# SC-200 Dumps

# Microsoft Security Operations Analyst

## https://www.certleader.com/SC-200-dumps.html

**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.

| 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 |

A. Mastered
B. Not Mastered

**Answer:** A

**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 |

**NEW QUESTION 2**
HOTSPOT - (Topic 1)
You need to recommend remediation actions for the Azure Defender alerts for Fabrikam.
What should you recommend for each threat? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

**Answer Area**

| Internal threat: | ▼ |
|---|---|
| | Add resource locks to the key vault. |
| | Modify the access policy settings for the key vault. |
| | Modify the role-based access control (RBAC) settings for the key vault. |

| External threat: | ▼ |
|---|---|
| | Implement Azure Firewall. |
| | Modify the Key Vault firewall settings. |
| | Modify the network security groups (NSGs). |

A. Mastered
B. Not Mastered

**Answer:** A

**Explanation:**

**Answer Area**

| Internal threat: | ▼ |
|---|---|
| | Add resource locks to the key vault. |
| | Modify the access policy settings for the key vault. |
| | Modify the role-based access control (RBAC) settings for the key vault. |

| External threat: | ▼ |
|---|---|
| | Implement Azure Firewall. |
| | Modify the Key Vault firewall settings. |
| | Modify the network security groups (NSGs). |

**NEW QUESTION 3**
HOTSPOT - (Topic 1)
You need to create an advanced hunting query to investigate the executive team issue.
How should you complete the query? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

```
┌─────────────────────┐ ▼
│ CloudAppEvents      │
│ DeviceFileEvents    │
│ DeviceProcessEvents │
└─────────────────────┘

| where TimeStamp > ago(2d)

| summarize activityCount =    ┌──────── ▼  by FolderPath, FileName,
                               │ avg()
ActionType, AccountDisplayName │ count()
                               │ sum()
                               └────────

| where activityCount > 5
```

A. Mastered
B. Not Mastered

**Answer:** A

**Explanation:**

```
┌─────────────────────┐ ▼
│ CloudAppEvents      │
│ DeviceFileEvents    │
│ DeviceProcessEvents │
└─────────────────────┘

| where TimeStamp > ago(2d)

| summarize activityCount =    ┌──────── ▼  by FolderPath, FileName,
                               │ avg()
ActionType, AccountDisplayName │ count()
                               │ sum()
                               └────────

| where activityCount > 5
```

**NEW QUESTION 4**
- (Topic 1)
You need to complete the query for failed sign-ins to meet the technical requirements. Where can you find the column name to complete the where clause?

A. Security alerts in Azure Security Center
B. Activity log in Azure
C. Azure Advisor
D. the query windows of the Log Analytics workspace

**Answer:** D

**NEW QUESTION 5**
DRAG DROP - (Topic 2)
You need to add notes to the events to meet the Azure Sentinel requirements.

Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of action to the answer area and arrange them in the correct order.

**Actions**

- Add a bookmark and map an entity.
- From Azure Monitor, run a Log Analytics query.
- Add the query to favorites.
- Select a query result.
- From the Azure Sentinel workspace, run a Log Analytics query.

**Answer Area**

A. Mastered
B. Not Mastered

**Answer:** A

**Explanation:**

**Actions**

- Add a bookmark and map an entity.
- From Azure Monitor, run a Log Analytics query.
- Add the query to favorites.
- Select a query result.
- From the Azure Sentinel workspace, run a Log Analytics query.

**Answer Area**

- From the Azure Sentinel workspace, run a Log Analytics query.
- Select a query result.
- Add a bookmark and map an entity.

**NEW QUESTION 6**
- (Topic 2)
You need to modify the anomaly detection policy settings to meet the Microsoft Defender for Cloud Apps requirements and resolve the reported problem.
Which policy should you modify?

A. Activity from suspicious IP addresses
B. Risky sign-in
C. Activity from anonymous IP addresses
D. Impossible travel

**Answer:** D

**NEW QUESTION 7**
- (Topic 2)
You need to restrict cloud apps running on CLIENT1 to meet the Microsoft Defender for Endpoint requirements.
Which two configurations should you modify? Each correct answer present part of the
solution.
NOTE: Each correct selection is worth one point.

A. the Onboarding settings from Device management in Microsoft Defender Security Center
B. Cloud App Security anomaly detection policies
C. Advanced features from Settings in Microsoft Defender Security Center
D. the Cloud Discovery settings in Cloud App Security

**Answer:** CD

**Explanation:**
All Cloud App Security unsanctioned apps must be blocked on the Windows 10 computers by using Microsoft Defender for Endpoint.
Reference:

https://docs.microsoft.com/en-us/cloud-app-security/mde-govern

**NEW QUESTION 8**
HOTSPOT - (Topic 2)
You need to configure the Microsoft Sentinel integration to 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**

In the Microsoft Defender for Cloud Apps portal: | Add a security extension
Add a security extension
Configure app connectors
Configure log collectors

From Microsoft Sentinel in the Azure portal: | Add a data connector
Add a data connector
Add a workbook
Configure the Logs settings

A. Mastered
B. Not Mastered

**Answer:** A

**Explanation:**

**Answer Area**

In the Microsoft Defender for Cloud Apps portal: | Add a security extension
Add a security extension
Configure app connectors
Configure log collectors

From Microsoft Sentinel in the Azure portal: | Add a data connector
Add a data connector
Add a workbook
Configure the Logs settings

**NEW QUESTION 9**
- (Topic 2)
You need to modify the anomaly detection policy settings to meet the Cloud App Security requirements. Which policy should you modify?

A. Activity from suspicious IP addresses
B. Activity from anonymous IP addresses
C. Impossible travel
D. Risky sign-in

**Answer:** C

**Explanation:**
Reference:
https://docs.microsoft.com/en-us/cloud-app-security/anomaly-detection-policy

**NEW QUESTION 10**
HOTSPOT - (Topic 3)
You need to implement the query for Workbook1 and Webapp1. The solution must meet the Microsoft Sentinel requirements. How should you configure the query? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

**Answer Area**

Data source to query: | JSON
A custom endpoint
A custom resource provider
JSON

On Webapp1: | Enable Cross-Origin Resource Sharing (CORS).
Enable Cross-Origin Resource Sharing (CORS).
Enable Same Origin Policy (SOP).
Enforce TLS 1.2.

A. Mastered
B. Not Mastered

**Answer:** A

**Explanation:**

**Answer Area**

| Data source to query: | JSON ▼ |
| --- | --- |
| | A custom endpoint |
| | A custom resource provider |
| | **JSON** |

| On Webapp1: | Enable Cross-Origin Resource Sharing (CORS). ▼ |
| --- | --- |
| | **Enable Cross-Origin Resource Sharing (CORS).** |
| | Enable Same Origin Policy (SOP). |
| | Enforce TLS 1.2. |
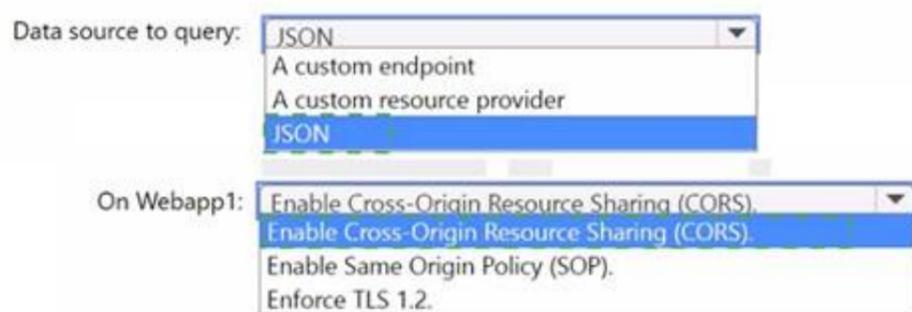
## NEW QUESTION 10
- (Topic 3)
You need to ensure that the Group1 members can meet the Microsoft Sentinel requirements.
Which role should you assign to Group1?

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

**Answer:** D

## NEW QUESTION 13
- (Topic 3)
You need to implement the Defender for Cloud requirements. Which subscription-level role should you assign to Group1?

A. Security Admin
B. Owner
C. Security Assessment Contributor
D. Contributor

**Answer:** B

## NEW QUESTION 17
HOTSPOT - (Topic 3)
You need to implement the ASIM query for DNS requests. The solution must meet the Microsoft Sentinel requirements. How should you configure the query? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

**Answer Area**

| ASIM parser: | Im_Dns ▼ |
| --- | --- |
| | **_Im_Dns** |
| | _Im_Dns_InfobloxNIOS |
| | imDns |

| Filter: | A filtering parameter ▼ |
| --- | --- |
| | **A filtering parameter** |
| | A pack parameter |
| | The WHERE clause |

A. Mastered
B. Not Mastered

**Answer:** A

**Explanation:**

**Answer Area**

| ASIM parser: | Im_Dns ▼ |
| --- | --- |
| | **_Im_Dns** |
| | _Im_Dns_InfobloxNIOS |
| | imDns |

| Filter: | A filtering parameter ▼ |
| --- | --- |
| | **A filtering parameter** |
| | A pack parameter |
| | The WHERE clause |
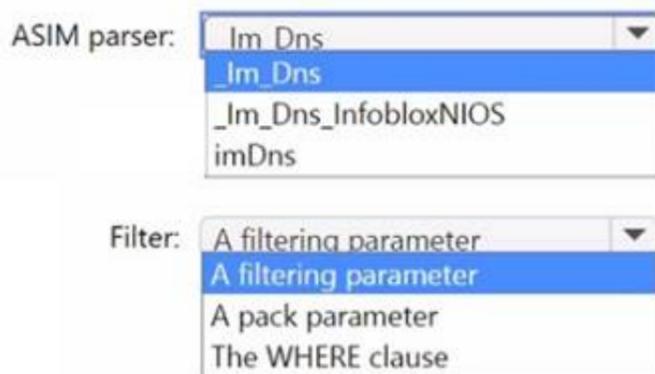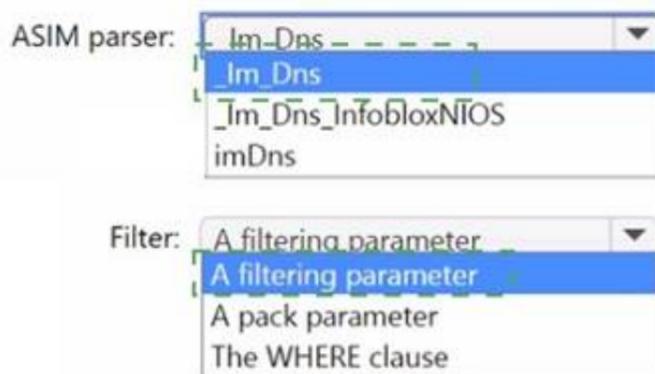
**NEW QUESTION 21**
- (Topic 3)
You need to implement the scheduled rule for incident generation based on rulequery1. What should you configure first?

