QUESTION 63
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:
https://docs.microsoft.com/en-us/azure/security-center/enable-azure-defender

QUESTION 64
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 app that has a manual trigger.
C. Create an Azure logic app that has an Azure Security Center alert trigger.
D. Create an Azure logic app that has an HTTP trigger.
E. From Azure Active Directory (Azure AD), add an app registration.

Answer: AC
Explanation:
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

QUESTION 65
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:
https://docs.microsoft.com/en-us/azure/sentinel/connect-data-sources

QUESTION 66
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:
https://docs.microsoft.com/en-us/azure/sentinel/tutorial-respond-threats-playbook

QUESTION 67
You have an Azure Sentinel deployment in the East US Azure region.
You create a Log Analytics workspace named LogsWest in the West US Azure region.
You need to ensure that you can use scheduled analytics rules in the existing Azure Sentinel deployment to generate alerts based on queries to LogsWest.
What should you do first?

A. Deploy Azure Data Catalog to the West US Azure region.
B. Modify the workspace settings of the existing Azure Sentinel deployment.
C. Add Azure Sentinel to a workspace.
D. Create a data connector in Azure Sentinel.

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

QUESTION 68
You create a custom analytics rule to detect threats in Azure Sentinel.
You discover that the rule fails intermittently.
What are two possible causes of the failures? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

A. The rule query takes too long to run and times out.
B. The target workspace was deleted.
C. Permissions to the data sources of the rule query were modified.
D. There are connectivity issues between the data sources and Log Analytics

Answer: AD
Explanation:
Incorrect Answers:
B: This would cause it to fail every time, not just intermittently.
C: This would cause it to fail every time, not just intermittently.

QUESTION 69

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

QUESTION 70
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:
https://docs.microsoft.com/en-us/azure/sentinel/connect-azure-security-center

QUESTION 71
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:
https://docs.microsoft.com/en-us/azure/sentinel/connect-azure-security-center

QUESTION 72

Hotspot Question
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.

Answer Area

```
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 ]
```

Answer:

Answer Area

```
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 ]
```

Explanation:
https://docs.microsoft.com/en-us/microsoft-365/security/defender/advanced-hunting-query-emails-devices?view=o365-

worldwide

QUESTION 73
Hotspot Question
You have a Microsoft 365 E5 subscription that uses Microsoft Defender and an Azure subscription that uses Azure Sentinel.
You need to identify all the devices that contain files in emails sent by a known malicious email sender. The query will be based on the match of the SHA256 hash.
How should you complete the query? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Answer Area

```
EmailAttachmentInfo
| where SenderFromAddress =~ "MaliciousSender@example.com"
where isnotempty [ ▼ ]
```

(DeviceId)
(RecipientEmailAddress)
(SenderFromAddress)
(SHA256)

```
| join (
DeviceFileEvents
| project FileName, SHA256
) on [ ▼ ]
```

(DeviceId)
(RecipientEmailAddress)
(SenderFromAddress)
(SHA256)

```
| project Timestamp, FileName, SHA256, DeviceName, DeviceId,
NetworkMessageId, SenderFromAddress, RecipientEmailAddress
```

Answer:

Answer Area

```
EmailAttachmentInfo
| where SenderFromAddress =~ "MaliciousSender@example.com"
where isnotempty [ ▼ ]
```

(DeviceId)
(RecipientEmailAddress)
(SenderFromAddress)
(SHA256)

```
| join (
DeviceFileEvents
| project FileName, SHA256
) on [ ▼ ]
```

(DeviceId)
(RecipientEmailAddress)
(SenderFromAddress)
(SHA256)

```
| project Timestamp, FileName, SHA256, DeviceName, DeviceId,
NetworkMessageId, SenderFromAddress, RecipientEmailAddress
```

Explanation:
https://docs.microsoft.com/en-us/microsoft-365/security/defender/advanced-hunting-query-emails-devices?view=o365-worldwide

QUESTION 74
Hotspot Question
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.

Answer Area

```
"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]"
        }
      ],
```

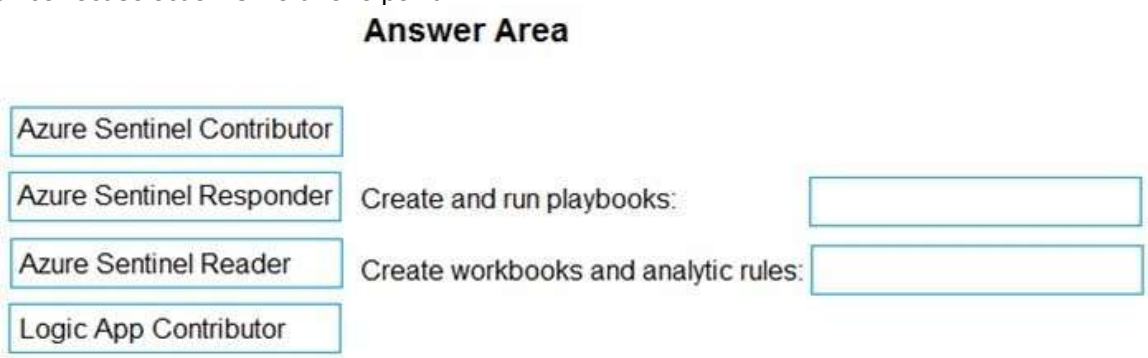
Answer:

