B. Logic App Contributor
C. Automation Operator
D. Microsoft Sentinel Playbook Operator

**Answer:** D

**NEW QUESTION 8**
HOTSPOT - (Topic 3)
You need to monitor the password resets. The solution must meet the Microsoft Sentinel requirements.
What should you do? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

**Answer Area**


A. Mastered
B. Not Mastered

**Answer:** A

**Explanation:**

**Answer Area**


**NEW QUESTION 9**
- (Topic 4)
Your company uses Azure Sentinel.
A new security analyst reports that she cannot assign and dismiss incidents in Azure Sentinel. You need to resolve the issue for the analyst. The solution must use the principle of least privilege. Which role should you assign to the analyst?

A. Azure Sentinel Responder
B. Logic App Contributor
C. Azure Sentinel Contributor
D. Azure Sentinel Reader

**Answer:** A

**Explanation:**
Reference:
https://docs.microsoft.com/en-us/azure/sentinel/roles

**NEW QUESTION 10**
- (Topic 4)
You use Microsoft Sentinel.
You need to receive an alert in near real-time 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 bookmark.
B. Create an analytics rule.
C. Create a livestream.
D. Create a hunting query.
E. Add a data connector.

**Answer:** DE

**NEW QUESTION 10**
- (Topic 4)
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

**Answer:** B

**Explanation:**
Reference:
https://docs.microsoft.com/en-us/azure/sentinel/connect-azure-security-center

**NEW QUESTION 14**
- (Topic 4)
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.

**Answer:** B

**Explanation:**

Reference:
https://docs.microsoft.com/en-us/azure/security-center/defender-for-key-vault-usage

**NEW QUESTION 19**
- (Topic 4)
You have the following environment:
? Azure Sentinel
? A Microsoft 365 subscription
? Microsoft Defender for Identity
? An Azure Active Directory (Azure AD) tenant
You configure Azure Sentinel to collect security logs from all the Active Directory member servers and domain controllers.
You deploy Microsoft Defender for Identity by using standalone sensors.
You need to ensure that you can detect when sensitive groups are modified in Active Directory.
Which two actions should you perform? Each correct answer presents part of the solution. NOTE: Each correct selection is worth one point.

A. Configure the Advanced Audit Policy Configuration settings for the domain controllers.
B. Modify the permissions of the Domain Controllers organizational unit (OU).
C. Configure auditing in the Microsoft 365 compliance center.
D. Configure Windows Event Forwarding on the domain controllers.

**Answer:** AD

**Explanation:**
Reference:
https://docs.microsoft.com/en-us/defender-for-identity/configure-windows-event-collection https://docs.microsoft.com/en-us/defender-for-identity/configure-event-collection

**NEW QUESTION 21**
- (Topic 4)
You have an Azure subscription that has Microsoft Defender for Cloud enabled.
You have a virtual machine that runs Windows 10 and has the Log Analytics agent installed.
You need to simulate an attack on the virtual machine that will generate an alert. What should you do first?

A. Run the Log Analytics Troubleshooting Tool.
B. Copy a executable and rename the file as ASC_AlerTest_662jf10N,exe
C. Modify the settings of the Microsoft Monitoring Agent.
D. Run the MMASetup executable and specify the -foo argument

**Answer:** B

**NEW QUESTION 22**
- (Topic 4)
You have two Azure subscriptions that use Microsoft Defender for Cloud.
You need to ensure that specific Defender for Cloud security alerts are suppressed at the root management group level. The solution must minimize administrative effort.
What should you do in the Azure portal?

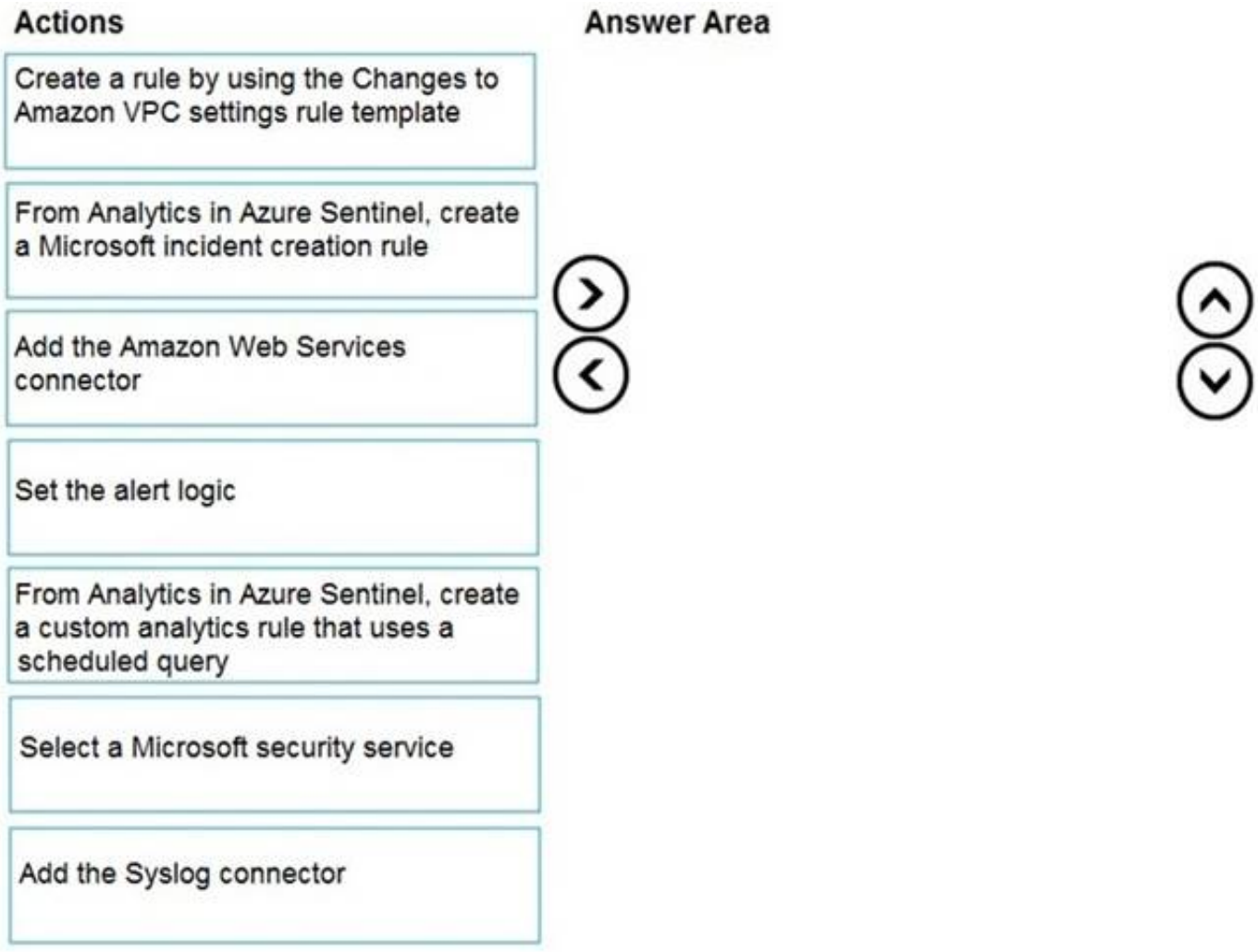
A. Create an Azure Policy assignment.
B. Modify the Workload protections settings in Defender for Cloud.
C. Create an alert rule in Azure Monitor.
D. Modify the alert settings in Defender for Cloud.