A. entity mapping
B. custom details
C. event grouping
D. alert details

**Answer:** D

**NEW QUESTION 22**
- (Topic 4)
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.

**Answer:** BC

**Explanation:**
B: To add a data connector, you would use the Azure Sentinel data connectors feature to connect to your Azure subscription and to configure log data collection for Azure Storage account key enumeration events.
C: After adding the data connector, you need to create an analytics rule to analyze the log data from the Azure storage connector, looking for the specific event of Azure storage account keys enumeration. This rule will trigger an alert when it detects the specific event, allowing you to take immediate action.

**NEW QUESTION 24**
- (Topic 4)
You implement Safe Attachments policies in Microsoft Defender for Office 365.
Users report that email messages containing attachments take longer than expected to be received.
You need to reduce the amount of time it takes to deliver messages that contain attachments without compromising security. The attachments must be scanned for malware, and any messages that contain malware must be blocked.
What should you configure in the Safe Attachments policies?

A. Dynamic Delivery
B. Replace
C. Block and Enable redirect
D. Monitor and Enable redirect

**Answer:** A

**Explanation:**
Reference:
https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/safe-attachments?view=o365-worldwide

**NEW QUESTION 25**
- (Topic 4)
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.

**Answer:** D

**Explanation:**
Reference:
https://docs.microsoft.com/en-us/azure/sentinel/tutorial-detect-threats-custom

**NEW QUESTION 28**
- (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 31**
DRAG DROP - (Topic 4)
You have an Azure Functions app that generates thousands of alerts in Azure Security Center each day for normal activity.
You need to hide the alerts automatically in Security Center.
Which three actions should you perform in sequence in Security Center? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

| Actions | Answer area |
|---|---|
| Select **Pricing & settings**. | |
| Select **Security alerts**. | |
| Select **IP** as the entity type and specify the IP address. | ⊙ ⊙ |
| Select **Azure Resource** as the entity type and specify the ID. | ⊙ ⊙ |
| Select **Suppression rules**, and then select **Create new suppression rule**. | |
| Select **Security policy**. | |

A. Mastered
B. Not Mastered

**Answer:** A

**Explanation:**

| Actions | Answer area |
|---|---|
| Select **Pricing & settings**. | Select **Security policy**. |
| Select **Security alerts**. | Select **Suppression rules**, and then select **Create new suppression rule**. |
| Select **IP** as the entity type and specify the IP address. | Select **Azure Resource** as the entity type and specify the ID. |
| Select **Azure Resource** as the entity type and specify the ID. | |
| Select **Suppression rules**, and then select **Create new suppression rule**. | |
| Select **Security policy**. | |

**NEW QUESTION 34**
- (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 36**
- (Topic 4)
You have a Microsoft 365 subscription. The subscription uses Microsoft 365 Defender and has data loss prevention (DLP) policies that have aggregated alerts configured.
You need to identify the impacted entities in an aggregated alert.
What should you review in the DIP alert management dashboard of the Microsoft Purview compliance portal?

A. the Details tab of the alert
B. Management log
C. the Sensitive Info Types tab of the alert
D. the Events tab of the alert

**Answer:** B

**NEW QUESTION 41**
HOTSPOT - (Topic 4)
You have the following SQL 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. '
```

**Answer Area**

| 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:**

**Answer Area**

| 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 43**
DRAG DROP - (Topic 4)
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 | Answer Area |
| --- | --- |
| 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. | |

A. Mastered
B. Not Mastered

**Answer:** A

**Explanation:**
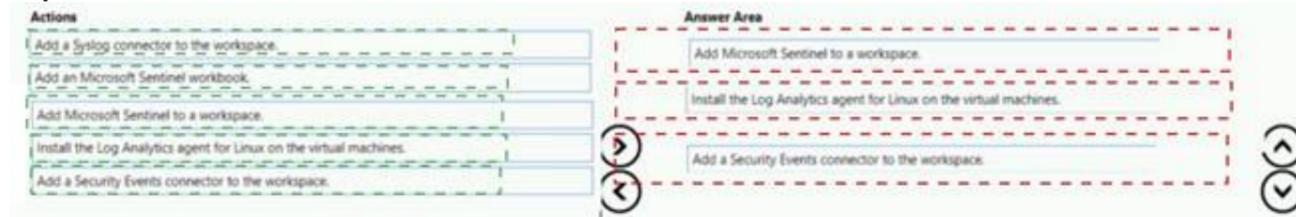


**NEW QUESTION 46**
- (Topic 4)
You have a Microsoft Sentinel workspace named Workspace1 and 200 custom Advanced Security Information Model (ASIM) parsers based on the DNS schema.
You need to make the 200 parsers available in Workspace1. The solution must minimize administrative effort. What should you do first?

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

**NEW QUESTION 51**
- (Topic 4)
You have a Microsoft Sentinel workspace.
You enable User and Entity Behavior Analytics (UFBA) by using Audit logs and Signin logs. The following entities are detected in the Azure AD tenant:
• App name: App1
• IP address: 192.168.1.2
• Computer name: Device1
• Used client app: Microsoft Edge
• Email address: user1@company.com
• Sign-in URL: https://www.company.com
Which entities can be investigated by using UEBA?

A. app name, computer name, IP address, email address, and used client app only
B. IP address and email address only
C. used client app and app name only
D. IP address only

**Answer:** D

**NEW QUESTION 55**
HOTSPOT - (Topic 4)
You have a Microsoft Sentinel workspace that contains a custom workbook.
You need to query the number of daily security alerts. The solution must meet the following requirements:
• Identify alerts that occurred during the last 30 days.
• Display the results in a timechart.
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:**

**Answer Area**

```
SecurityAlert

| where TimeGenerated >= ago(30d)

|  [▼]                count() by ProviderName,  [▼]            (TimeGenerated, 1d)
   lookup                                        bin
   project                                       make series
   summarize                                     range

| render timechart
```

## NEW QUESTION 60

HOTSPOT - (Topic 4)

You have a Microsoft 365 E5 subscription that uses Microsoft Teams.

You need to perform a content search of Teams chats for a user by using the Microsoft Purview compliance portal. The solution must minimize the scope of the search.

How should you configure the content search? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

**Answer Area**

Locations: Exchange mailboxes [▼]
- Exchange mailboxes
- Exchange public folders
- SharePoint sites

Keywords: Kind [▼]
- Category
- ItemClass
- Kind

A. Mastered
B. Not Mastered

**Answer:** A

**Explanation:**

**Answer Area**

Locations: Exchange mailboxes [▼]
- Exchange mailboxes
- Exchange public folders
- SharePoint sites

Keywords: Kind [▼]
- Category
- ItemClass
- Kind
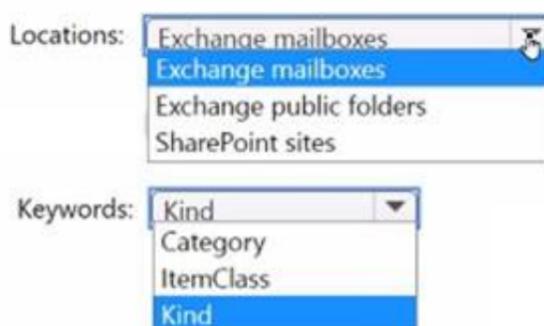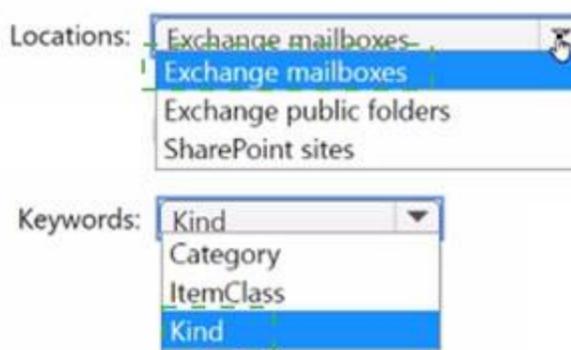
## NEW QUESTION 62

- (Topic 4)

You recently deployed Azure Sentinel.

You discover that the default Fusion rule does not generate any alerts. You verify that the rule is enabled.

You need to ensure that the Fusion rule can generate alerts. What should you do?

A. Disable, and then enable the rule.
B. Add data connectors
C. Create a new machine learning analytics rule.
D. Add a hunting bookmark.

**Answer:** B

**Explanation:**

Reference:

https://docs.microsoft.com/en-us/azure/sentinel/connect-data-sources

## NEW QUESTION 67

HOTSPOT - (Topic 4)

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.
View the window
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

A. Mastered
B. Not Mastered

**Answer:** A

**Explanation:**

**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

**NEW QUESTION 70**
- (Topic 4)
You have an Azure subscription that uses Microsoft Defender for Cloud.
You have an Amazon Web Services (AWS) subscription. The subscription contains multiple virtual machines that run Windows Server.
You need to enable Microsoft Defender for Servers on the virtual machines.
Which two actions should you perform? Each correct answer presents part of the solution. NOTE: Each correct answer is worth one point.

A. From Defender for Cloud, enable agentless scanning.
B. Install the Azure Virtual Machine Agent (VM Agent) on each virtual machine.
C. Onboard the virtual machines to Microsoft Defender for Endpoint.
D. From Defender for Cloud, configure auto-provisioning.
E. From Defender for Cloud, configure the AWS connector.

**Answer:** BC

**NEW QUESTION 74**
HOTSPOT - (Topic 4)
You have a Microsoft 365 E5 subscription.
You plan to perform cross-domain investigations by using Microsoft 365 Defender.
You need to create an advanced hunting query to identify devices affected by a malicious email attachment.
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 Area

```
EmailAttachmentInfo

| where SenderFromAddress =~ "MaliciousSender@example.com"

| where isnotempty (SHA256)

| [ join ▼ ] (
    extend
    join
    project
    union

DeviceFileEvents

| [ project ▼ ] FileName, SHA256
    extend
    join
    project
    union

) on SHA256

| [ project ▼ ] Timestamp, FileName, SHA256, DeviceName, DeviceId,
    extend
    join
    project
    union

NetworkMessageId, SenderFromAddress, RecipientEmailAddress
```

A. Mastered
B. Not Mastered

**Answer:** A

**Explanation:**

## Answer Area

```
EmailAttachmentInfo

| where SenderFromAddress =~ "MaliciousSender@example.com"

| where isnotempty (SHA256)

|  [ ▼ ]  (
    extend
    join
    project
    union

DeviceFileEvents

|  [ ▼ ]  FileName, SHA256
    extend
    join
    project
    union

) on SHA256

|  [ ▼ ]  Timestamp, FileName, SHA256, DeviceName, DeviceId,
    extend
    join
    project
    union

NetworkMessageId, SenderFromAddress, RecipientEmailAddress
```

**NEW QUESTION 78**
HOTSPOT - (Topic 4)
You need to use an Azure Resource Manager template to create a workflow automation that will trigger an automatic remediation when specific security alerts are received by Azure Security Center.
How should you complete the portion of the template that will provision the required Azure resources? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