Answer Area

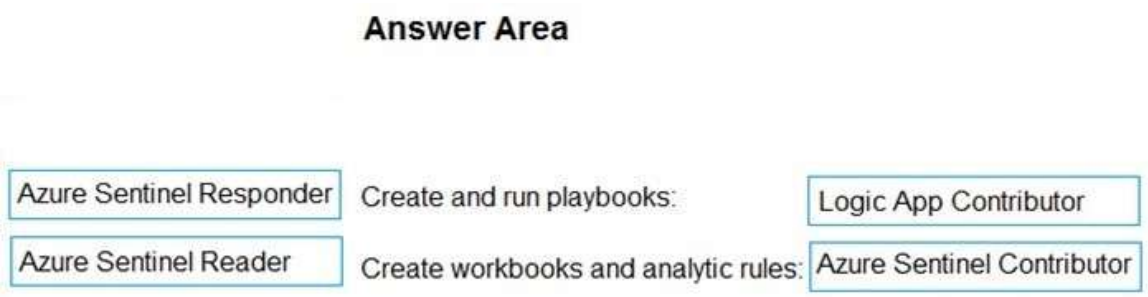
```
"resources": [
  {
    "type": "Microsoft.Security/automations",
    "apiVersion": "2019-01-01-preview",
    "name": "[parameters('name')]",
    "location": "[parameters('location')]",
    "properties": {
      "description": "[format(variables('description'), '{0}', parameters
('subscriptionId'))]",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

Explanation:
https://docs.microsoft.com/en-us/azure/security-center/quickstart-automation-alert

QUESTION 75
Drag and Drop Question
Your company deploys Azure Sentinel.
You plan to delegate the administration of Azure Sentinel to various groups.
You need to delegate the following tasks:
- Create and run playbooks
- Create workbooks and analytic rules.
The solution must use the principle of least privilege.
Which role should you assign for each task? To answer, drag the appropriate roles to the correct tasks. Each role may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.
NOTE: Each correct selection is worth one point.

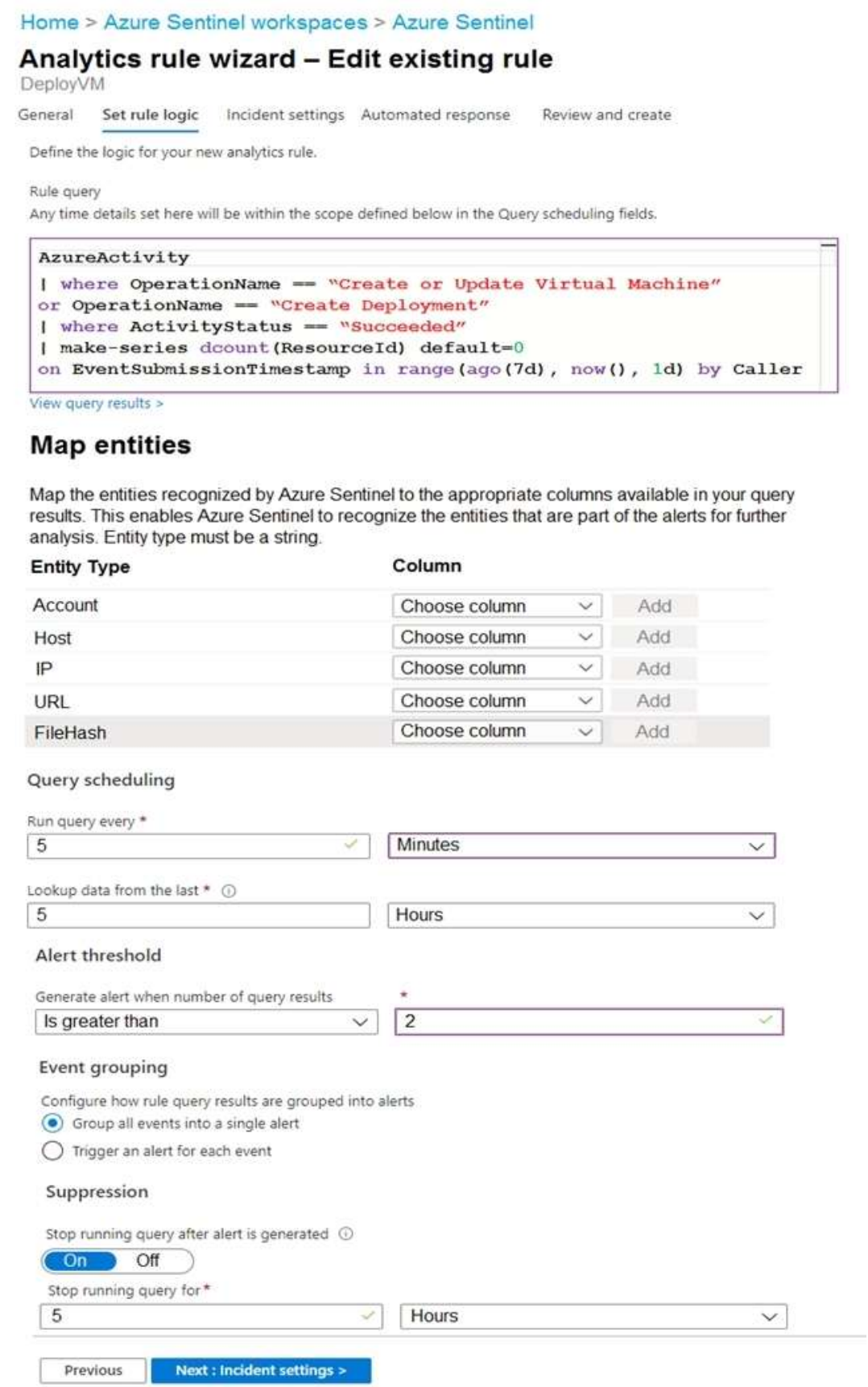


Answer:



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

QUESTION 76
Hotspot Question
You use Azure Sentinel to monitor irregular Azure activity.
You create custom analytics rules to detect threats as shown in the following exhibit.



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.

Answer Area

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

Answer:

Answer Area

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

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

QUESTION 77
You are using the Microsoft 365 Defender portal to conduct an investigation into a multi-stage incident related to a suspected malicious document. After reviewing all the details, you have determined that the alert tied to this potentially malicious document is also related to another incident in your environment. However, the alert is not currently listed as a part of that second incident. Your investigation into the alert is ongoing, as is your investigation into the two related incidents.
You need to appropriately categorize the alert and ensure that it is associated with the second incident.
What two actions should you take in the Manage alert pane to fulfill this part of the investigation? Each correct answer presents a part of the solution.

A. Select the Link alert to another incident option.
B. Set classification to True alert.
C. Set status to New.
D. Set status to In progress.
E. Enter the Incident ID of the related incident in the Comment section.

Answer: AD

Explanation:

The correct action to classify the alert would be to set the status to In progress. While the alert may seem to be legitimate as it is linked to another incident, until a final determination is reached, you should set the status to In progress to ensure that others know it is being worked on. Once a determination is reached, you can then change it to Resolved and select the appropriate classification (True alert or False alert).