**Answer:** D

**Explanation:**
You can use alerts suppression rules to suppress false positives or other unwanted

security alerts from Defender for Cloud.
Note: To create a rule directly in the Azure portal:
* 1. From Defender for Cloud's security alerts page:
Select the specific alert you don't want to see anymore, and from the details pane, select Take action.
Or, select the suppression rules link at the top of the page, and from the suppression rules page select Create new suppression rule:
* 2. In the new suppression rule pane, enter the details of your new rule.
Your rule can dismiss the alert on all resources so you don't get any alerts like this one in the future.
Your rule can dismiss the alert on specific criteria - when it relates to a specific IP address, process name, user account, Azure resource, or location.
* 3. Enter details of the rule.
* 4. Save the rule.
Reference: https://docs.microsoft.com/en-us/azure/defender-for-cloud/alerts-suppression- rules

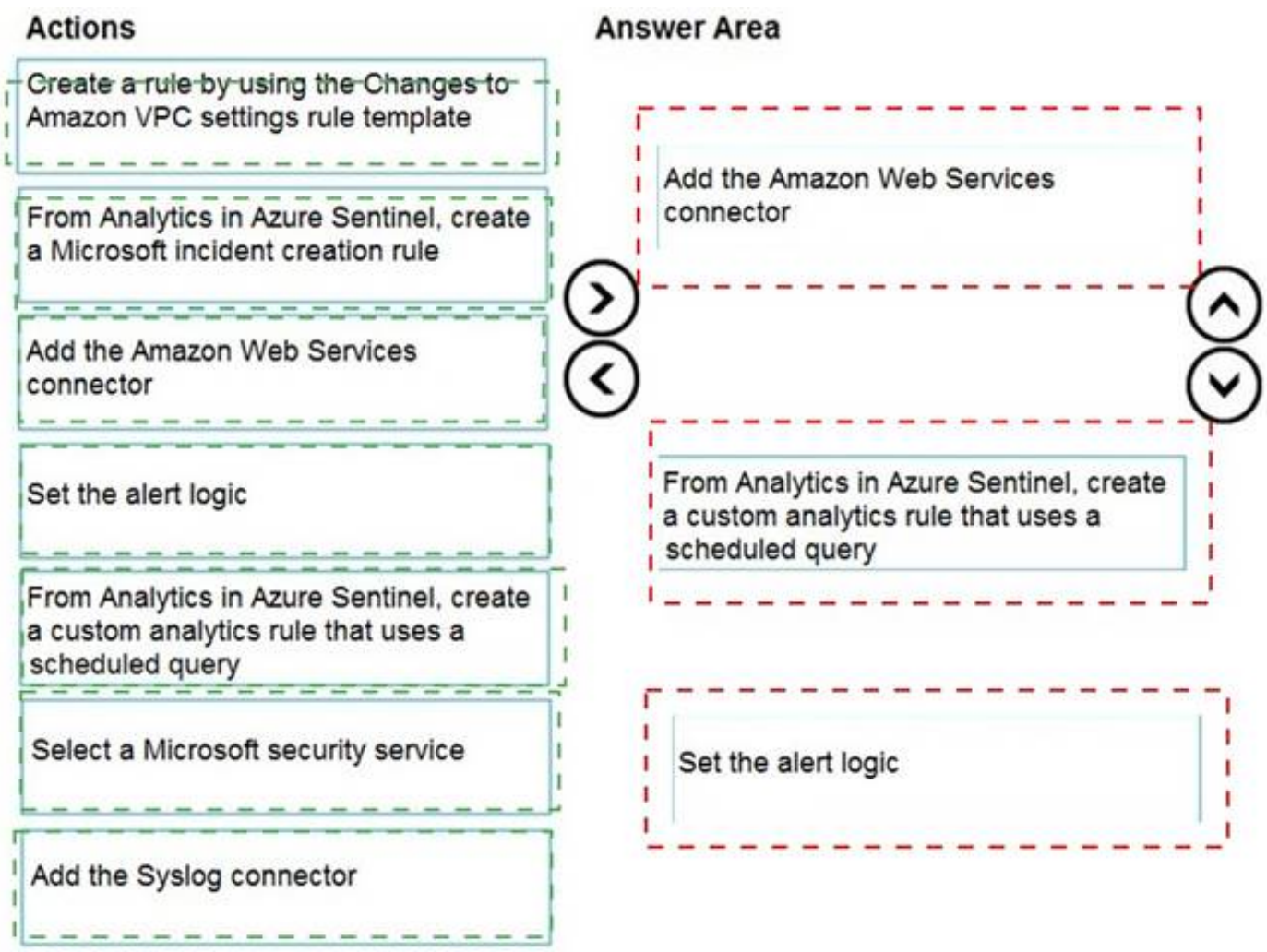
**NEW QUESTION 23**
DRAG DROP - (Topic 4)
You need to use an Azure Sentinel analytics rule to search for specific criteria in Amazon Web Services (AWS) logs and to generate incidents.
Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.
a Microsoft 365 E5




A. Mastered
B. Not Mastered

**Answer:** A

**Explanation:**




**NEW QUESTION 28**
- (Topic 4)
You create a hunting query in Azure Sentinel.
You need to receive a notification in the Azure portal as soon as the hunting query detects a match on the query. The solution must minimize effort.
What should you use?

A. a playbook
B. a notebook
C. a livestream
D. a bookmark

**Answer:** C

**Explanation:**
Use livestream to run a specific query constantly, presenting results as they come in.
Reference:
https://docs.microsoft.com/en-us/azure/sentinel/hunting

**NEW QUESTION 30**
- (Topic 4)
You plan to create a custom Azure Sentinel query that will provide a visual representation of the security alerts generated by Azure Security Center.
You need to create a query that will be used to display a bar graph. What should you include in the query?

A. extend
B. bin
C. count
D. workspace

**Answer:** B

**Explanation:**
Reference:
https://docs.microsoft.com/en-us/azure/azure-monitor/visualize/workbooks-chart- visualizations

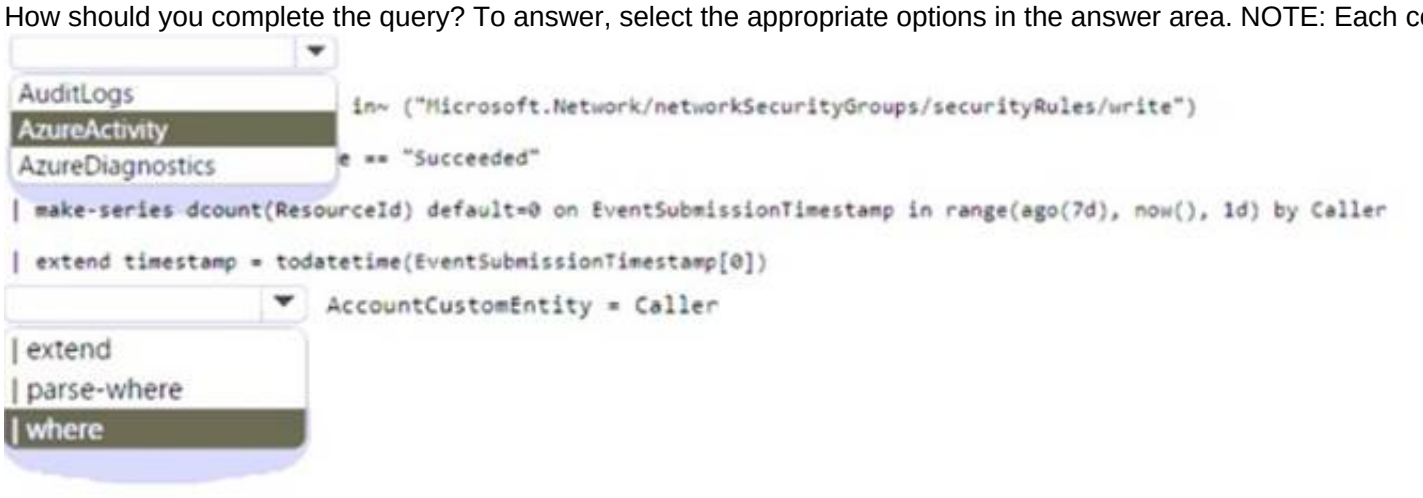
**NEW QUESTION 34**
- (Topic 4)
You need to correlate data from the SecurityEvent Log Anarytks table to meet the Microsoft Sentinel requirements for using UEBA. Which Log Analytics table should you use?