```
"resources": [
    {
        "type": "  [ ▼ ] /automations",
                    Microsoft.Automation
                    Microsoft.Logic
                    Microsoft.Security
        "apiVersion": "2019-01-01-preview",
        "name": "[parameters('name')]",
        "location": "[parameters('location')]",
        "properties": {
            "description": "[format(variables('description'), '{0}', parameters
('subscriptionId'))]",
            "isEnabled": true,
            "actions": [
                {
                    "actionType": "LogicApp",
                    "logicAppResourceId": "[resourceId('ITEM2/workflows', parameters
('appName'))]",
                    "uri": "[listCallbackURL(resourceId(parameters('subscriptionId'),
parameters('resourceGroupName'), '  [ ▼ ] /workflows/triggers',
                                                Microsoft.Automation
                                                Microsoft.Logic
                                                Microsoft.Security
parameters('appName'), 'manual'), '2019-05-01').value]"
                }
            ],
```

A. Mastered
B. Not Mastered

**Answer:** A

**Explanation:**

```
"resources": [
    {
        "type": "  [Microsoft.Automation / Microsoft.Logic / Microsoft.Security]  /automations",
        "apiVersion": "2019-01-01-preview",
        "name": "[parameters('name')]",
        "location": "[parameters('location')]",
        "properties": {
            "description": "[format(variables('description'), '{0}', parameters('subscriptionId'))]",
            "isEnabled": true,
            "actions": [
                {
                    "actionType": "LogicApp",
                    "logicAppResourceId": "[resourceId('ITEM2/workflows', parameters('appName'))]",
                    "uri": "[listCallbackURL(resourceId(parameters('subscriptionId'),
parameters('resourceGroupName'), ' [Microsoft.Automation / Microsoft.Logic / Microsoft.Security]  /workflows/triggers',
parameters('appName'), 'manual'), '2019-05-01').value]"
                }
            ],
```

## NEW QUESTION 81

- (Topic 4)
You have a custom Microsoft Sentinel workbook named Workbooks.
You need to add a grid to Workbook1. The solution must ensure that the grid contains a maximum of 100 rows.
What should you do?

A. In the query editor interface, configure Settings.
B. In the query editor interface, select Advanced Editor
C. In the grid query, include the project operator.
D. In the grid query, include the take operator.

**Answer:** B

## NEW QUESTION 85

- (Topic 4)
You need to receive a security alert when a user attempts to sign in from a location that was never used by the other users in your organization to sign in.
Which anomaly detection policy should you use?

A. Impossible travel
B. Activity from anonymous IP addresses
C. Activity from infrequent country
D. Malware detection

**Answer:** C

**Explanation:**
Activity from a country/region that could indicate malicious activity. This policy profiles your environment and triggers alerts when activity is detected from a location that was not recently or was never visited by any user in the organization. Activity from the same user in different locations within a time period that is shorter than the expected travel time between the two locations. This can indicate a credential breach, however, it's also possible that the user's actual location is masked, for example, by using a VPN.
Reference:
https://docs.microsoft.com/en-us/cloud-app-security/anomaly-detection-policy

## NEW QUESTION 88

- (Topic 4)
You have an Azure subscription named Sub1 and a Microsoft 365 subscription. Sub1 is linked to an Azure Active Directory (Azure AD) tenant named contoso.com. You create an Azure Sentinel workspace named workspace1. In workspace1, you activate an Azure AD connector for contoso.com and an Office 365 connector for the Microsoft 365 subscription.
You need to use the Fusion rule to detect multi-staged attacks that include suspicious sign- ins to contoso.com followed by anomalous Microsoft Office 365 activity.
Which two actions should you perform? Each correct answer present part of the solution
NOTE: Each correct selection is worth one point.

A. Create custom rule based on the Office 365 connector templates.
B. Create a Microsoft incident creation rule based on Microsoft Defender for Cloud.
C. Create a Microsoft Cloud App Security connector.
D. Create an Azure AD Identity Protection connector.

**Answer:** AB

**Explanation:**
 To use the Fusion rule to detect multi-staged attacks that include suspicious sign-ins to contoso.com followed by anomalous Microsoft Office 365 activity, you should perform the following two actions:
? Create an Azure AD Identity Protection connector. This will allow you to monitor
suspicious activities in your Azure AD tenant and detect malicious sign-ins.
? Create a custom rule based on the Office 365 connector templates. This will allow you to monitor and detect anomalous activities in the Microsoft 365
subscription. Reference: https://docs.microsoft.com/en-us/azure/sentinel/fusion-rules

**NEW QUESTION 91**
- (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 93**
- (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 94**
HOTSPOT - (Topic 4)
You need to create a query for a workbook. The query must meet the following requirements:
? List all incidents by incident number.
? Only include the most recent log for each incident.
How should you complete the query? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

```
SecurityIncident
```

| project ▼ | arg_max ▼ | (LasModifiedTime,*) by IncidentNumber |
|-----------|-----------|----------------------------------------|
| sort | limit | |
| summarize | top | |

A. Mastered
B. Not Mastered

**Answer:** A

**Explanation:**

```
SecurityIncident
```

| project ▼ | arg_max ▼ | (LasModifiedTime,*) by IncidentNumber |
|-----------|-----------|----------------------------------------|
| sort | limit | |
| summarize | top | |

**NEW QUESTION 96**
HOTSPOT - (Topic 4)
You have an Azure subscription that is linked to a hybrid Azure AD tenant and contains a Microsoft Sentinel workspace named Sentinel1.
You need to enable User and Entity Behavior Analytics (UEBA) for Sentinel 1 and configure UEBA to use data collected from Active Directory Domain Services (AD OS).
What should you do? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

**Answer Area**

To the AD DS domain controllers, deploy: `The Azure Connected Machine agent ▼`
- Microsoft Defender for Identity sensors
- **The Azure Connected Machine agent**
- The Azure Monitor agent

For Sentinel1, configure: `The Audit Logs data source ▼`
- **The Audit Logs data source**
- The Security Events data source
- The Signin Logs data source

A. Mastered
B. Not Mastered

**Answer:** A

**Explanation:**

**Answer Area**

To the AD DS domain controllers, deploy: `The Azure Connected Machine agent ▼`
- Microsoft Defender for Identity sensors
- **The Azure Connected Machine agent**
- The Azure Monitor agent

For Sentinel1, configure: `The Audit Logs data source ▼`
- **The Audit Logs data source**
- The Security Events data source
- The Signin Logs data source

**NEW QUESTION 97**
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.

```
[_____ ▼]
AuditLogs                    in~ ("Microsoft.Network/networkSecurityGroups/securityRules/write")
AzureActivity
AzureDiagnostics             e == "Succeeded"

| make-series dcount(ResourceId) default=0 on EventSubmissionTimestamp in range(ago(7d), now(), 1d) by Caller

| extend timestamp = todatetime(EventSubmissionTimestamp[0])
[_____ ▼]   AccountCustomEntity = Caller
| extend
| parse-where
| where
```

A. Mastered
B. Not Mastered

**Answer:** A

**Explanation:**

```
┌──────────────────────────┐ ▼
│ AuditLogs                │      in~ ("Microsoft.Network/networkSecurityGroups/securityRules/write")
│ AzureActivity            │
│ AzureDiagnostics         │      e == "Succeeded"
└──────────────────────────┘
| make-series dcount(ResourceId) default=0 on EventSubmissionTimestamp in range(ago(7d), now(), 1d) by Caller

| extend timestamp = todatetime(EventSubmissionTimestamp[0])

┌──────────────────────────┐ ▼
│                          │      AccountCustomEntity = Caller
└──────────────────────────┘
| extend    |
| parse-where
| where     |
```

**NEW QUESTION 99**
- (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 Microsoft incident creation rule for a data connector. Does this meet the goal?

A. Yes
B. No

**Answer:** A

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

**NEW QUESTION 100**
- (Topic 4)
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

**Answer:** A

**Explanation:**
 Reference:
https://docs.microsoft.com/en-us/azure/key-vault/general/network-security

**NEW QUESTION 101**
- (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 106**
- (Topic 4)
Your company uses line-of-business apps that contain Microsoft Office VBA macros.
You plan to enable protection against downloading and running additional payloads from the Office VBA macros as additional child processes.
You need to identify which Office VBA macros might be affected.
Which two commands can you run to achieve the goal? Each correct answer presents a complete solution.
NOTE: Each correct selection is worth one point.

A. `Add-MpPreference -AttackSurfaceReductionRules_Ids D4F940AB -401B - 4EFC -AADC -AD5F3C50688A -AttackSurfaceReductionRules_Actions Enabled`

B. `Set-MpPreference -AttackSurfaceReductionRules_Ids D4F940AB -401B -4EFC - AADC -AD5F3C50688A -AttackSurfaceReductionRules_Actions AuditMode`

C. `Add-MpPreference -AttackSurfaceReductionRules_Ids D4F940AB -401B -4EFC -AADC -AD5F3C50688A -AttackSurfaceReductionRules_Actions AuditMode`

D. `Set-MpPreference -AttackSurfaceReductionRules_Ids D4F940AB -401B -4EFC - AADC -AD5F3C50688A -AttackSurfaceReductionRules_Actions Enabled`

A. Option A
B. Option B
C. Option C
D. Option D

**Answer:** BC

**Explanation:**
 Reference:
https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/attack-surface- reduction

**NEW QUESTION 110**
HOTSPOT - (Topic 4)
You have an Microsoft Sentinel workspace named SW1.
You plan to create a custom workbook that will include a time chart.
You need to create a query that will identify the number of security alerts per day for each provider.
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 Area**

```
SecurityAlert
| where TimeGenerated >= ago(30d)
| summarize count() by ProviderName,   [bin ▼] (TimeGenerated, 1d)
                                        bin
| [render ▼] timechart                  series_add
  materialize                           series_fill_linear
  project                               take
  render
```

A. Mastered
B. Not Mastered

**Answer:** A

**Explanation:**

**Answer Area**