The correct action to correlate the alert to the other incident would be to select the Link alert to another incident option. While ideally the alert would automatically be included in both incidents, that is not always the case. If you notice an alert that is not linked to an incident that it is clearly connected to, using the Link alert to another incident option ensures they are tied together.

You should not set the classification to True alert. While a point can be made that it seems this malicious file involved in multiple incidents is likely to be a True alert, you are not yet able to make that determination. It also is not time to classify it as a false alert. The best practice while continuing an investigation would be not to change the classification at all, which means leaving it as the default Not set classification.

You should not enter the Incident ID of the related incident in the Comment section. While this might be helpful from an administrative perspective, it creates no link to the other incident.

You should not set the status to New. This is the default status of any alert. The question specifically seeks to ensure your peers know the alert is being investigated, so setting (or leaving) the status as New would make it impossible to differentiate from other uninvestigated alerts.

All of the actions mentioned in the options can be found in the Manage alert pane, which can be reached via the Alerts tab in the Incidents section of the Microsoft 365 Defender portal. This is an excellent central location from which you can manage incidents, and the components that make them up, including alerts.

QUESTION 78

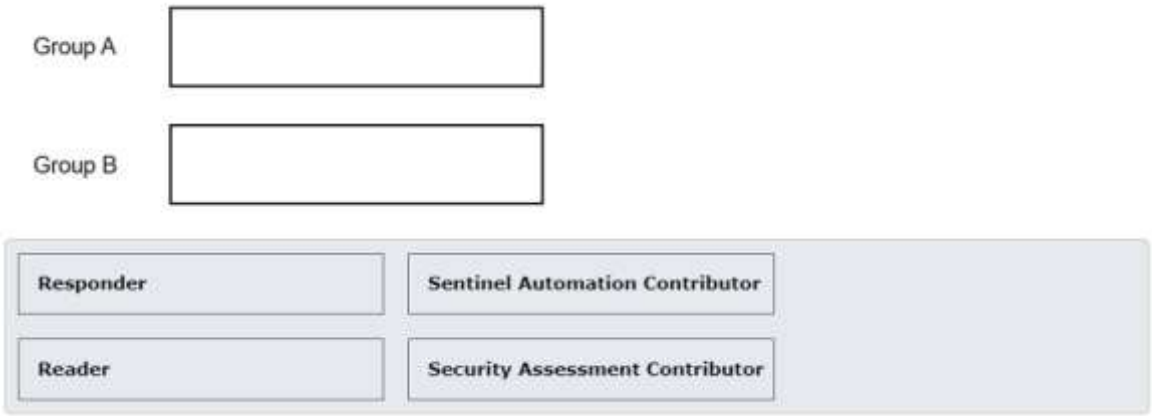
Drag and Drop Question

Your company starts using Azure Sentinel. The manager wants the administration of the implemented solution to be divided into two groups, Group A and Group B, where:

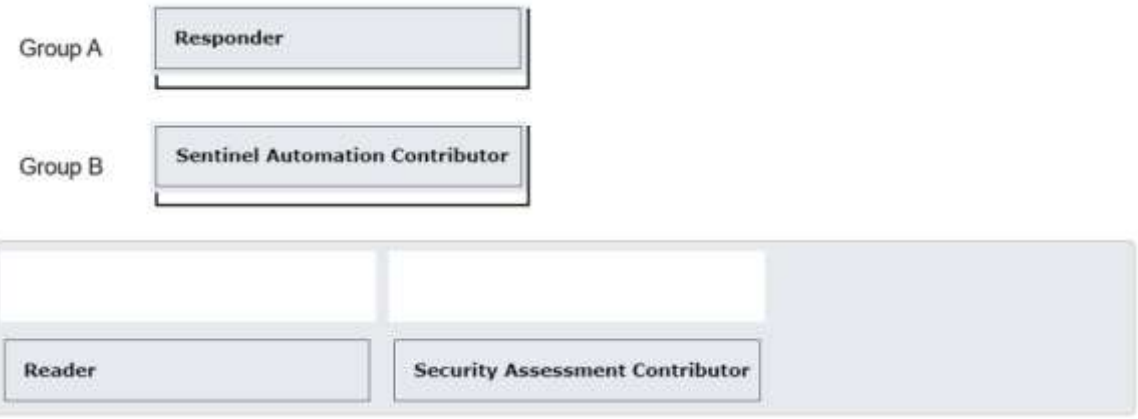
- Group A takes responsibility for replacing the tags of Threat Intelligence Indicator.
- Group B takes responsibility for adding playbooks to automation rules.

You need to assign the appropriate roles for both groups to fulfill the manager's request.

How should you assign the roles? To answer, drag the appropriate role to each group. A role may be used once, more than once, or not at all.



Answer:



Explanation:
You should assign the Responder role to Group A. This role gives the user permission to manage incidents in Azure Sentinel (like assigning users for incidents, dismissing alerts, etc.) and to view several Azure Sentinel resources, including reports, incidents, and workbooks. This role also gives permission to replace Tags of Threat Intelligence Indicator. This role does not give permission to add playbooks to automation rules. Threat Intelligence Indicator is a cloud-based solution used within companies to analyze and act upon threat activities.