A. SentwlAuoNt
B. AADRiskyUsers
C. IdentityOirectoryEvents
D. Identityinfo

**Answer:** C

**NEW QUESTION 39**

HOTSPOT - (Topic 4)
You have an Azure subscription that contains an Microsoft Sentinel workspace.
You need to create a hunting query using Kusto Query Language (KQL) that meets the following requirements:
• Identifies an anomalous number of changes to the rules of a network security group (NSG) made by the same security principal
• Automatically associates the security principal with an Microsoft Sentinel entity
How should you complete the query? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.




A. Mastered
B. Not Mastered

**Answer:** A

**Explanation:**


**NEW QUESTION 43**
HOTSPOT - (Topic 4)
You have a custom detection rule that includes the following KQL query.

```
AlertInfo
| where Severity == "High"
| distinct AlertId
| join AlertEvidence on AlertId
| where EntityType in ("User", "Mailbox")
| where EvidenceRole == "Impacted"
| summarize by Timestamp, AlertId, AccountName, AccountObjectId, EntityType, DeviceId, SHA256
| join EmailEvents on $left.AccountObjectId == $right.RecipientObjectId
| where DeliveryAction == "Delivered"
| summarize by Timestamp, AlertId, ReportId, RecipientObjectId, RecipientEmailAddress, EntityType, DeviceId, SHA256
```

For each of the following statements, select Yes if True. Otherwise select No. NOTE: Each correct selection is worth one point.

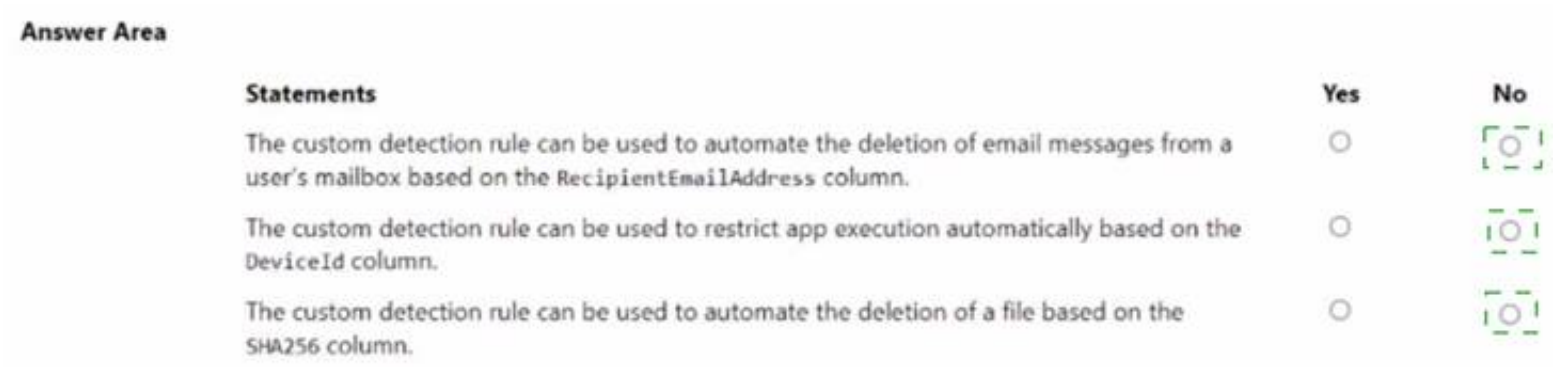
**Answer Area**

| Statements | Yes | No |
|---|---|---|
| The custom detection rule can be used to automate the deletion of email messages from a user's mailbox based on the `RecipientEmailAddress` column. | ○ | ○ |
| The custom detection rule can be used to restrict app execution automatically based on the `DeviceId` column. | ○ | ○ |
| The custom detection rule can be used to automate the deletion of a file based on the `SHA256` column. | ○ | ○ |