```
SecurityAlert
| where TimeGenerated >= ago(30d)
| summarize count() by ProviderName,   [bin ▼] (TimeGenerated, 1d)
                                        bin
| [render ▼] timechart                  series_add
  materialize                           series_fill_linear
  project                               take
  render
```

**NEW QUESTION 114**
DRAG DROP - (Topic 4)
You are investigating an incident by using Microsoft 365 Defender.
You need to create an advanced hunting query to detect 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.

**Values**

| project LogonFailures=count()

| summarize LogonFailures=count() by DeviceName, LogonType

| where ActionType == FailureReason

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

ActionType == "LogonFailed"

**Answer Area**

and

A. Mastered
B. Not Mastered

**Answer:** A

**Explanation:**

**Values**

| project LogonFailures=count()

| summarize LogonFailures=count() by DeviceName, LogonType

| where ActionType == FailureReason

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

ActionType == "LogonFailed"

**Answer Area**

| summarize LogonFailures=count() by DeviceName, LogonType

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

| where ActionType == FailureReason

ActionType == "LogonFailed"

| project LogonFailures=count()

and

**NEW QUESTION 117**
DRAG DROP - (Topic 4)
You have resources in Azure and Google cloud.
You need to ingest Google Cloud Platform (GCP) data into Azure Defender.
In which order should you perform the actions? To answer, move all actions from the list of actions to the answer area and arrange them in the correct order.

**Actions**

Enable Security Health Analytics.

From Azure Security Center, add cloud connectors.

Configure the GCP Security Command Center.

Create a dedicated service account and a private key.

Enable the GCP Security Command Center API.

**Answer Area**

A. Mastered
B. Not Mastered

**Answer:** A

**Explanation:**

## Actions

| |
|---|
| Enable Security Health Analytics. |
| From Azure Security Center, add cloud connectors. |
| Configure the GCP Security Command Center. |
| Create a dedicated service account and a private key. |
| Enable the GCP Security Command Center API. |

## Answer Area

| |
|---|
| Configure the GCP Security Command Center. |
| Enable Security Health Analytics. |
| Enable the GCP Security Command Center API. |
| Create a dedicated service account and a private key. |
| From Azure Security Center, add cloud connectors. |
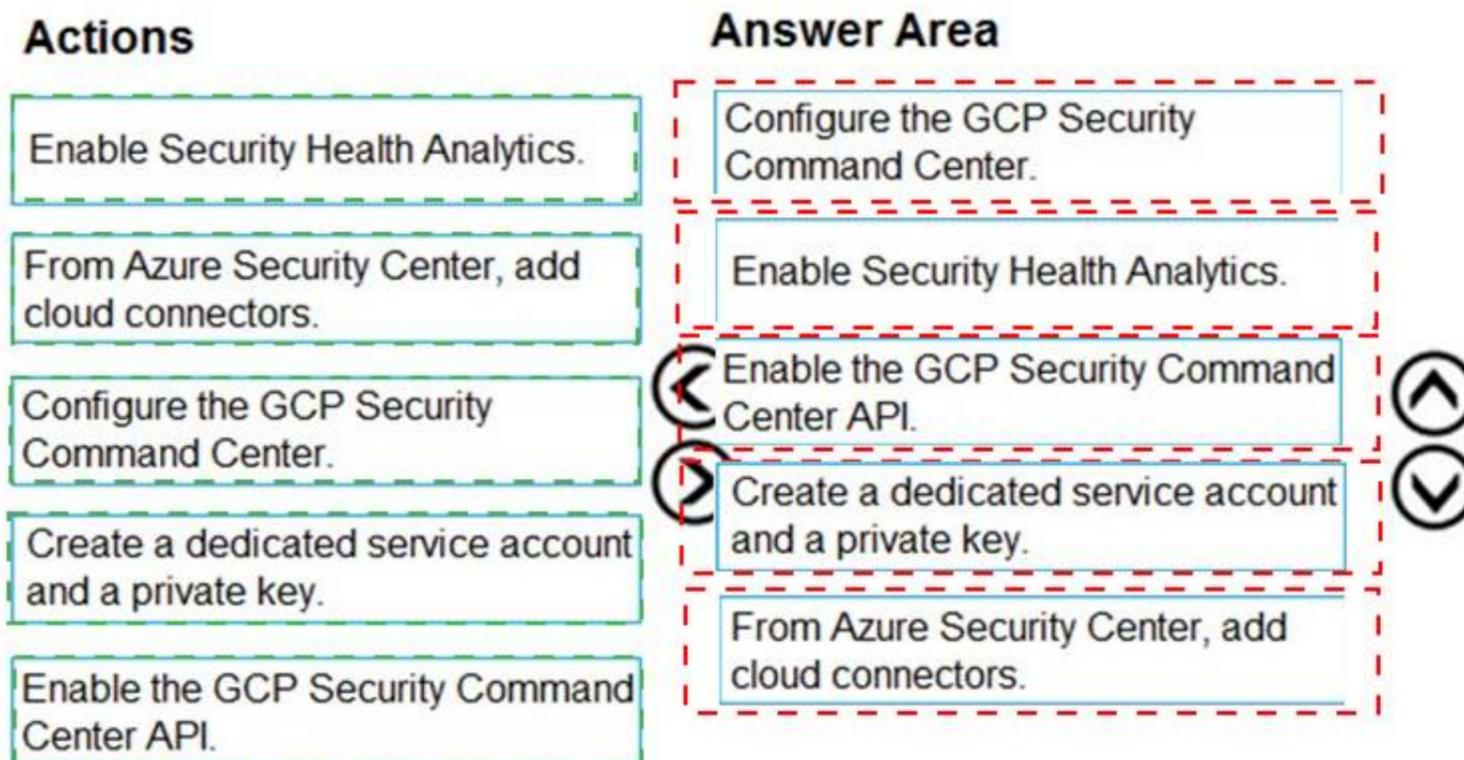
**NEW QUESTION 119**
- (Topic 4)
You use Azure Sentinel.
You need to use a built-in role to provide a security analyst with the ability to edit the queries of custom Azure Sentinel workbooks. The solution must use the principle of least privilege.
Which role should you assign to the analyst?

A. Azure Sentinel Contributor
B. Security Administrator
C. Azure Sentinel Responder
D. Logic App Contributor

**Answer:** C

**Explanation:**
Azure Sentinel Contributor can create and edit workbooks, analytics rules, and other Azure Sentinel resources.
Reference:
https://docs.microsoft.com/en-us/azure/sentinel/roles

**NEW QUESTION 122**
- (Topic 4)
You have a Microsoft Sentinel workspace.
You receive multiple alerts for failed sign in attempts to an account. You identify that the alerts are false positives.
You need to prevent additional failed sign-in alerts from being generated for the account. The solution must meet the following requirements.
• Ensure that failed sign-in alerts are generated for other accounts.
• Minimize administrative effort What should do?

A. Create an automation rule.
B. Create a watchlist.
C. Modify the analytics rule.
D. Add an activity template to the entity behavior.

**Answer:** A

**Explanation:**
An automation rule will allow you to specify which alerts should be suppressed, ensuring that failed sign-in alerts are generated for other accounts while minimizing administrative effort. To create an automation rule, navigate to the Automation Rules page in the Microsoft Sentinel workspace and configure the rule parameters to suppress the false positive alerts.

**NEW QUESTION 127**
- (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: You add each account as a Sensitive account. Does this meet the goal?

A. Yes
B. No

**Answer:** B

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

**NEW QUESTION 132**
DRAG DROP - (Topic 4)
You open the Cloud App Security portal as shown in the following exhibit.
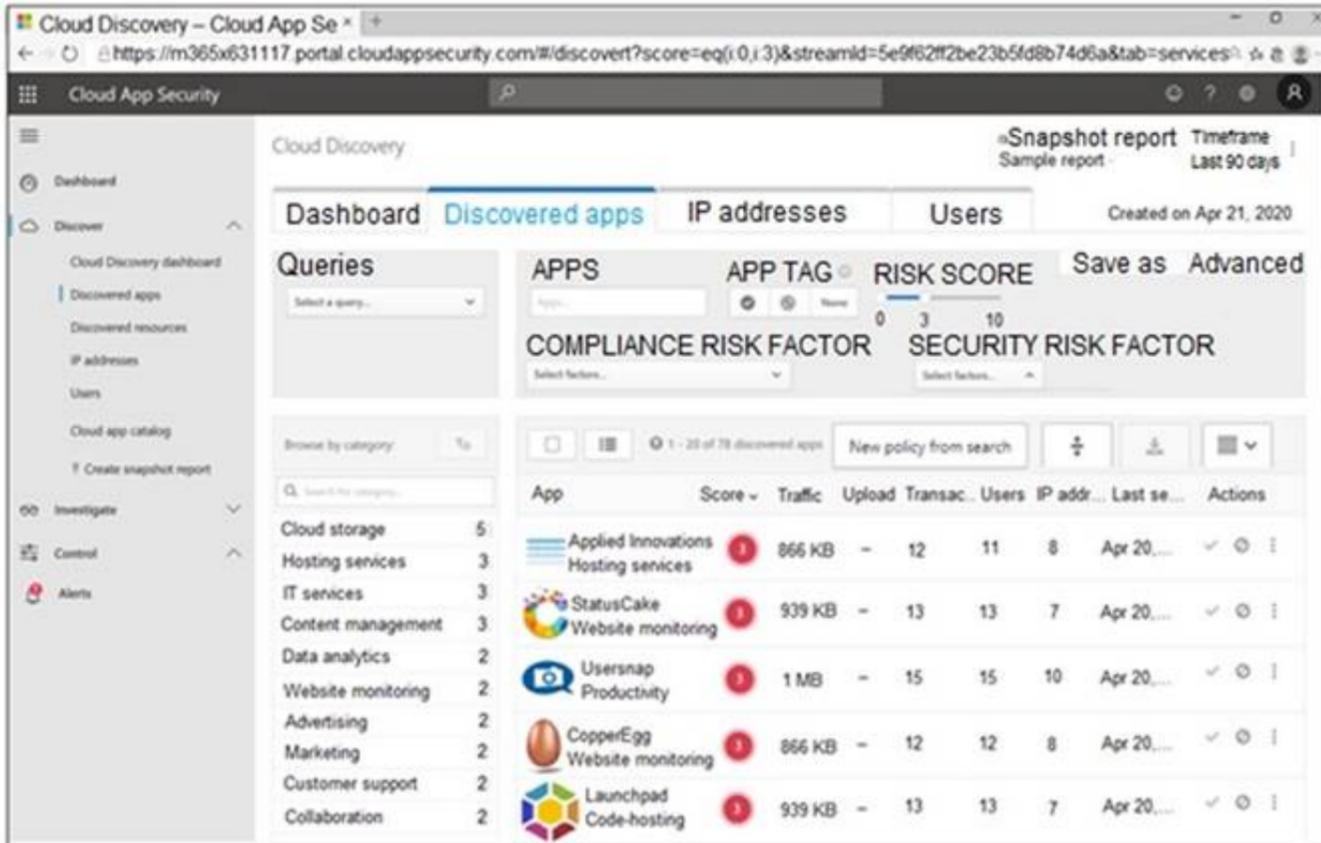


You need to remediate the risk for the Launchpad app.
Which four actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.



A. Mastered
B. Not Mastered

**Answer:** A

**Explanation:**
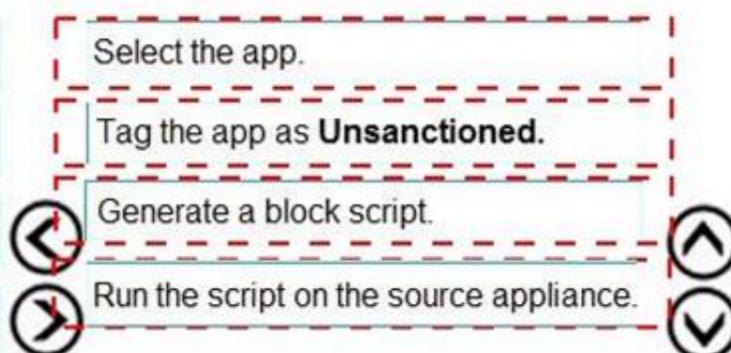
**NEW QUESTION 136**
- (Topic 4)
You have an Azure subscription that uses Microsoft Sentinel.
You need to minimize the administrative effort required to respond to the incidents and remediate the security threats detected by Microsoft Sentinel.
Which two features should you use? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

A. Microsoft Sentinel bookmarks
B. Azure Automation runbooks
C. Microsoft Sentinel automation rules
D. Microsoft Sentinel playbooks
E. Azure Functions apps

**Answer:** CE

**Explanation:**
Reference: https://docs.microsoft.com/en-us/azure/sentinel/tutorial-respond-threats- playbook?tabs=LAC

**NEW QUESTION 139**
HOTSPOT - (Topic 4)
You need to meet the Microsoft Sentinel requirements for collecting Windows Security event logs. What should you do? To answer, select the appropriate options in the answer area. NOTE Each correct selection is worth one point.
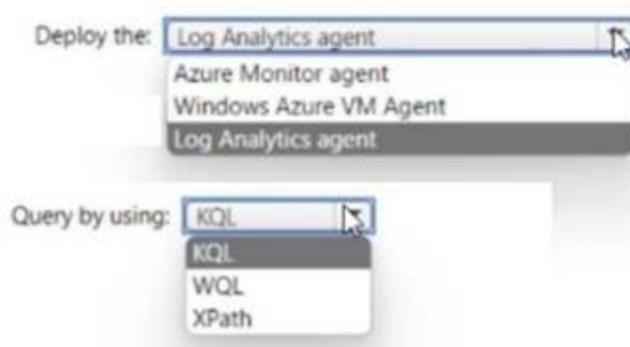


A. Mastered
B. Not Mastered

**Answer:** A

**Explanation:**
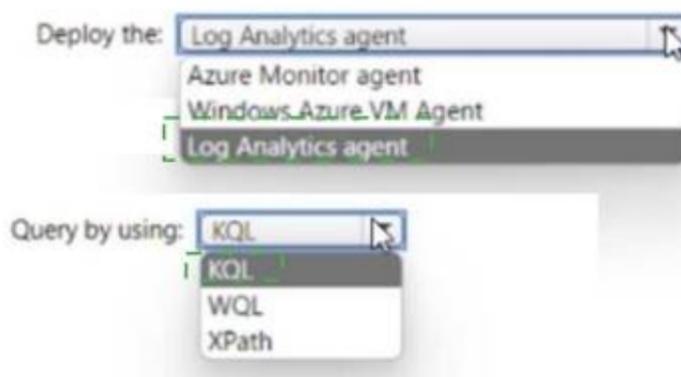


**NEW QUESTION 144**
HOTSPOT - (Topic 4)
You have a Microsoft 365 E5 subscription that uses Microsoft Defender 36S.
Your network contains an on-premises Active Directory Domain Services (AD DS) domain that syncs with Azure AD.
You need to identify the 100 most recent sign-in attempts recorded on devices and AD DS domain controllers.
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**