You should assign the Azure Sentinel Automation Contributor role to Group B. In addition to viewing Azure Sentinel resources, managing incidents, and working with workbooks, this role allows Azure Sentinel to add playbooks to automation rules. This meets the scenario requirement.
You should not assign the Reader role to either group. This role gives a user permission to view incidents in Azure Sentinel, but not the permission to replace tags of Threat Intelligence Indicator or to add playbooks to automation rules as required in the scenario.
You should not assign the Security Assessment Contributor role to either of the groups. This role gives permission to create security assessments on the company's Azure Sentinel subscription, which is useful for knowing if another subscription of Azure Sentinel is needed. This role does not give the permission to replace tags of Threat Intelligence Indicator or to add playbooks to automation rules as required in the scenario.
Reference:
https://docs.microsoft.com/en-us/azure/sentinel/roles
https://docs.microsoft.com/en-us/azure/role-based-access-control/built-in-roles

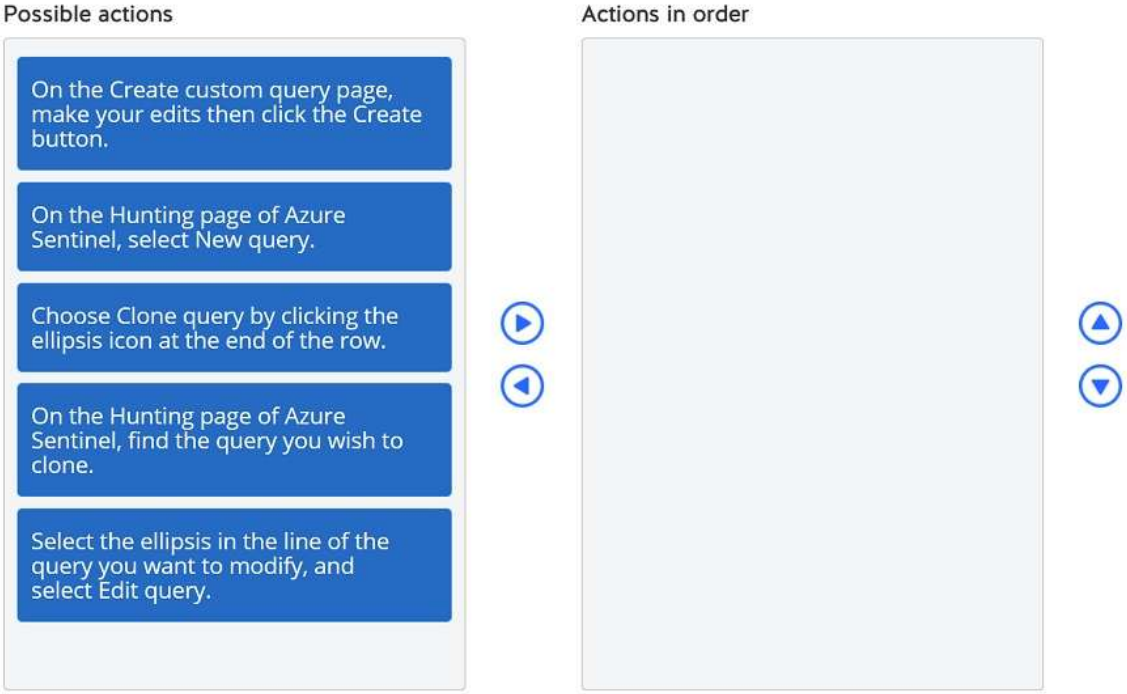
QUESTION 79
You are currently using Azure Sentinel for the collection of Windows security events. You want to use Azure Sentinel to identify Remote Desktop Protocol (RDP) activity that is unusual for your environment.
You need to enable the Anomalous RDP Login Detection rule.
What two prerequisites do you need to ensure are in place before you can enable this rule? Each correct answer presents part of the solution.

A. Collect Security events or Windows Security Events with Event ID 4624.
B. Let the machine learning algorithm collect 30 days' worth of Windows Security events data.
C. Select an event set other than None.
D. Collect Security events or Windows Security Events with Event ID 4720.

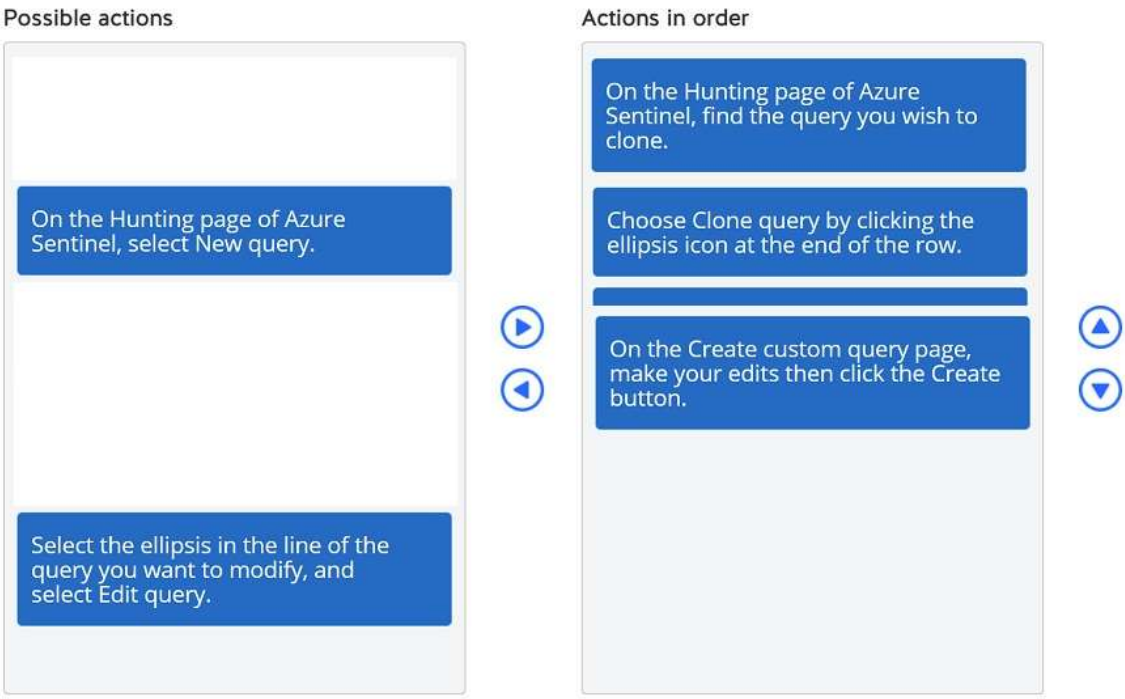
Answer: AC
Explanation:
One of the best features of a Security information and event management (SIEM) tool like Azure Sentinel is correlating important data and finding events that deserve your attention. The Anomalous RDP Login Detection rule does just that. Enabling this rule requires two prerequisites:
You should collect Security events or Windows Security Events with Event ID 4624. This is the event ID for an account successfully logging on to a machine/system. This covers many log in types, including RDP. Without this data, Azure Sentinel would be blind to RDP logins entirely. This process would be completed in the Security Events Data Connector or Windows Security Events (Preview) Data Connector pages within Azure Sentinel.