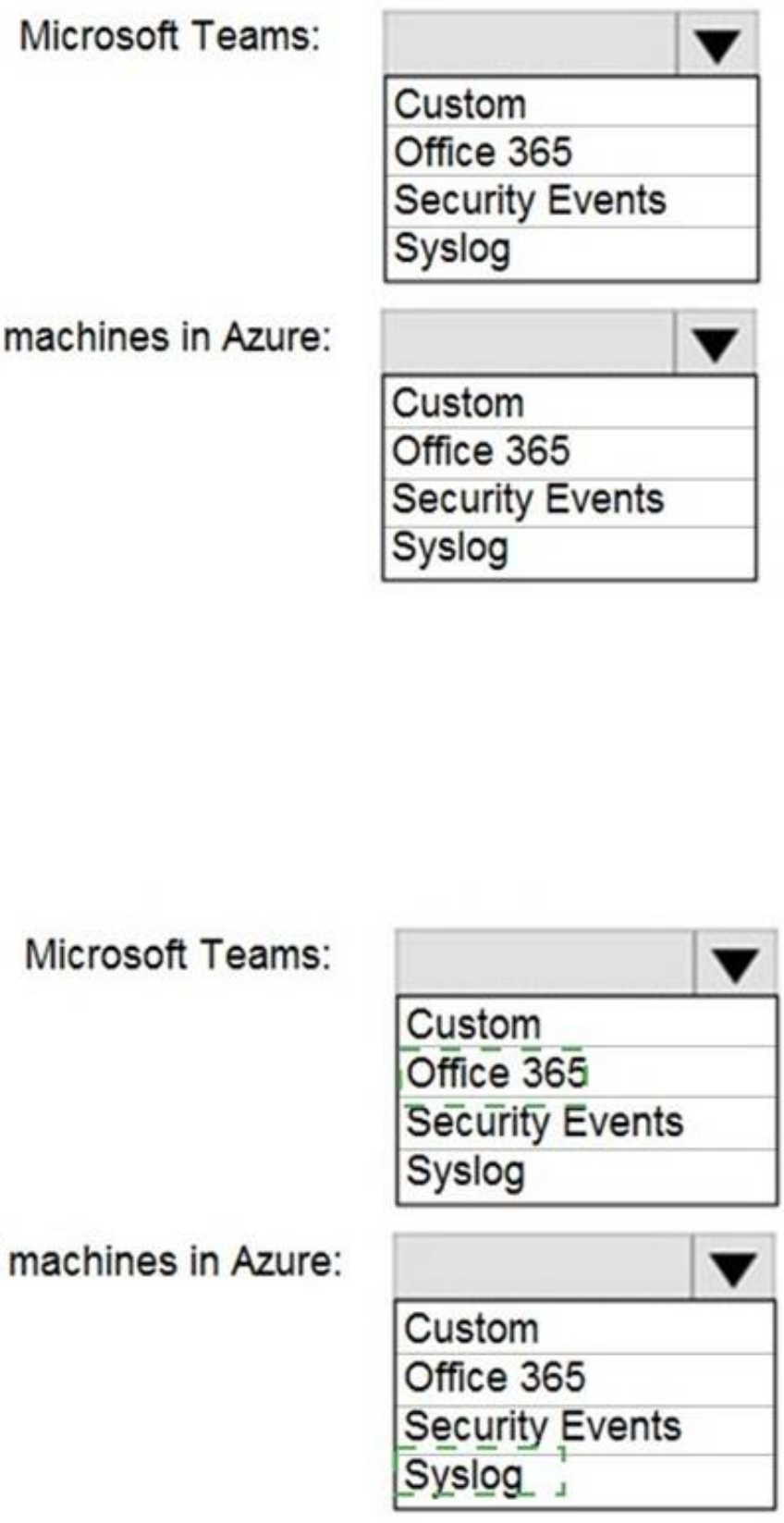
A. Mastered
B. Not Mastered

**Answer:** A

**Explanation:**




**NEW QUESTION 45**
HOTSPOT - (Topic 4)
You deploy Azure Sentinel.
You need to implement connectors in Azure Sentinel to monitor Microsoft Teams and Linux virtual machines in Azure. The solution must minimize administrative effort.
Which data connector type should you use for each workload? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.




A. Mastered
B. Not Mastered

**Answer:** A

**Explanation:**




**NEW QUESTION 48**
- (Topic 4)
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?

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

**NEW QUESTION 51**
- (Topic 4)
You create an Azure subscription named sub1.
In sub1, you create a Log Analytics workspace named workspace1.
You enable Azure Security Center and configure Security Center to use workspace1.
You need to ensure that Security Center processes events from the Azure virtual machines that report to workspace1.
What should you do?

A. In workspace1, install a solution.
B. In sub1, register a provider.
C. From Security Center, create a Workflow automation.
D. In workspace1, create a workbook.

**Answer:** A

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

**NEW QUESTION 56**
- (Topic 4)
Your company has a single office in Istanbul and a Microsoft 365 subscription.
The company plans to use conditional access policies to enforce multi-factor authentication (MFA).
You need to enforce MFA for all users who work remotely. What should you include in the solution?

A. a fraud alert
B. a user risk policy
C. a named location
D. a sign-in user policy

**Answer:** C

**Explanation:**
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/location- condition

**NEW QUESTION 58**
- (Topic 4)
You have a Microsoft 365 E5 subscription that contains 100 Linux devices. The devices are onboarded to Microsoft Defender 365. You need to initiate the collection of investigation packages from the devices by using the Microsoft 365 Defender portal. Which response action should you use?

A. Run antivirus scan
B. Initiate Automated Investigation
C. Collect investigation package
D. Initiate Live Response Session

**Answer:** D

**NEW QUESTION 60**
- (Topic 4)
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 Microsoft Defender for Identity integration with Active Directory.
From the Microsoft Defender for identity portal, you need to configure several accounts for attackers to exploit.
Solution: From Entity tags, you add the accounts as Honeytoken accounts. Does this meet the goal?

A. Yes
B. No

**Answer:** A

**Explanation:**
Reference:
https://docs.microsoft.com/en-us/defender-for-identity/manage-sensitive-honeytoken- accounts

**NEW QUESTION 63**
- (Topic 4)
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?

A. the risk detections report
B. the risky users report
C. Identity Secure Score recommendations
D. the risky sign-ins report

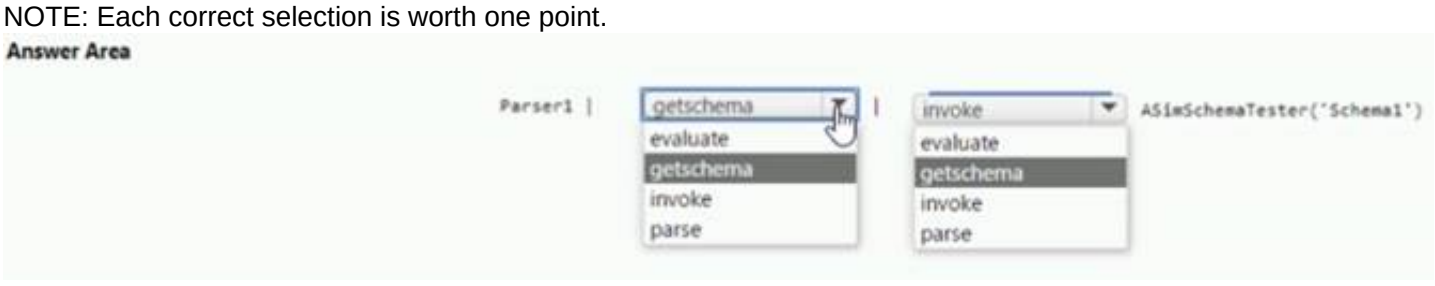
**Answer:** B

**NEW QUESTION 65**
- (Topic 4)
You have a Microsoft Sentinel workspace that uses the Microsoft 365 Defender data connector.
From Microsoft Sentinel, you investigate a Microsoft 365 incident.
You need to update the incident to include an alert generated by Microsoft Defender for Cloud Apps.
What should you use?

A. the entity side panel of the Timeline card in Microsoft Sentinel
B. the investigation graph on the Incidents page of Microsoft Sentinel
C. the Timeline tab on the Incidents page of Microsoft Sentinel
D. the Alerts page in the Microsoft 365 Defender portal

**Answer:** A

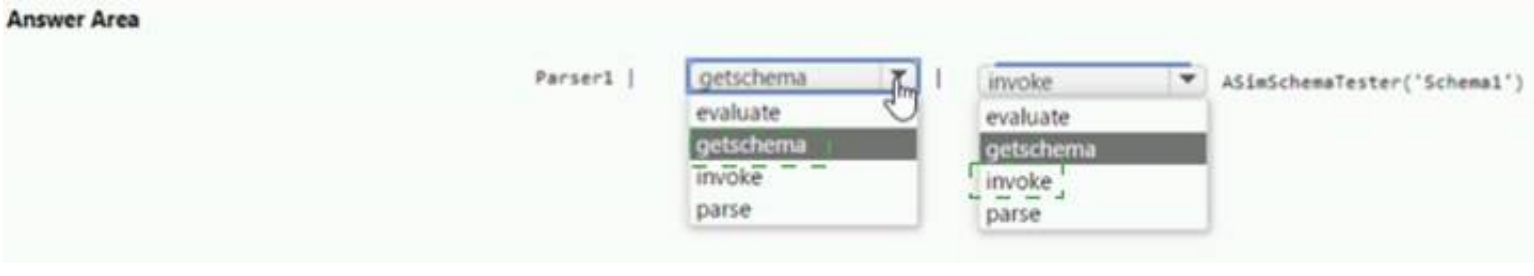
**NEW QUESTION 69**
HOTSPOT - (Topic 4)
You have a Microsoft Sentinel workspace
You develop a custom Advanced Security information Model (ASIM) parser named Parser1 that produces a schema named Schema1.
You need to validate Schema1.
How should you complete the command? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.