```
DeviceLogonEvents
| extend Table = 'table1'
| take 100
| union                ▼ (
  join kind=full outer
  join kind=inner
  union
    IdentityLogonEvents  ▼
    IdentityInfo
    IdentityLogonEvents
    IdentityQueryEvents

  | extend Table = 'table2'
  | take 100
)
| project-reorder Timestamp, Table, AccountDomain, AccountName, AccountUpn, AccountSid
| order by Timestamp asc
```

A. Mastered
B. Not Mastered

**Answer:** A

**Explanation:**

**Answer Area**

```
DeviceLogonEvents
| extend Table = 'table1'
| take 100
| union                ▼ (
  join kind=full outer
  join kind=inner
  union
    IdentityLogonEvents  ▼
    IdentityInfo
    IdentityLogonEvents
    IdentityQueryEvents

  | extend Table = 'table2'
  | take 100
)
| project-reorder Timestamp, Table, AccountDomain, AccountName, AccountUpn, AccountSid
| order by Timestamp asc
```

**NEW QUESTION 147**
- (Topic 4)
You have an existing Azure logic app that is used to block Azure Active Directory (Azure AD) users. The logic app is triggered manually.
You deploy Azure Sentinel.
You need to use the existing logic app as a playbook in Azure Sentinel. What should you do first?

A. And a new scheduled query rule.
B. Add a data connector to Azure Sentinel.
C. Configure a custom Threat Intelligence connector in Azure Sentinel.
D. Modify the trigger in the logic app.

**Answer:** D

**Explanation:**
https://docs.microsoft.com/en-us/azure/sentinel/playbook-triggers-actions https://docs.microsoft.com/en-us/azure/sentinel/tutorial-respond-threats-playbook

**NEW QUESTION 148**
HOTSPOT - (Topic 4)
You have a Microsoft 365 E5 subscription that contains 200 Windows 10 devices enrolled

in Microsoft Defender for Endpoint.
You need to ensure that users can access the devices by using a remote shell connection directly from the Microsoft 365 Defender portal. The solution must use the principle of least privilege.
What should you do in the Microsoft 365 Defender portal? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

| To configure Microsoft Defender for Endpoint: | ▼ |
| --- | --- |
| | Turn on endpoint detection and response (EDR) in block mode |
| | Turn on Live Response |
| | Turn off Tamper Protection |

| To configure the devices: | ▼ |
| --- | --- |
| | Add a network assessment job |
| | Create a device group that contains the devices and set Automation level to Full |
| | Create a device group that contains the devices and set Automation level to No automated response |

A. Mastered
B. Not Mastered

**Answer:** A

**Explanation:**
Box 1: Turn on Live Response
Live response is a capability that gives you instantaneous access to a device by using a remote shell connection. This gives you the power to do in-depth investigative work and take immediate response actions.
Box: 2 : Add a network assessment job
Network assessment jobs allow you to choose network devices to be scanned regularly and added to the device inventory.

---

## NEW QUESTION 151
- (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 155
DRAG DROP - (Topic 4)
You have an Azure subscription. The subscription contains 10 virtual machines that are onboarded to Microsoft Defender for Cloud.
You need to ensure that when Defender for Cloud detects digital currency mining behavior on a virtual machine, you receive an email notification. The solution must generate a test email.
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**

| Answer Area |
| --- |

| From Workflow automation in Defender for Cloud, change the status of the workflow automation. |
| From Logic App Designer, run a trigger. |
| From Security alerts in Defender for Cloud, create a sample alert. |
| From Logic App Designer, create a logic app. |
| From Workflow automation in Defender for Cloud, add a workflow automation. |

A. Mastered
B. Not Mastered

**Answer:** A

**Explanation:**
Step 1: From Logic App Designer, create a logic app.
Create a logic app and define when it should automatically run
* 1. From Defender for Cloud's sidebar, select Workflow automation.
* 2. To define a new workflow, click Add workflow automation. The options pane for your new automation opens.
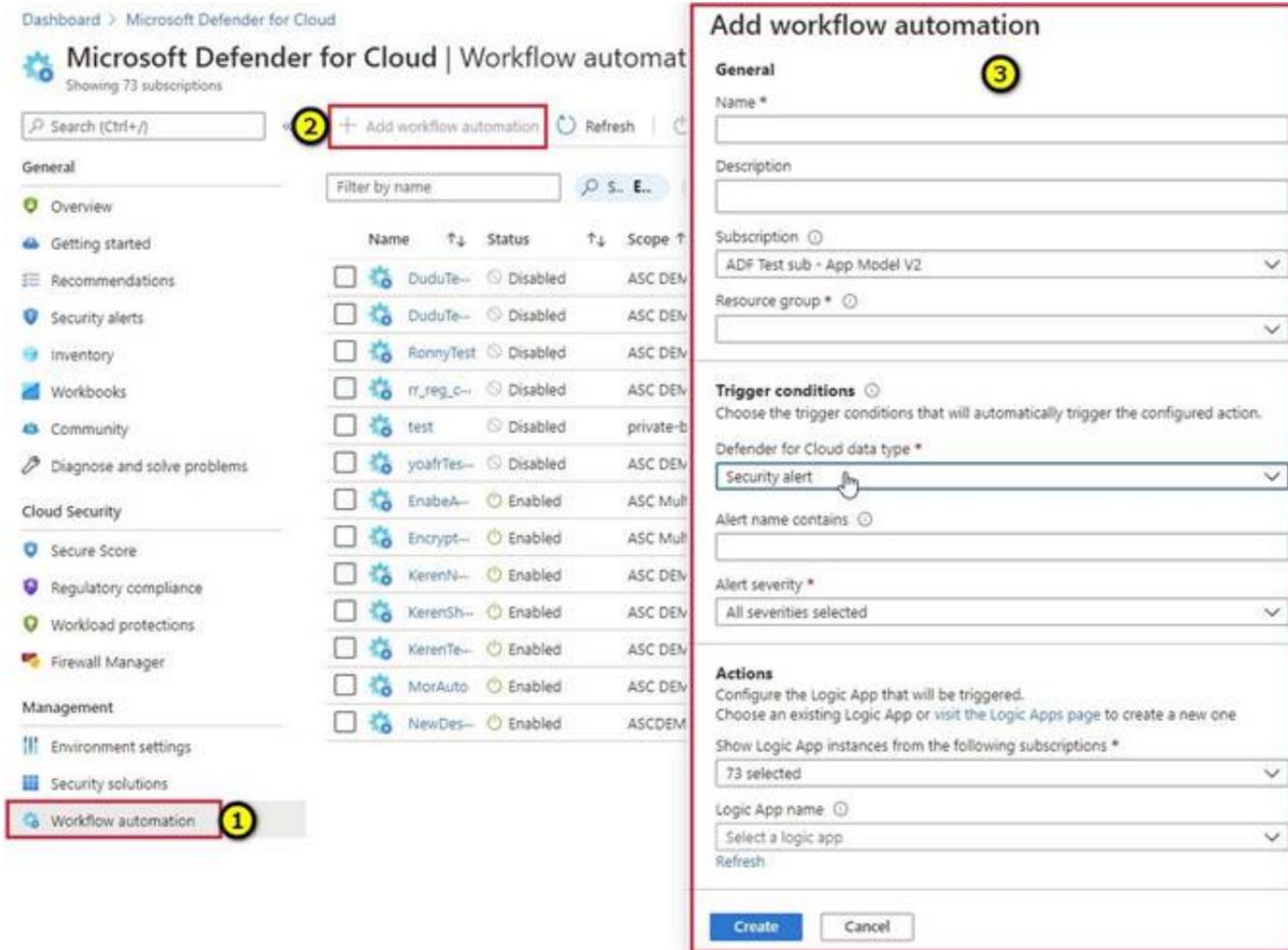
Here you can enter:
A name and description for the automation.
The triggers that will initiate this automatic workflow. For example, you might want your Logic App to run when a security alert that contains "SQL" is generated.
The Logic App that will run when your trigger conditions are met.
* 3. From the Actions section, select visit the Logic Apps page to begin the Logic App creation process.
* 4. Etc.
Step 2: From Logic App Designer, run a trigger. Manually trigger a Logic App
You can also run Logic Apps manually when viewing any security alert or recommendation.
Step 3: From Workflow automation in Defender for cloud, add a workflow automation. Configure workflow automation at scale using the supplied policies
Automating your organization's monitoring and incident response processes can greatly improve the time it takes to investigate and mitigate security incidents.
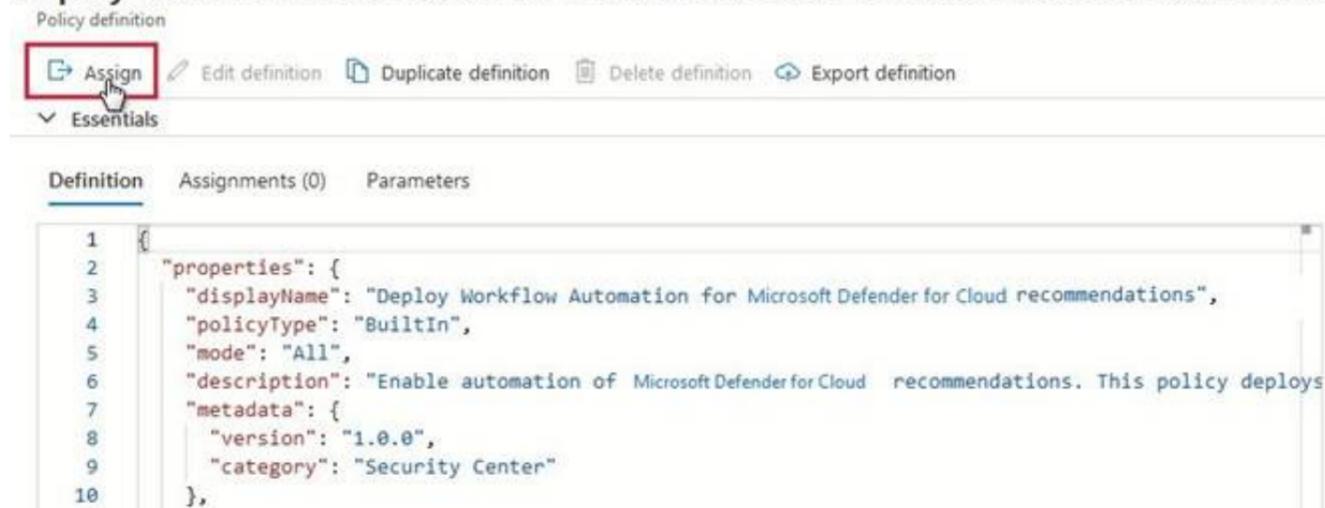


## NEW QUESTION 159
- (Topic 4)
You need to ensure that you can run hunting queries to meet the Microsoft Sentinel requirements. Which type of workspace should you create?

A. Azure Synapse AnarytKS
B. AzureDalabricks
C. Azure Machine Learning
D. LogAnalytics

**Answer:** D


## NEW QUESTION 163
DRAG DROP - (Topic 4)
You have the resources shown in the following table.

| Name | Description |
|---|---|
| SW1 | An Azure Sentinel workspace |
| CEF1 | A Linux sever configured to forward Common Event Format (CEF) logs to SW1 |
| Server1 | A Linux server configured to send Common Event Format (CEF) logs to CEF1 |
| Server2 | A Linux server configured to send Syslog logs to CEF1 |

You need to prevent duplicate events from occurring in SW1.

What should you use for each action? To answer, drag the appropriate resources to the correct actions. Each resource 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.

**Resources**

SW1

CEF1

Server1

Server2

**Answer Area**

From the Syslog configuration, remove the facilities that send CEF messages.

From the Log Analytics agent, disable Syslog synchronization.

A. Mastered
B. Not Mastered

**Answer:** A

**Explanation:**

**Resources**

SW1

CEF1

Server1

Server2

**Answer Area**

From the Syslog configuration, remove the facilities that send CEF messages.  | Server1 |

From the Log Analytics agent, disable Syslog synchronization.  | CEF1 |

**NEW QUESTION 168**
- (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 Mitigate the threat section.

Does this meet the goal?

A. Yes
B. No

**Answer:** A

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

**NEW QUESTION 170**
- (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 scheduled query rule for a data connector. 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 173**
- (Topic 4)
You need to configure Microsoft Cloud App Security to generate alerts and trigger remediation actions in response to external sharing of confidential files.
Which two actions should you perform in the Cloud App Security portal? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

A. From Settings, select Information Protection, select Azure Information Protection, and then select Only scan files for Azure Information Protection classification labels and content inspection warnings from this tenant
B. Select Investigate files, and then filter App to Office 365.
C. Select Investigate files, and then select New policy from search
D. From Settings, select Information Protection, select Azure Information Protection, and then select Automatically scan new files for Azure Information Protection classification labels and content inspection warnings
E. From Settings, select Information Protection, select Files, and then enable file monitoring.
F. Select Investigate files, and then filter File Type to Document.

**Answer:** DE

**Explanation:**
Reference:
https://docs.microsoft.com/en-us/cloud-app-security/tutorial-dlp https://docs.microsoft.com/en-us/cloud-app-security/azip-integration

**NEW QUESTION 176**
- (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 179**
HOTSPOT - (Topic 4)
You have a Microsoft Sentinel workspace named sws1.
You need to create a query that will detect when a user creates an unusually large numbers of Azure AD user accounts.
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 Area**

A. Mastered
B. Not Mastered

**Answer:** A

**Explanation:**

**Answer Area**