You should also select an event set other than None. This is a configuration step completed during the data connector implementation described above. This step ensures that the connector detailed in the above step is actually passing data. Options other than None include All events, Common, and Minimal. Although it may seem counterintuitive that

there would even be a None event set, this can be used to disable a connector without deleting/removing it. This can be helpful in certain troubleshooting scenarios.
You should not create a data collection rule that includes Event ID 4720. This is the Event ID for the creation of a user account, not for logging on to a machine or system. While it may seem picky to expect a security professional to memorize exact event IDs, it is incredibly helpful to recognize some of the most common ones. Log ins (4624) and user creation (4720) are two that are very critical to know well in the event of conducting time sensitive research of a potential compromise and privilege escalation/account creation incident response (IR) scenario.
You should not let the machine learning algorithm collect 30 days' worth of Windows Security events data. This is, however, a very important time frame in regards to the time after you enable the rule. This rule relies on a machine learning algorithm that ultimately requires 30 days' worth of data before it can build a baseline. This baseline is a profile of your company's normal user behavior, so you need to allow 30 days of Windows Security events data to be ingested before this rule will result in the discovery of any incidents. Remember, however, that the question only refers to the process to enable the rule and not the generation of incidents thereafter.
Finally, the actual process to enable the rule after these prerequisites are set is fairly simple. Starting in the Azure Sentinel portal, you will click Analytics, and then click the Rule templates tab. Next, you must choose the (Preview) Anomalous RDP Login Detection rule and simply move the Status slider from Disabled (the default) to Enabled.

QUESTION 80
Drag and Drop Question
You are threat hunting using Azure Sentinel. You have created a query designed to identify a specific event on your domain controller.
You need to create several similar queries because you have multiple domain controllers and want to keep each query separate. The solution should minimize administrative effort.
Which three actions should you perform in sequence to clone a query? To answer, move the appropriate actions from the list of possible actions to the answer area and arrange them in the correct order.

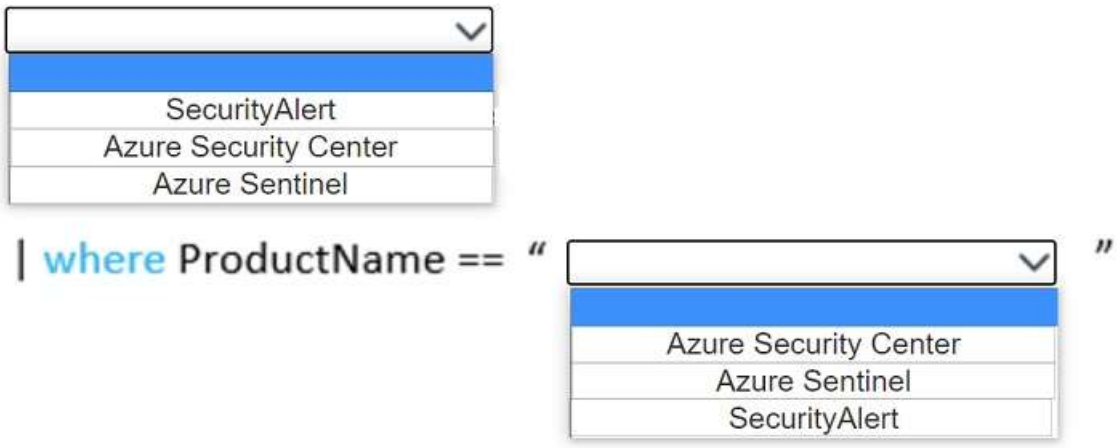


Answer:

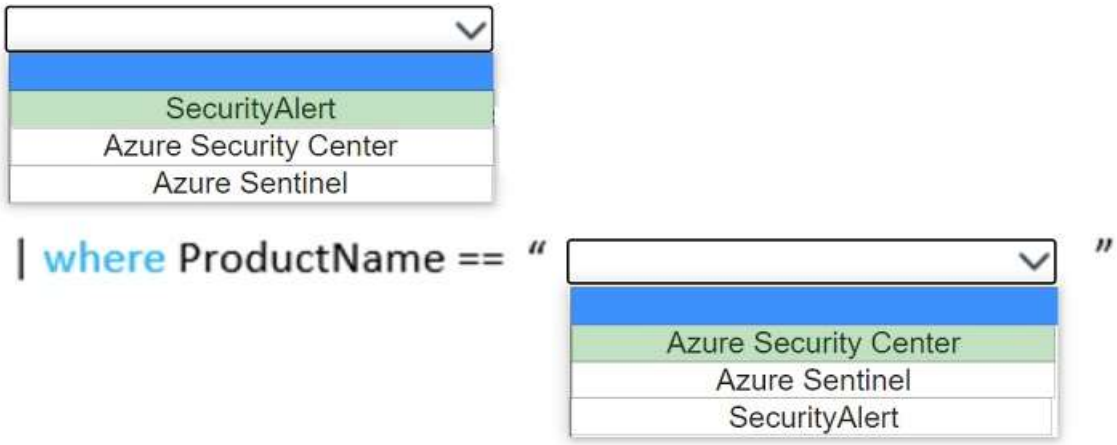


Explanation:
You should perform the following tasks in order:
On the Hunting page of Azure Sentinel, find the query you wish to clone.
Choose Clone query by clicking the ellipsis icon at the end of the row.
On the Create custom query page, make your edits then click the Create button.
First, you should find the query you wish to clone. You will do this by navigating to the Hunting page within Azure Sentinel and then looking through the list of queries. This will allow you to ensure the right initial query is cloned in the next step.
Next, you should choose the Clone query option. This is accessible via the ellipsis at the end of the row for the query you found in step one. This will make a copy of the query you identified in the first step and will take you to the page where you can make changes to that copy.
Finally, you should make your edits then click the Create button. These edits will be made on the Create custom query page, which is the page you are taken to after selecting Clone query in step two. This will allow you to tweak the copy to your needs. When you click Create, the initial query you copied will still exist in its original state, and a new query with the changes you make in this step will be generated/saved.
This process would allow you, for example, to alter the IP or hostname in the query to match your other domain controllers (DCs) but keep the rest of the query the same. As mentioned above, it also leaves the original query untouched/as-is. This is a fast, efficient way to make several queries that are related but require minor tweaks to meet the desired outcome. Starting each query from scratch would take much longer and would be more likely to result in human error in the query syntax.
You should not select New query on the Hunting page of Azure Sentinel. While this option could ultimately be chosen to generate the queries for your other DCs, as mentioned above, you would be starting from scratch. If you only need to change a few minor things in your query, going to New query is a waste of time as the clone option gives you a better starting point.
You should not select the ellipsis in the line of the query you want to modify, and select Edit query. This would allow you to edit an existing query, but it would not create a copy of it. Any edits made here would alter the original query. With the Clone query option, you leave the original unaltered, while efficiently creating new queries based on it.

QUESTION 81
Hotspot Question
You are using Azure Defender and Azure Sentinel to protect your cloud workloads and monitor your environment.
You need to use the Kusto Query Language (KQL) to construct a query that identifies Azure Defender alerts.
What query should you write to meet this requirement? To answer, complete the query by selecting the correct options from the drop-down menus.



Answer:



Explanation:
You should complete the query as follows:

```
SecurityAlert
| where ProductName == "Azure Security Center"
```

This completes a basic query to identify all security alerts in Azure Security Center. Placing SecurityAlert first queries the SecurityAlert table, and then using | where ProductName == "Azure Security Center" afterwards ensures that in that SecurityAlert table you are only looking for entries where the ProductName column has a value of Azure Security Center. From here, you can expand. For example, you could use KQL to specify time frames or specific devices to query. Kusto Query Language (KQL) is the language you will use when building queries in Azure Sentinel. Queries serve as a way to search through the massive amount of data Azure Sentinel has access to.
You should not begin the query with Azure Security Center. The structure of a query requires that you first identify the key table you will be querying. The SecurityAlert table includes the security alerts that are being digested by Azure Sentinel. You should first query this table, then narrow the search to the alerts coming from the Azure Security Center product.
You should not begin the query with Azure Sentinel. Again, the structure of a query requires that you first identify the key table you will be querying. In this case, that would be the SecurityAlert table. More importantly, while Azure Sentinel is the solution aggregating this data and performing the query, it should not be used as the ProductName. This should be specified as the Azure Security Center.
You should not end the query with Azure Sentinel. As mentioned in the paragraph above, the ProductName (solution source) for the SecurityAlert (alerts) table you should query is Azure Security Center. The query would be run in Azure Sentinel, but do not confuse the solution being queried with the one running the query.
You should not end the query with SecurityAlert. Here you need to name the solution you want to query. In this case, that is Azure Security Center. SecurityAlert would not be a valid ProductName.

QUESTION 82
Case Study 1 - Contoso Ltd

Overview

A company named Contoso Ltd. has a main office and five branch offices located throughout North America. The main office is in Seattle. The branch offices are in Toronto, Miami, Houston, Los Angeles, and Vancouver.

Contoso has a subsidiary named Fabrikam, Ltd. that has offices in New York and San Francisco.

Existing Environment

End-User Environment

All users at Contoso use Windows 10 devices. Each user is licensed for Microsoft 365. In addition, iOS devices are distributed to the members of the sales team at Contoso.

Cloud and Hybrid Infrastructure

All Contoso applications are deployed to Azure.