A. Mastered
B. Not Mastered

**Answer:** A

**Explanation:**



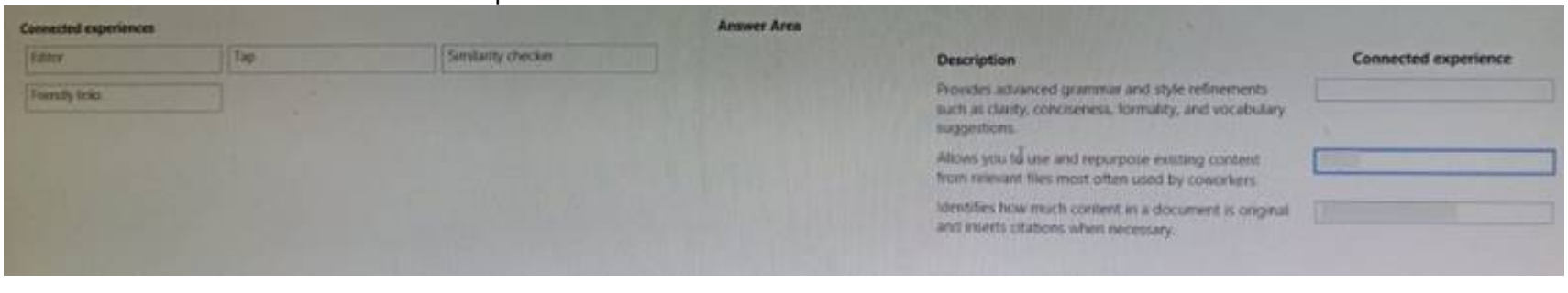

**NEW QUESTION 71**
- (Topic 4)
You create an Azure subscription.
You enable Microsoft Defender for Cloud for the subscription.
You need to use Defender for Cloud to protect on-premises computers. What should you do on the on-premises computers?

A. Configure the Hybrid Runbook Worker role.
B. Install the Connected Machine agent.
C. Install the Log Analytics agent
D. Install the Dependency agent.

**Answer:** C

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

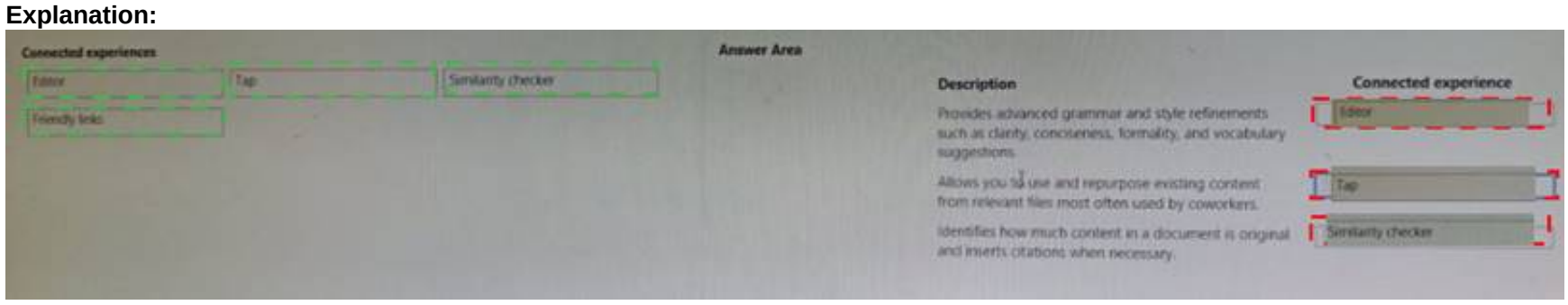
**NEW QUESTION 74**
DRAG DROP - (Topic 4)
A company wants to analyze by using Microsoft 365 Apps.
You need to describe the connected experiences the company can use.
Which connected experiences should you describe? To answer, drag the appropriate connected experiences to the correct description. Each 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.



A. Mastered
B. Not Mastered

**Answer:** A

**Explanation:**




**NEW QUESTION 79**
HOTSPOT - (Topic 4)
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 area. NOTE: Each correct selection is worth one point.


A. Mastered
B. Not Mastered

**Answer:** A

**Explanation:**


**NEW QUESTION 83**
- (Topic 4)
You have a Microsoft 365 E5 subscription that uses Microsoft Defender for Endpoint
You need to create a query that will link the AlertInfo, AlertEvidence, and DeviceLogonEvents tables. The solution must return all the rows in the tables.
Which operator should you use?

A. join kind = inner
B. evaluate hin
C. Remote =
D. search *
E. union kind = inner

**Answer:** A

**NEW QUESTION 88**

HOTSPOT - (Topic 4)
You have the following KQL query.

```
let IPList = _GetWatchlist('Bad_IPs');
Event
  | where Source == "Microsoft-Windows-Sysmon"
  | where EventID == 3
  | extend EvData = parse_xml(EventData)
  | extend EventDetail = EvData.DataItem.EventData.Data
  | extend SourceIP = EventDetail.[9].["#text"], DestinationIP = EventDetail.[14].["#text"]
  | where SourceIP in (IPList) or DestinationIP in (IPList)
  | extend IPMatch = case( SourceIP in (IPList), "SourceIP", DestinationIP in (IPList), "DestinationIP", "None")
  | extend timestamp = TimeGenerated, AccountCustomEntity = UserName, HostCustomEntity = Computer, '
```

| Statements | Yes | No |
|---|---|---|
| The `UserName` field is set as the account entity. | ○ | ○ |
| The watchlist cannot be updated after it is created. | ○ | ○ |
| The `IPList` variable is set as the IP address entity. | ○ | ○ |

A. Mastered
B. Not Mastered

**Answer:** A

**Explanation:**

| Statements | Yes | No |
|---|---|---|
| The `UserName` field is set as the account entity. | ○ | ○ |
| The watchlist cannot be updated after it is created. | ○ | ○ |
| The `IPList` variable is set as the IP address entity. | ○ | ○ |

**NEW QUESTION 90**
- (Topic 4)
You have an Azure subscription that uses resource type for Cloud. You need to filter the security alerts view to show the following alerts:
• Unusual user accessed a key vault
• Log on from an unusual location
• Impossible travel activity Which severity should you use?

A. Informational
B. Low
C. Medium
D. High

**Answer:** C

**NEW QUESTION 94**
- (Topic 4)
You have a Microsoft Sentinel workspace named Workspaces
You need to exclude a built-in. source-specific Advanced Security Information Model (ASIM) parser from a built-in unified ASIM parser.
What should you create in Workspace1?

A. a workbook
B. a hunting query
C. a watchlist
D. an analytic rule

**Answer:** D

**Explanation:**
To exclude a built-in, source-specific Advanced Security Information Model (ASIM) parser from a built-in unified ASIM parser, you should create an analytic rule in the Microsoft Sentinel workspace. An analytic rule allows you to customize the behavior of the unified ASIM parser and exclude specific source-specific parsers from being used.
Reference: https://docs.microsoft.com/en-us/azure/sentinel/analytics-create-analytic-rule