```
AzureActivity                    ▼
  AuditLogs
  AzureActivity                    user"
  BehaviorAnalytics              s "True"
  SecurityEvent

| where ActionType == "Add user"

| where ActivityInsights has "True"

| join(

BehaviorAnalytics               ▼
  AuditLogs
  AzureActivity                  = $right._ItemId
  BehaviorAnalytics
  SecurityEvent
                    ostring(UsersInsights.AccountDisplayName),

| sort by TimeGenerated desc

| project TimeGenerated, UserName, UserPrincipalName, UsersInsights,
ActivityType,_ActionType
```

**NEW QUESTION 183**
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 188**
HOTSPOT - (Topic 4)
You need to assign role-based access control (RBAQ roles to Group1 and Group2 to meet The Microsoft Defender for Cloud requirements and the business requirements Which role should you assign to each group? 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 193**
- (Topic 4)
You provision a Linux virtual machine in a new Azure subscription.
You enable Azure Defender and onboard the virtual machine to Azure Defender.
You need to verify that an attack on the virtual machine triggers an alert in Azure Defender. Which two Bash commands should you run on the virtual machine? Each correct answer
presents part of the solution.
NOTE: Each correct selection is worth one point.

A. cp /bin/echo ./asc_alerttest_662jfi039n
B. ./alerttest testing eicar pipe
C. cp /bin/echo ./alerttest
D. ./asc_alerttest_662jfi039n testing eicar pipe

**Answer:** AD

**Explanation:**
Reference:
https://docs.microsoft.com/en-us/azure/security-center/security-center-alert-validation#simulate-alerts-on-your- azure-vms-linux-

**NEW QUESTION 198**
- (Topic 4)
You have an Azure subscription that uses Microsoft Defender for Servers Plan 1 and contains a server named Server1.
You enable agentless scanning.
You need to prevent Server1 from being scanned. The solution must minimize administrative effort.
What should you do?

A. Create an exclusion tag.
B. Upgrade the subscription to Defender for Servers Plan 2.
C. Create a governance rule.
D. Create an exclusion group.

**Answer:** D

**NEW QUESTION 203**
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.

**Answer Area**

```
SecurityEvent
| where EventID in ("4624","4672")
| where Computer == "SERVER1"
| join kind=inner (
| join kind=fullouter (          These are the selections for the first missing value.
| join kind=inner (
| join kind=innerunique (
IdentityInfo
BehaviorAnalytics            rated, *) by AccountObjectId) on $left.SubjectUserSid == $right.AccountSID
IdentityInfo
| wh SecurityEvent
```

A. Mastered
B. Not Mastered

**Answer:** A

**Explanation:**

**Answer Area**

```
SecurityEvent
| where EventID in ("4624","4672")
| where Computer == "SERVER1"
| join kind=inner (
| join kind=fullouter (          These are the selections for the first missing value.
| join kind=inner (
| join kind=innerunique (
IdentityInfo
BehaviorAnalytics            rated, *) by AccountObjectId) on $left.SubjectUserSid == $right.AccountSID
IdentityInfo
| wh SecurityEvent
```

**NEW QUESTION 204**
- (Topic 4)
You have an Azure subscription that contains a Log Analytics workspace.
You need to enable just-in-time (JIT) VM access and network detections for Azure resources.
Where should you enable Azure Defender?

A. at the subscription level
B. at the workspace level
C. at the resource level

**Answer:** A

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

**NEW QUESTION 207**
- (Topic 4)
You need to deploy the native cloud connector to Account! to meet the Microsoft Defender for Cloud requirements. What should you do in Account! first?

A. Create an AWS user for Defender for Cloud.
B. Create an Access control (1AM) role for Defender for Cloud.
C. Configure AWS Security Hub.
D. Deploy the AWS Systems Manager (SSM) agent

**Answer:** D

**NEW QUESTION 212**
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 214**
- (Topic 4)
You are configuring Azure Sentinel.
You need to send a Microsoft Teams message to a channel whenever a sign-in from a suspicious IP address is detected.
Which two actions should you perform in Azure Sentinel? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

A. Add a playbook.
B. Associate a playbook to an incident.
C. Enable Entity behavior analytics.
D. Create a workbook.
E. Enable the Fusion rule.

**Answer:** AB

**Explanation:**
Reference:
https://docs.microsoft.com/en-us/azure/sentinel/tutorial-respond-threats-playbook

**NEW QUESTION 218**
- (Topic 4)
You have five on-premises Linux servers.
You have an Azure subscription that uses Microsoft Defender for Cloud. You need to use Defender for Cloud to protect the Linux servers.
What should you install on the servers first?

A. the Dependency agent
B. the Log Analytics agent
C. the Azure Connected Machine agent
D. the Guest Configuration extension

**Answer:** B

**Explanation:**
Defender for Cloud depends on the Log Analytics agent. Use the Log Analytics agent if you need to:

* Collect logs and performance data from Azure virtual machines or hybrid machines hosted outside of Azure
* Etc.
Reference:
https://docs.microsoft.com/en-us/azure/defender-for-cloud/os-coverage https://docs.microsoft.com/en-us/azure/azure-monitor/agents/agents-overview#log-analytics-agent

**NEW QUESTION 223**
HOTSPOT - (Topic 4)
Your network contains an on-premises Active Directory Domain Services (AD DS) domain that syncs with Azure AD.
You have a Microsoft 365 E5 subscription that uses Microsoft Defender 365.
You need to identify all the interactive authentication attempts by the users in the finance department of your company.
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**

```
IdentityQueryEvents          ▼
BehaviorAnalytics
IdentityInfo
IdentityQueryEvents

| where Department == 'Finance'

| project-rename objid = AccountObjectId

| join    AuditLogs          ▼    on $left.objid == $right.AccountObjectId
          AuditLogs
          IdentityLogonEvents
          SigninLogs
```

A. Mastered
B. Not Mastered

**Answer:** A

**Explanation:**

**Answer Area**