You enable Microsoft Cloud App Security.

Contoso and Fabrikam have different Azure Active Directory (Azure AD) tenants. Fabrikam recently purchased an Azure subscription and enabled Azure Defender for all supported resource types.

Current Problems

The security team at Contoso receives a large number of cybersecurity alerts. The security team spends too much time identifying which cybersecurity alerts are legitimate threats, and which are not.

The Contoso sales team uses only iOS devices. The sales team members exchange files with customers by using a variety of third-party tools. In the past, the sales team experienced various attacks on their devices.

The marketing team at Contoso has several Microsoft SharePoint Online sites for collaborating with external vendors. The marketing team has had several incidents in which vendors uploaded files that contain malware.

The executive team at Contoso suspects a security breach. The executive team requests that you identify which files had more than five activities during the past 48 hours, including data access, download, or deletion for Microsoft Cloud App Security-protected applications.

Requirements

Planned Changes

Contoso plans to integrate the security operations of both companies and manage all security operations centrally.

Technical Requirements

Contoso identifies the following technical requirements:

- Receive alerts if an Azure virtual machine is under brute force attack.
- Use Azure Sentinel to reduce organizational risk by rapidly remediating active attacks on the environment.
- Implement Azure Sentinel queries that correlate data across the Azure AD tenants of Contoso and Fabrikam.
- Develop a procedure to remediate Azure Defender for Key Vault alerts for Fabrikam in case of external attackers and a potential compromise of its own Azure AD applications.
- Identify all cases of users who failed to sign in to an Azure resource for the first time from a given country. A junior security administrator provides you with the following incomplete query.

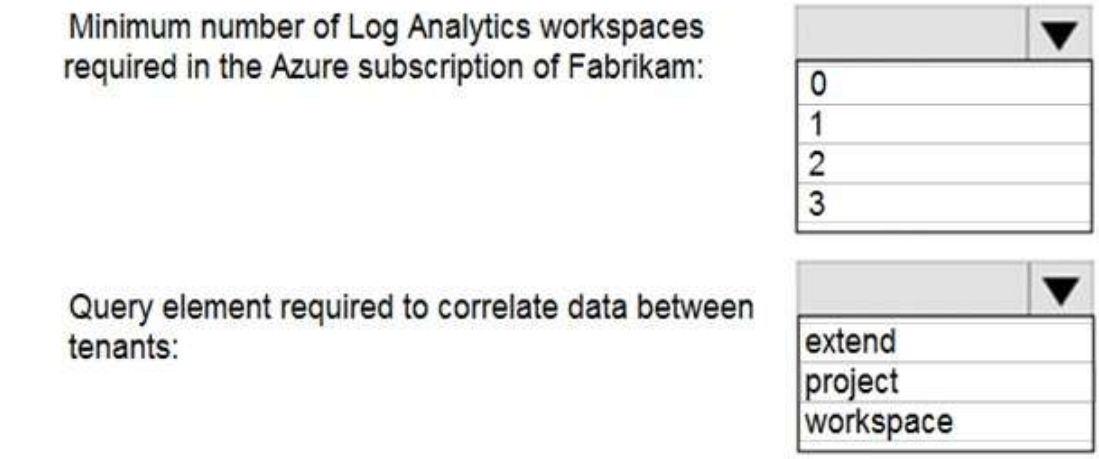
```
BehaviorAnalytics
 | where ActivityType == "FailedLogOn"
 | where _________ == True
```

Hotspot Question

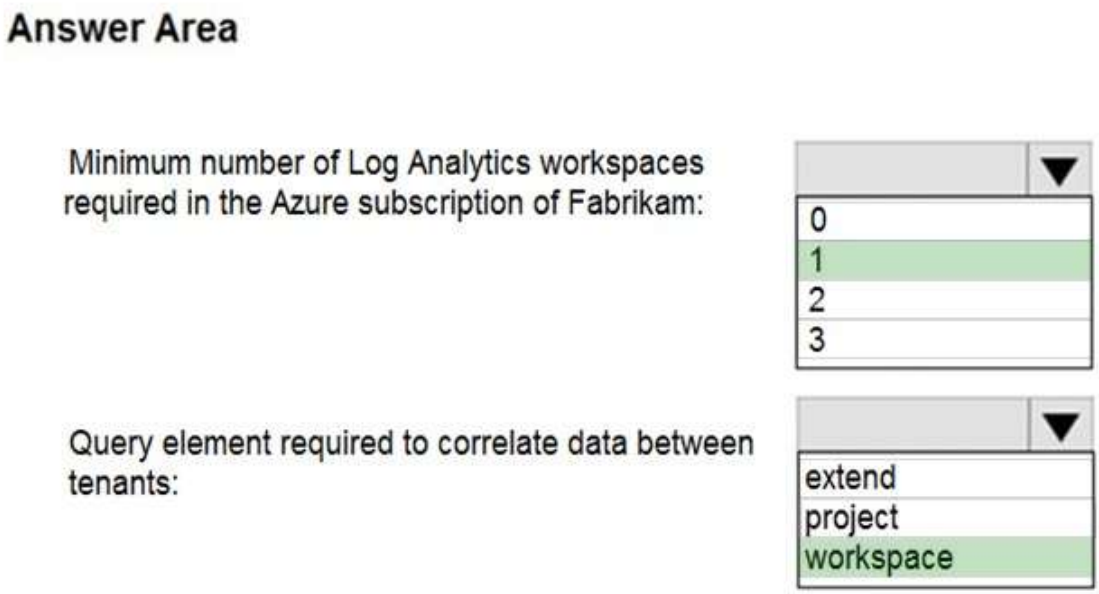
You need to implement Azure Sentinel queries for Contoso and Fabrikam to meet the technical requirements.

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.



Answer:



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

QUESTION 83
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:
https://docs.microsoft.com/en-us/cloud-app-security/tutorial-dlp
https://docs.microsoft.com/en-us/cloud-app-security/azip-integration