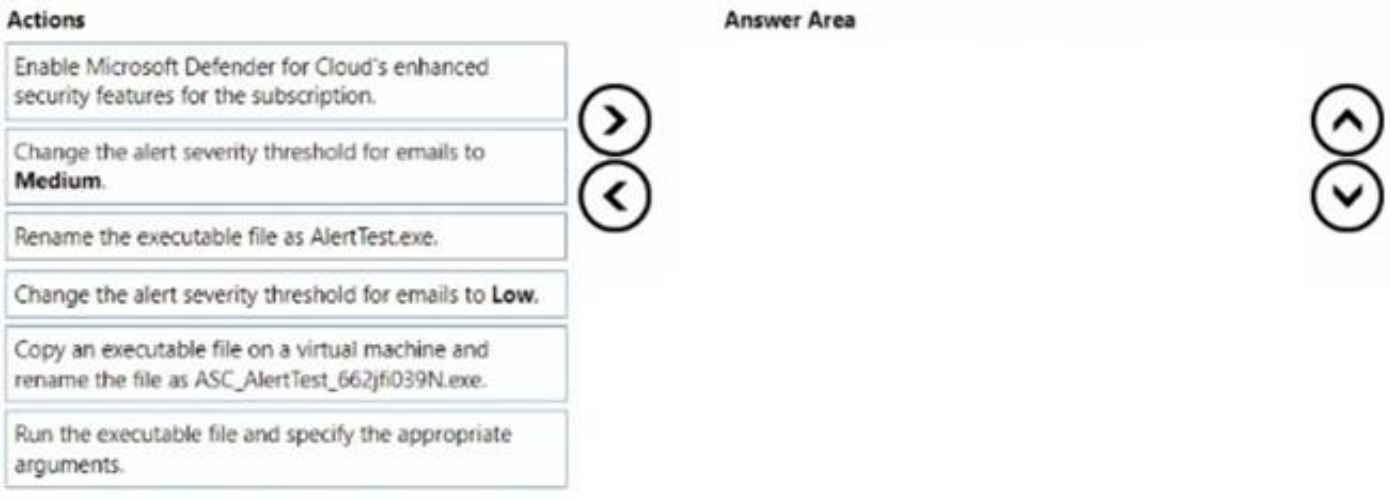
**NEW QUESTION 96**
- (Topic 4)
You have a suppression rule in Azure Security Center for 10 virtual machines that are used for testing. The virtual machines run Windows Server.
You are troubleshooting an issue on the virtual machines.
In Security Center, you need to view the alerts generated by the virtual machines during the last five days.
What should you do?

A. Change the rule expiration date of the suppression rule.
B. Change the state of the suppression rule to Disabled.
C. Modify the filter for the Security alerts page.
D. View the Windows event logs on the virtual machines.

**Answer:** B

**Explanation:**
Reference:
https://docs.microsoft.com/en-us/azure/security-center/alerts-suppression-rules

**NEW QUESTION 97**
DRAG DROP - (Topic 4)
You create a new Azure subscription and start collecting logs for Azure Monitor.
You need to validate that Microsoft Defender for Cloud will trigger an alert when a malicious file is present on an Azure virtual machine running Windows Server.
Which three actions should you perform in a sequence? To answer, move the appropriate actions from the list of action to the answer area and arrange them in the correct order.
NOTE: More than one order of answer choices is correct. You will receive credit for any of the correct orders you select.




A. Mastered
B. Not Mastered

**Answer:** A

**Explanation:**
To validate that Microsoft Defender for Cloud will trigger an alert when a malicious file is present on an Azure virtual machine running Windows Server, you should perform the following three actions in sequence:
? Copy an executable file on a virtual machine and rename the file as ASC_AlertTest_662jfi039N.exe
? Run the executable file and specify the appropriate arguments
? Enable Microsoft Defender for Cloud's enhanced security features for the subscription.
These actions will simulate a malicious activity on the virtual machine and generate an alert in Defender for Cloud. You can then verify the alert details and response recommendations in the Azure portal. For more information, see Alert validation - Microsoft Defender for Cloud.

**NEW QUESTION 101**
- (Topic 4)
Your company uses Microsoft Sentinel
A new security analyst reports that she cannot assign and resolve incidents in Microsoft Sentinel.
You need to ensure that the analyst can assign and resolve incidents. The solution must use the principle of least privilege.
Which role should you assign to the analyst?

A. Microsoft Sentinel Responder
B. Logic App Contributor
C. Microsoft Sentinel Reader
D. Microsoft Sentinel Contributor

**Answer:** A

**Explanation:**
The Microsoft Sentinel Responder role allows users to investigate, triage, and resolve security incidents, which includes the ability to assign incidents to other users. This role is designed to provide the necessary permissions for incident management and response while still adhering to the principle of least privilege. Other roles such as Logic App Contributor and Microsoft Sentinel Contributor would have more permissions than necessary and may not be suitable for the analyst's needs. Microsoft Sentinel Reader role is not sufficient as it doesn't have permission to assign and resolve incidents.
Reference: https://docs.microsoft.com/en-us/azure/sentinel/role-based-access-control-rbac

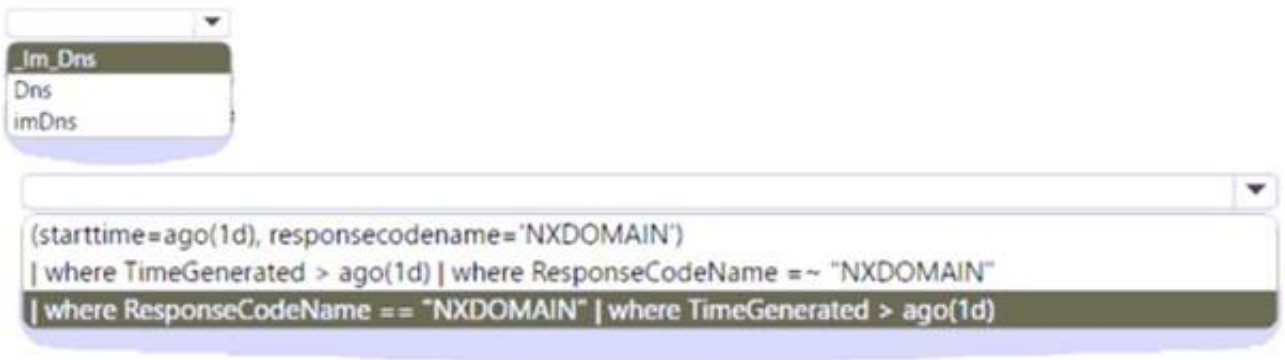
**NEW QUESTION 102**

- (Topic 4)
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:** AD

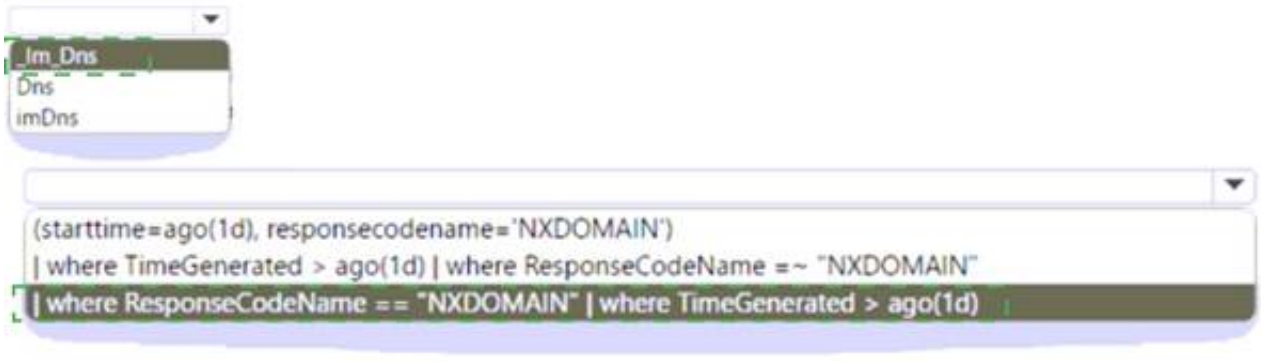
**NEW QUESTION 107**
HOTSPOT - (Topic 4)
You have a Microsoft Sentinel workspace named Workspaces You configure Workspace1 to c
ollect DNS events and deploy the Advanced Security information Model (ASIM) unifying parser for the DNS schema.
You need to query the ASIM DNS schema to list all the DNS events from the last 24 hours that have a response code of 'NXDOMAIN' and were aggregated by the source IP address in 15-minute intervals. The solution must maximize query performance.
How should you complete the query? To answer, select the appropriate options in the answer area
NOTE: Each correct selection is worth one point.