```
IdentityQueryEvents          ▼
BehaviorAnalytics
IdentityInfo
IdentityQueryEvents

| where Department == 'Finance'

| project-rename objid = AccountObjectId

| join    AuditLogs          ▼    on $left.objid == $right.AccountObjectId
          AuditLogs
          IdentityLogonEvents
          SigninLogs
```

**NEW QUESTION 228**
DRAG DROP - (Topic 4)
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

**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

[ ]

[ ]

A. Mastered
B. Not Mastered

**Answer:** A

**Explanation:**

**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**

DeviceLogonEvents

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

ActionType == FailureReason

| summarize LogonFailures=count()
by DeviceName, LogonType

**NEW QUESTION 230**
DRAG DROP - (Topic 4)
You have an Azure subscription linked to an Azure Active Directory (Azure AD) tenant. The tenant contains two users named User1 and User2.
You plan to deploy Azure Defender.
You need to enable User1 and User2 to perform tasks at the subscription level as shown in the following table.

| User | Task |
|------|------|
| User1 | • Assign initiatives<br>• Edit security policies<br>• Enable automatic provisioning |
| User2 | • View alerts and recommendations<br>• Apply security recommendations<br>• Dismiss alerts |

The solution must use the principle of least privilege.
Which role should you assign to each user? To answer, drag the appropriate roles to the correct users. 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.

**Roles**

| Contributor |
| Owner |
| Security administrator |
| Security reader |

**Answer Area**

User1: [ ]

User2: [ ]

A. Mastered
B. Not Mastered

**Answer:** A

**Explanation:**
Box 1: Owner
Only the Owner can assign initiatives.
Box 2: Contributor
Only the Contributor or the Owner can apply security recommendations.


**NEW QUESTION 232**
- (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 233**
- (Topic 4)
Your company stores the data for every project in a different Azure subscription. All the subscriptions use the same Azure Active Directory (Azure AD) tenant.
Every project consists of multiple Azure virtual machines that run Windows Server. The Windows events of the virtual machines are stored in a Log Analytics workspace in each machine's respective subscription.
You deploy Azure Sentinel to a new Azure subscription.
You need to perform hunting queries in Azure Sentinel to search across all the Log Analytics workspaces of all the subscriptions.
Which two actions should you perform? Each correct answer presents part of the solution. NOTE: Each correct selection is worth one point.

A. Add the Security Events connector to the Azure Sentinel workspace.
B. Create a query that uses the workspace expression and the union operator.
C. Use the alias statement.
D. Create a query that uses the resource expression and the alias operator.
E. Add the Azure Sentinel solution to each workspace.

**Answer:** BE

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


**NEW QUESTION 235**
DRAG DROP - (Topic 4)
You plan to connect an external solution that will send Common Event Format (CEF) messages to Azure Sentinel.
You need to deploy the log forwarder.
Which three actions should you perform in sequence? To answer, move the appropriate actions form the list of actions to the answer area and arrange them in the correct order.

## Actions

| Deploy an OMS Gateway on the network. |
| --- |

| Set the syslog daemon to forward the events directly to Azure Sentinel. |
| --- |

| Configure the syslog daemon. Restart the syslog daemon and the Log Analytics agent. |
| --- |

| Download and install the Log Analytics agent. |
| --- |

| Set the Log Analytics agent to listen on port 25226 and forward the CEF messages to Azure Sentinel. |
| --- |

## Answer Area

A. Mastered
B. Not Mastered

**Answer:** A

**Explanation:**

## Actions

| Deploy an OMS Gateway on the network. |
| --- |

| Set the syslog daemon to forward the events directly to Azure Sentinel. |
| --- |

| Configure the syslog daemon. Restart the syslog daemon and the Log Analytics agent. |
| --- |

| Download and install the Log Analytics agent. |
| --- |

| Set the Log Analytics agent to listen on port 25226 and forward the CEF messages to Azure Sentinel. |
| --- |

## Answer Area

| Download and install the Log Analytics agent. |
| --- |

| Set the Log Analytics agent to listen on port 25226 and forward the CEF messages to Azure Sentinel. |
| --- |

| Configure the syslog daemon. Restart the syslog daemon and the Log Analytics agent. |
| --- |

**NEW QUESTION 238**
HOTSPOT - (Topic 4)
You purchase a Microsoft 365 subscription.
You plan to configure Microsoft Cloud App Security.
You need to create a custom template-based policy that detects connections to Microsoft 365 apps that originate from a botnet network.
What should you use? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

**Policy template type:**

| ▼ |
| --- |
| Access policy |
| Activity policy |
| Anomaly detection policy |

**Filter based on:**

| ▼ |
| --- |
| IP address tag |
| Source |
| User agent string |

A. Mastered
B. Not Mastered

**Answer:** A

**Explanation:**

**Policy template type:**

| Access policy |
| Activity policy |
| Anomaly detection policy |

**Filter based on:**

| IP address tag |
| Source |
| User agent string |

**NEW QUESTION 240**
HOTSPOT - (Topic 4)
You have an Azure subscription that uses Microsoft Defender for Cloud. You create a Google Cloud Platform (GCP) organization named GCP1.
You need to onboard GCP1 to Defender for Cloud by using the native cloud connector. The solution must ensure that all future GCP projects are onboarded automatically.
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.

Answer Area

Create: A management project and a custom role
A management group and an Azure AD service principal
**A management project and a custom role**
An Azure AD administrative unit and a managed identity

By: Running a script in GCP Cloud Shell
Deploying a Bicep template
Running a script in Azure Cloud Shell
**Running a script in GCP Cloud Shell**

A. Mastered
B. Not Mastered

**Answer:** A

**Explanation:**

Answer Area

Create: A management project and a custom role
A management group and an Azure AD service principal
**A management project and a custom role**
An Azure AD administrative unit and a managed identity

By: Running a script in GCP Cloud Shell
Deploying a Bicep template
Running a script in Azure Cloud Shell
**Running a script in GCP Cloud Shell**

**NEW QUESTION 241**
HOTSPOT - (Topic 4)
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 area. NOTE Each correct selection is worth one point.
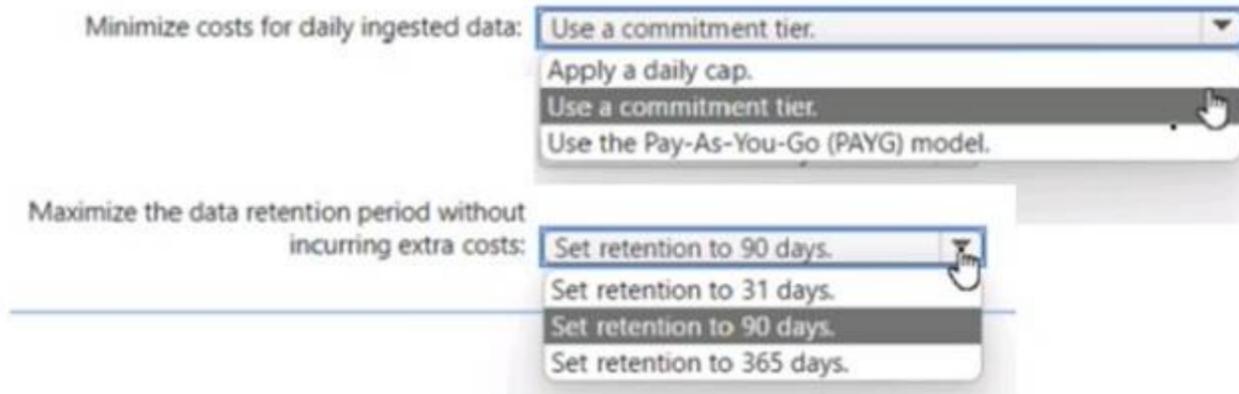
A. Mastered
B. Not Mastered

**Answer:** A

**Explanation:**
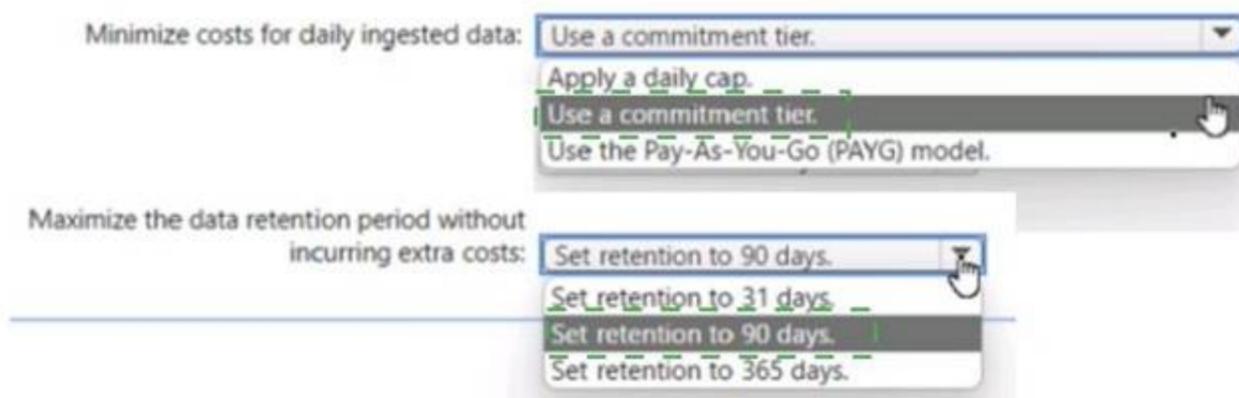


**NEW QUESTION 244**
- (Topic 4)
You have a playbook in Azure Sentinel.
When you trigger the playbook, it sends an email to a distribution group.
You need to modify the playbook to send the email to the owner of the resource instead of the distribution group.
What should you do?

A. Add a parameter and modify the trigger.
B. Add a custom data connector and modify the trigger.
C. Add a condition and modify the action.
D. Add a parameter and modify the action.

**Answer:** D

**Explanation:**
Reference:
https://azsec.azurewebsites.net/2020/01/19/notify-azure-sentinel-alert-to-your-email- automatically/

**NEW QUESTION 246**
- (Topic 4)
You are configuring Azure Sentinel.
You need to send a Microsoft Teams message to a channel whenever an incident representing a sign-in risk event is activated in Azure Sentinel.
Which two actions should you perform in Azure Sentinel? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

A. Enable Entity behavior analytics.
B. Associate a playbook to the analytics rule that triggered the incident.
C. Enable the Fusion rule.
D. Add a playbook.
E. Create a workbook.

**Answer:** AB

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

**NEW QUESTION 248**
- (Topic 4)
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. Block DeviceProcessEvents with DeviceNetworkEvents.
E. Add DeviceId and ReportId to the output of the query.

**Answer:** AE

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

**NEW QUESTION 250**
- (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 253**
HOTSPOT - (Topic 4)
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.

If you hover over the virtual machine named vm1, you 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 |

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

| ▼ |
| --- |
| Entities |
| Info |
| Insights |
| Timeline |

A. Mastered
B. Not Mastered

**Answer:** A

**Explanation:**

If you hover over the virtual machine named vm1, you 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 |

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

| ▼ |
| --- |
| Entities |
| Info |
| Insights |
| Timeline |

**NEW QUESTION 255**
- (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 259**
- (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 260**
- (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 Azure Identity Protection, you configure the sign-in risk policy. Does this meet the goal?

A. Yes
B. No

**Answer:** B

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

**NEW QUESTION 263**
- (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 268**
- (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 270**
- (Topic 4)
You have a Microsoft Sentinel playbook that is triggered by using the Azure Activity connector.
You need to create a new near-real-time (NRT) analytics rule that will use the playbook. What should you configure for the rule?

A. the Incident automation settings
B. entity mapping
C. the query rule
D. the Alert automation settings

**Answer:** B

**NEW QUESTION 271**
- (Topic 4)
A company uses Azure Sentinel.
You need to create an automated threat response. What should you use?

A. a data connector

B. a playbook
C. a workbook
D. a Microsoft incident creation rule

**Answer:** B

**Explanation:**
Reference:
https://docs.microsoft.com/en-us/azure/sentinel/tutorial-respond-threats-playbook

**NEW QUESTION 272**
DRAG DROP - (Topic 4)
You have a Microsoft Sentinel workspace named workspace1 and an Azure virtual machine named VM1.
You receive an alert for suspicious use of PowerShell on VM1.
You need to investigate the incident, identify which event triggered the alert, and identify whether the following actions occurred on VM1 after the alert:
? The modification of local group memberships
? The purging of event logs
Which three actions should you perform in sequence in the Azure portal? 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:**
Step 1: From the Investigation blade, select Insights
The Investigation Insights Workbook is designed to assist in investigations of Azure Sentinel Incidents or individual IP/Account/Host/URL entities.
Step 2: From the Investigation blade, select the entity that represents VM1.
The Investigation Insights workbook is broken up into 2 main sections, Incident Insights
and Entity Insights.
Incident Insights
The Incident Insights gives the analyst a view of ongoing Sentinel Incidents and allows for quick access to their associated metadata including alerts and entity information.
Entity Insights
The Entity Insights allows the analyst to take entity data either from an incident or through manual entry and explore related information about that entity. This workbook presently provides view of the following entity types:
IP Address Account Host
URL
Step 3: From the details pane of the incident, select Investigate. Choose a single incident and click View full details or Investigate.

**NEW QUESTION 275**
DRAG DROP - (Topic 4)
You have a Microsoft Sentinel workspace that contains an Azure AD data connector. You need to associate a bookmark with an Azure AD-related incident.
What should you do? To answer, drag the appropriate blades to the correct tasks. Each blade 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:**
You can use the Logs blade or incident blade to create a bookmark of an Azure AD-related incident. Once the bookmark is created, you can associate it with the incident by using the incident blade. This allows you to quickly and easily access important information related to the incident in the future.

**NEW QUESTION 280**
- (Topic 4)
You have an Azure subscription that uses Microsoft Sentinel.
You need to create a custom report that will visualise sign-in information over time.
What should you create first?

A. a workbook

B. a hunting query
C. a notebook
D. a playbook

**Answer:** A

**Explanation:**
A workbook is a data-driven interactive report in Microsoft Sentinel. You can use workbooks to create custom reports based on data from your Azure subscription.
Reference: https://docs.microsoft.com/en-us/azure/sentinel/workbooks-overview


**NEW QUESTION 284**
HOTSPOT - (Topic 4)
You have an Azure subscription that uses Azure Defender.
You plan to use Azure Security Center workflow automation to respond to Azure Defender threat alerts.
You need to create an Azure policy that will perform threat remediation automatically. 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.

Set available effects to:

| ▼ |
| --- |
| Append |
| DeployIfNotExists |
| EnforceRegoPolicy |

To perform remediation use:

| ▼ |
| --- |
| An Azure Automation runbook that has a webhook |
| An Azure Logic Apps app that has the trigger set to When an Azure Security Center Alert is created or triggered |
| An Azure Logic Apps app that has the trigger set to When a response to an Azure Security Center alert is triggered |

A. Mastered
B. Not Mastered

**Answer:** A

**Explanation:**

Set available effects to:

| ▼ |
| --- |
| Append |
| DeployIfNotExists |
| EnforceRegoPolicy |

To perform remediation use:

| ▼ |
| --- |
| An Azure Automation runbook that has a webhook |
| An Azure Logic Apps app that has the trigger set to When an Azure Security Center Alert is created or triggered |
| An Azure Logic Apps app that has the trigger set to When a response to an Azure Security Center alert is triggered |


**NEW QUESTION 288**
- (Topic 4)
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. What should you do?

A. From Security alerts, select the alert, select Take Action, and then expand the Prevent future attacks section.
B. From Security alerts, select Take Action, and then expand the Mitigate the threat section.
C. From Regulatory compliance, download the report.
D. From Recommendations, download the CSV report.

**Answer:** B

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


**NEW QUESTION 290**
DRAG DROP - (Topic 4)
You have a Microsoft 365 E5 subscription that uses Microsoft Exchange Online. You need to identify phishing email messages.
Which three cmdlets should you run in sequence? To answer, move the appropriate cmdlets from the list of cmdlets to the answer area and arrange them in the
correct order.

| Cmdlets | | Answer Area |
|---|---|---|
| Connect-IPPSSession | | |
| Start-ComplianceSearch | | |
| New-ComplianceSearch | > | |
| Connect-ExchangeOnline | < | |
| Search-UnifiedAuditLog | | |

A. Mastered
B. Not Mastered

**Answer:** A

**Explanation:**

| Cmdlets | Answer Area |
|---|---|
| Connect-IPPSSession | New-ComplianceSearch |
| Start-ComplianceSearch | Connect-ExchangeOnline |
| New-ComplianceSearch | Search-UnifiedAuditLog |
| Connect-ExchangeOnline | |
| Search-UnifiedAuditLog | |

**NEW QUESTION 293**
HOTSPOT - (Topic 4)
You use Azure Sentinel to monitor irregular Azure activity.
You create custom analytics rules to detect threats as shown in the following exhibit.

Home > Azure Sentinel workspaces > Azure Sentinel

## Analytics rule wizard – Edit existing rule
DeployVM

General   **Set rule logic**   Incident settings   Automated response   Review and create

Define the logic for your new analytics rule.

Rule query
Any time details set here will be within the scope defined below in the Query scheduling fields.

