

Microsoft

Exam Questions SC-200

Microsoft Security Operations Analyst



NEW QUESTION 1

- (Exam Topic 1)

The issue for which team can be resolved by using Microsoft Defender for Office 365?

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

Answer: B

Explanation:

Reference:

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

NEW QUESTION 2

- (Exam 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:

Reference:

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

NEW QUESTION 3

- (Exam 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:

Reference:

<https://docs.microsoft.com/en-us/azure/key-vault/general/secure-your-key-vault>

NEW QUESTION 4

- (Exam Topic 1)

You need to recommend a solution to meet the technical requirements for the Azure virtual machines. What should you include in the recommendation?

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

Answer: B

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/security-center/azure-defender>

NEW QUESTION 5

- (Exam Topic 2)

You need to implement the Azure Information Protection requirements. What should you configure first?

- A. Device health and compliance reports settings in Microsoft Defender Security Center
- B. scanner clusters in Azure Information Protection from the Azure portal
- C. content scan jobs in Azure Information Protection from the Azure portal
- D. Advanced features from Settings in Microsoft Defender Security Center

Answer: D

Explanation:

<https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/information-protection-in-windows-overview>

NEW QUESTION 6

- (Exam 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 7

- (Exam Topic 2)

You need to configure the Azure Sentinel integration to meet the Azure Sentinel requirements. What should you do? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

In the Cloud App Security portal:

	▼
Add a security extension	
Configure app connectors	
Configure log collectors	

From Azure Sentinel in the Azure portal:

	▼
Add a data connector	
Add a workbook	
Configure the Logs settings	

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Graphical user interface, text, application Description automatically generated

Reference:

<https://docs.microsoft.com/en-us/cloud-app-security/siem-sentinel>

NEW QUESTION 8

- (Exam Topic 3)

You have an Azure Storage account that will be accessed by multiple Azure Function apps during the development of an application. You need to hide Azure Defender alerts for the storage account. Which entity type and field should you use in a suppression rule? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Entity type:

IP address

Azure Resource

Host

User account

Field:

Name

Resource Id

Address

Command line

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Graphical user interface, application Description automatically generated
Reference:
<https://techcommunity.microsoft.com/t5/azure-security-center/suppression-rules-for-azure-security-center-alerts>

NEW QUESTION 9

- (Exam Topic 3)

You have a Microsoft 365 subscription that uses Microsoft 365 Defender and contains a user named User1. You are notified that the account of User1 is compromised. You need to review the alerts triggered on the devices to which User1 signed in. How should you complete the query? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

DeviceInfo

| where LoggedOnUsers contains 'user1'

| distinct DeviceId

|

▼

 kind=inner AlertEvidence on DeviceId

extend

join

project

| project AlertId

| join AlertInfo on AlertId

|

▼

 AlertId, Timestamp, Title, Severity, Category

project

summarize

take

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Box 1: join
An inner join.
This query uses kind=inner to specify an inner-join, which prevents deduplication of left side values for DeviceId.
This query uses the DeviceInfo table to check if a potentially compromised user (<account-name>) has logged on to any devices and then lists the alerts that have been triggered on those devices.
DeviceInfo
//Query for devices that the potentially compromised account has logged onto
| where LoggedOnUsers contains '<account-name>'
| distinct DeviceId
//Crosscheck devices against alert records in AlertEvidence and AlertInfo tables
| join kind=inner AlertEvidence on DeviceId
| project AlertId
//List all alerts on devices that user has logged on to
| join AlertInfo on AlertId
| project AlertId, Timestamp, Title, Severity, Category DeviceInfo LoggedOnUsers AlertEvidence "project AlertID"
Box 2: project
Reference:
<https://docs.microsoft.com/en-us/microsoft-365/security/defender/advanced-hunting-query-emails-devices?view>