A. Mastered
B. Not Mastered

**Answer:** A

**Explanation:**




**NEW QUESTION 110**
- (Topic 4)
You have a Microsoft 365 subscription that uses Microsoft 365 Defender. You need to identify all the entities affected by an incident.
Which tab should you use in the Microsoft 365 Defender portal?

A. Investigations
B. Devices
C. Evidence and Response
D. Alerts

**Answer:** C

**Explanation:**
The Evidence and Response tab shows all the supported events and suspicious entities in the alerts in the incident.
Reference: https://docs.microsoft.com/en-us/microsoft-365/security/defender/investigate- incidents

**NEW QUESTION 113**
- (Topic 4)
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 Security alerts, you select the alert, select Take Action, and then expand the Prevent future attacks section.
Does this meet the goal?

A. Yes
B. No

**Answer:** B

**Explanation:**
You need to resolve the existing alert, not prevent future alerts. Therefore, you need to select the 'Mitigate the threat' option.
Reference:
https://docs.microsoft.com/en-us/azure/security-center/security-center-managing-and- responding-alerts

**NEW QUESTION 117**
- (Topic 4)
You have an Azure subscription that uses Microsoft Sentinel and contains 100 Linux virtual machines.
You need to monitor the virtual machines by using Microsoft Sentinel. The solution must meet the fallowing requirements:
• Minimize administrative effort
• Minimize the parsing required to read log data What should you configure?

A. REST API integration
B. a SysJog connector
C. a Log Analytics Data Collector API
D. a Common Event Format (CEF) connector

**Answer:** B

**NEW QUESTION 118**
- (Topic 4)
You receive a security bulletin about a potential attack that uses an image file.
You need to create an indicator of compromise (IoC) in Microsoft Defender for Endpoint to prevent the attack.
Which indicator type should you use?

A. a URL/domain indicator that has Action set to Alert only
B. a URL/domain indicator that has Action set to Alert and block
C. a file hash indicator that has Action set to Alert and block
D. a certificate indicator that has Action set to Alert and block

**Answer:** C

**Explanation:**
Reference:
https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/indicator-file?view=o365-worldwide

**NEW QUESTION 122**
- (Topic 4)
You are configuring Microsoft Cloud App Security.
You have a custom threat detection policy based on the IP address ranges of your company's United States-based offices.
You receive many alerts related to impossible travel and sign-ins from risky IP addresses. You determine that 99% of the alerts are legitimate sign-ins from your corporate offices. You need to prevent alerts for legitimate sign-ins from known locations.
Which two actions should you perform? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

A. Override automatic data enrichment.
B. Add the IP addresses to the corporate address range category.
C. Increase the sensitivity level of the impossible travel anomaly detection policy.
D. Add the IP addresses to the other address range category and add a tag.
E. Create an activity policy that has an exclusion for the IP addresses.

**Answer:** AD

**NEW QUESTION 124**
- (Topic 4)
You have a Microsoft Sentinel workspace named workspace1 that contains custom Kusto queries.
You need to create a Python-based Jupyter notebook that will create visuals. The visuals will display the results of the queries and be pinned to a dashboard. The solution must minimize development effort.
What should you use to create the visuals?

A. plotly
B. TensorFlow
C. msticpy
D. matplotlib

**Answer:** C

**Explanation:**
msticpy is a library for InfoSec investigation and hunting in Jupyter Notebooks. It includes functionality to: query log data from multiple sources. enrich the data with Threat Intelligence, geolocations and Azure resource data. extract Indicators of Activity (IoA) from logs and unpack encoded data.
MSTICPy reduces the amount of code that customers need to write for Microsoft Sentinel, and provides:

Data query capabilities, against Microsoft Sentinel tables, Microsoft Defender for Endpoint, Splunk, and other data sources.
Threat intelligence lookups with TI providers, such as VirusTotal and AlienVault OTX. Enrichment functions like geolocation of IP addresses, Indicator of Compromise (IoC) extraction, and WhoIs lookups.
Visualization tools using event timelines, process trees, and geo mapping.
Advanced analyses, such as time series decomposition, anomaly detection, and clustering.
Reference:
https://docs.microsoft.com/en-us/azure/sentinel/notebook-get-started https://msticpy.readthedocs.io/en/latest/

**NEW QUESTION 129**
- (Topic 4)
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

**Answer:** B

**Explanation:**
Reference:
https://docs.microsoft.com/en-us/azure/security-center/security-center-managing-and- responding-alerts

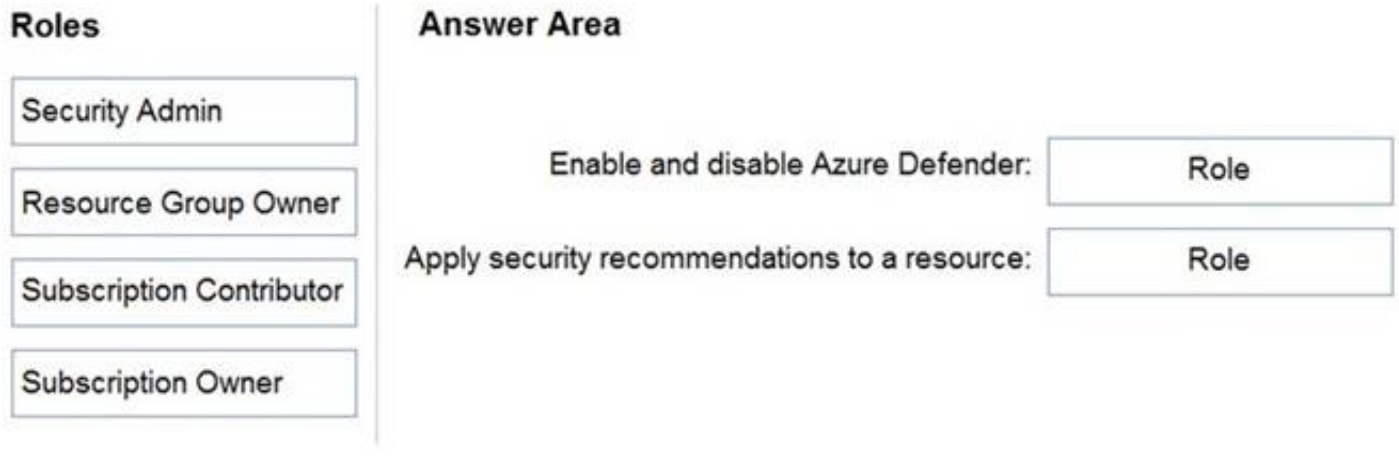
**NEW QUESTION 130**
- (Topic 4)
You use Azure Defender.
You have an Azure Storage account that contains sensitive information.
You need to run a PowerShell script if someone accesses the storage account from a suspicious IP address.
Which two actions should you perform? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

A. From Azure Security Center, enable workflow automation.
B. Create an Azure logic appthat has a manual trigger
C. Create an Azure logic app that has an Azure Security Center alert trigger.
D. Create an Azure logic appthat has an HTTP trigger.
E. From Azure Active Directory (Azure AD), add an app registration.