```
AzureActivity
| where OperationName == "Create or Update Virtual Machine"
or OperationName == "Create Deployment"
| where ActivityStatus == "Succeeded"
| make-series dcount(ResourceId) default=0
on EventSubmissionTimestamp in range(ago(7d), now(), 1d) by Caller
```

View query results >

## Map entities

Map the entities recognized by Azure Sentinel to the appropriate columns available in your query results. This enables Azure Sentinel to recognize the entities that are part of the alerts for further analysis. Entity type must be a string.

| Entity Type | Column | |
|---|---|---|
| Account | Choose column ⌄ | Add |
| Host | Choose column ⌄ | Add |
| IP | Choose column ⌄ | Add |
| URL | Choose column ⌄ | Add |
| FileHash | Choose column ⌄ | Add |

### Query scheduling

Run query every *
| 5 | ✓ | Minutes ⌄ |

Lookup data from the last * ⓘ
| 5 | | Hours ⌄ |

### Alert threshold

Generate alert when number of query results *
| Is greater than ⌄ | 2 ✓ |

### Event grouping

Configure how rule query results are grouped into alerts
◉ Group all events into a single alert
◯ Trigger an alert for each event

### Suppression

Stop running query after alert is generated ⓘ
[ On | Off ]

Stop running query for *
| 5 | ✓ | Hours ⌄ |

[ Previous ]  [ **Next : Incident settings >** ]

You do NOT define any incident settings as part of the rule definition.
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.

If a user deploys three Azure virtual machines simultaneously, how many times will you receive **[answer choice]** in the next five hours.

| ⌄ |
|---|
| 0 alerts |
| 1 alert |
| 2 alerts |
| 3 alerts |

If three separate users deploy one Azure virtual machine each within five minutes of each other, you will receive **[answer choice]**.

| ⌄ |
|---|
| 0 alerts |
| 1 alert |
| 2 alerts |
| 3 alerts |

A. Mastered
B. Not Mastered

**Answer:** A

**Explanation:**
Graphical user interface, text, application, email Description automatically generated


**NEW QUESTION 294**
- (Topic 4)
You are investigating a potential attack that deploys a new ransomware strain.
You plan to perform automated actions on a group of highly valuable machines that contain sensitive information.
You have three custom device groups.
You need to be able to temporarily group the machines to perform actions on the devices. Which three actions should you perform? Each correct answer presents part of the solution. NOTE: Each correct selection is worth one point.

A. Add a tag to the device group.
B. Add the device users to the admin role.
C. Add a tag to the machines.
D. Create a new device group that has a rank of 1.
E. Create a new admin role.
F. Create a new device group that has a rank of 4.

**Answer:** ACD

**Explanation:**
https://docs.microsoft.com/en-us/learn/modules/deploy-microsoft-defender-for-endpoints- environment/4-manage-access


**NEW QUESTION 298**
- (Topic 4)
You have a Microsoft 365 E5 subscription that uses Microsoft Defender for Endpoint
You need to identify any devices that triggered a malware alert and collect evidence related to the alert. The solution must ensure that you can use the results to initiate device isolation for the affected devices.
What should you use in the Microsoft 365 Defender portal?

A. Incidents
B. Investigations
C. Advanced hunting
D. Remediation

**Answer:** A


**NEW QUESTION 302**
- (Topic 4)
You have a Microsoft 365 subscription that uses Azure Defender. You have 100 virtual machines in a resource group named RG1.
You assign the Security Admin roles to a new user named SecAdmin1.
You need to ensure that SecAdmin1 can apply quick fixes to the virtual machines by using Azure Defender. The solution must use the principle of least privilege.
Which role should you assign to SecAdmin1?

A. the Security Reader role for the subscription
B. the Contributor for the subscription
C. the Contributor role for RG1
D. the Owner role for RG1

**Answer:** C


**NEW QUESTION 305**
- (Topic 4)
You have a third-party security information and event management (SIEM) solution.
You need to ensure that the SIEM solution can generate alerts for Azure Active Directory (Azure AD) sign-events in near real time.
What should you do to route events to the SIEM solution?

A. Create an Azure Sentinel workspace that has a Security Events connector.
B. Configure the Diagnostics settings in Azure AD to stream to an event hub.
C. Create an Azure Sentinel workspace that has an Azure Active Directory connector.
D. Configure the Diagnostics settings in Azure AD to archive to a storage account.

**Answer:** B

**Explanation:**
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/overview- monitoring


**NEW QUESTION 310**
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 311**
......

100% Valid and Newest Version SC-200 Questions & Answers shared by Certleader
https://www.certleader.com/SC-200-dumps.html (197 Q&As)

# Thank You for Trying Our Product

* 100% Pass or Money Back

   All our products come with a 90-day Money Back Guarantee.

* One year free update

   You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

   We currently serve more than 30,000,000 customers.

* Shop Securely

   All transactions are protected by VeriSign!

**100% Pass Your SC-200 Exam with Our Prep Materials Via below:**

https://www.certleader.com/SC-200-dumps.html