**Answer:** AC

**Explanation:**
Reference:
https://docs.microsoft.com/en-us/azure/storage/common/azure-defender-storage-configure?tabs=azure-security-center
https://docs.microsoft.com/en-us/azure/security-center/workflow-automation

**NEW QUESTION 133**
DRAG DROP - (Topic 4)
You have an Azure subscription.
You need to delegate permissions to meet the following requirements:
? Enable and disable Azure Defender.
? Apply security recommendations to resource.
The solution must use the principle of least privilege.
Which Azure Security Center role should you use for each requirement? To answer, drag the appropriate roles to the correct requirements. Each role may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.
NOTE: Each correct selection is worth one point.

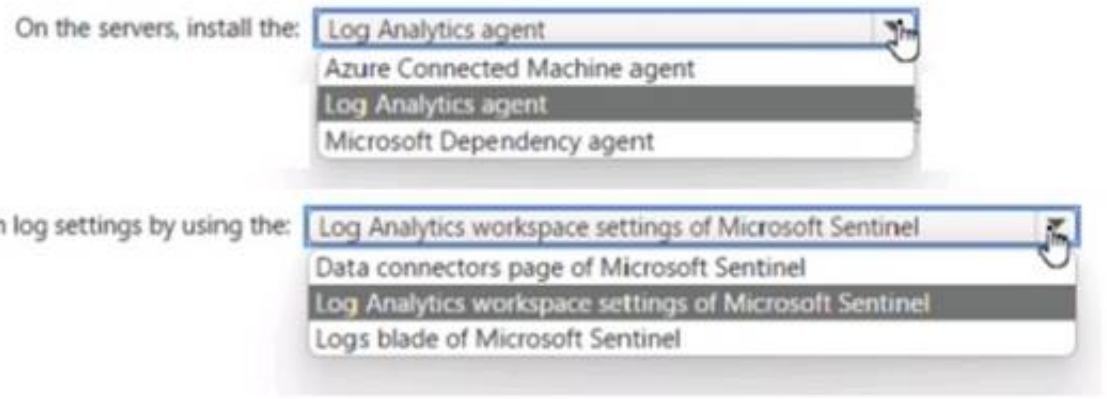



A. Mastered
B. Not Mastered

**Answer:** A

**Explanation:**


**NEW QUESTION 138**
HOTSPOT - (Topic 4)
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.

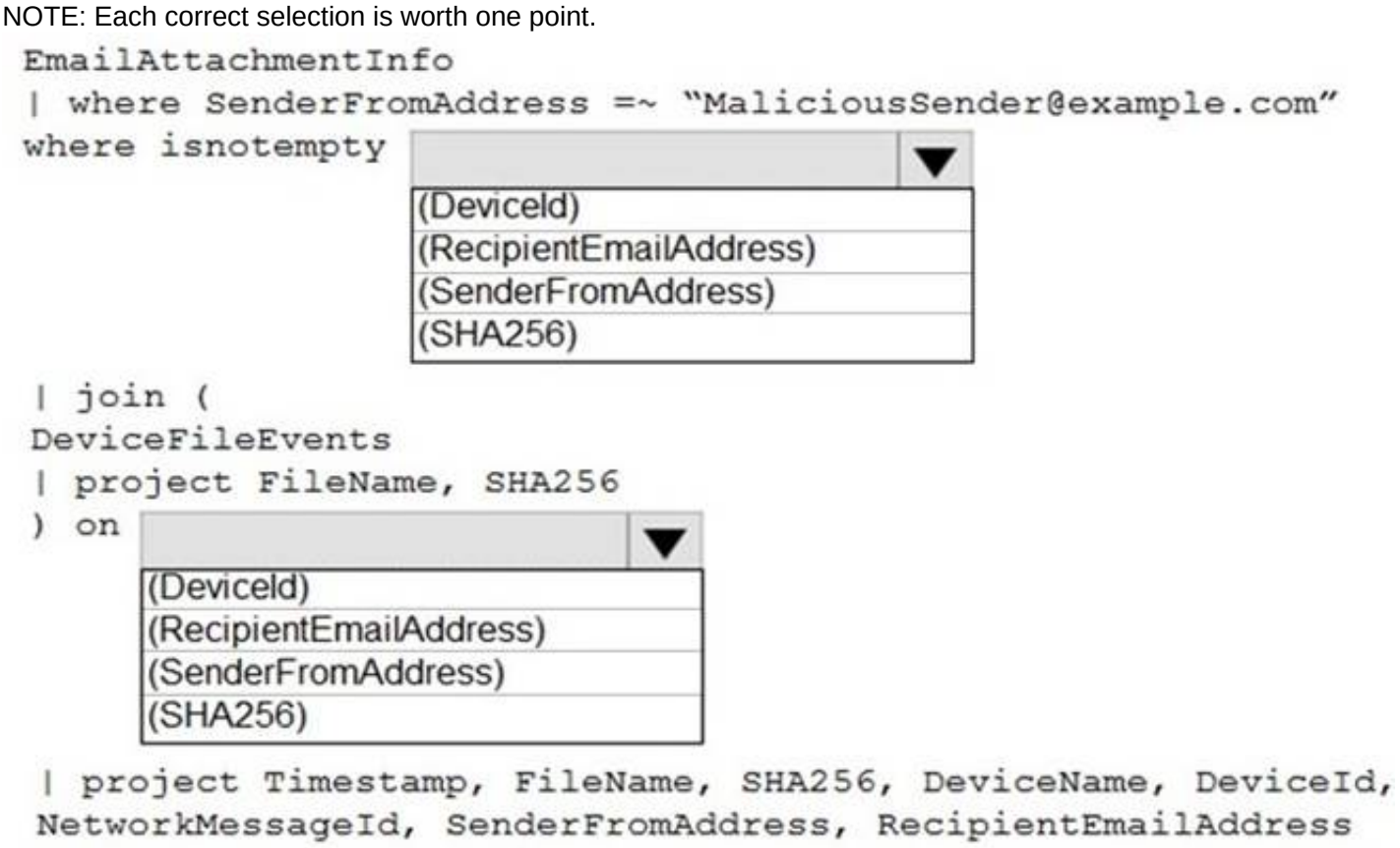



A. Mastered
B. Not Mastered

**Answer:** A

**Explanation:**
To upload custom logs from the on-premises servers to Microsoft Sentinel, you should install the Log Analytics agent on each of the 100 servers. The Log Analytics agent is a
lightweight agent that runs on the server and allows it to connect to the cloud-based Microsoft Defender Security Center. Once installed, the agent will allow the Microsoft Sentinel service to collect and analyze the custom log data from the servers.

**NEW QUESTION 141**
HOTSPOT - (Topic 4)
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.




A. Mastered
B. Not Mastered

**Answer:** A

**Explanation:**

```
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
```

**NEW QUESTION 144**
- (Topic 4)
You have an Azure subscription that has Microsoft Defender for Cloud enabled.
You have a virtual machine named Server! that runs Windows Server 2022 and is hosted in Amazon Web Services (AWS).
You need to collect logs and resolve vulnerabilities for Server1 by using Defender for Cloud.
What should you install first on Server1?

A. the Microsoft Monitoring Agent
B. the Azure Arc agent
C. the Azure Monitor agent
D. the Azure Pipelines agent

**Answer:** C

**NEW QUESTION 145**
HOTSPOT - (Topic 4)
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]
```

A. Mastered
B. Not Mastered

**Answer:** A

**Explanation:**

```
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]
```

**NEW QUESTION 148**

.....

# THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual SC-200 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the SC-200 Product From:

**https://www.2passeasy.com/dumps/SC-200/**

## Money Back Guarantee

## SC-200 Practice Exam Features:

* SC-200 Questions and Answers Updated Frequently

* SC-200 Practice Questions Verified by Expert Senior Certified Staff

* SC-200 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* SC-200 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year