NEW QUESTION 10

- (Exam Topic 3)
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

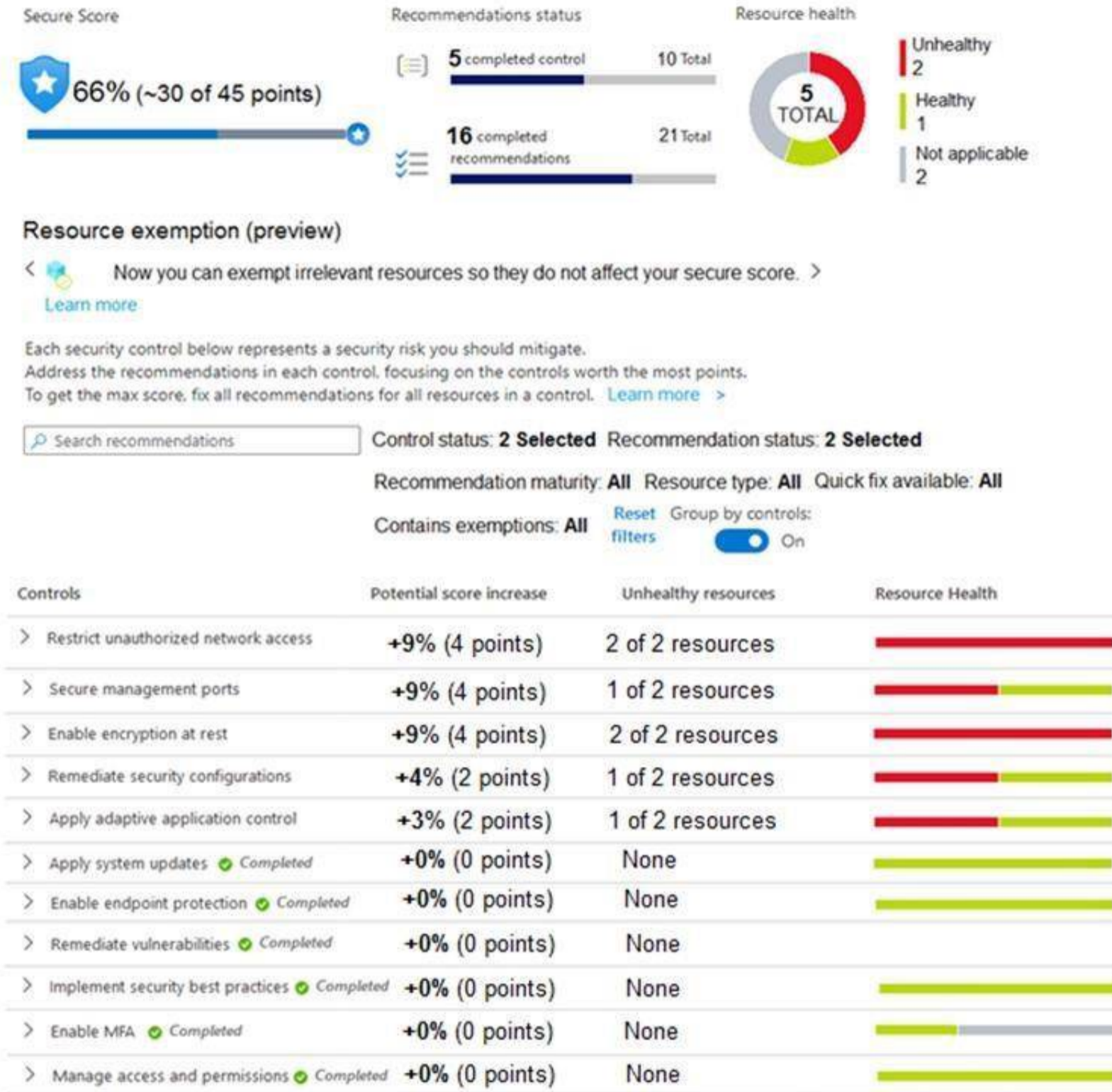
Answer: A

Explanation:

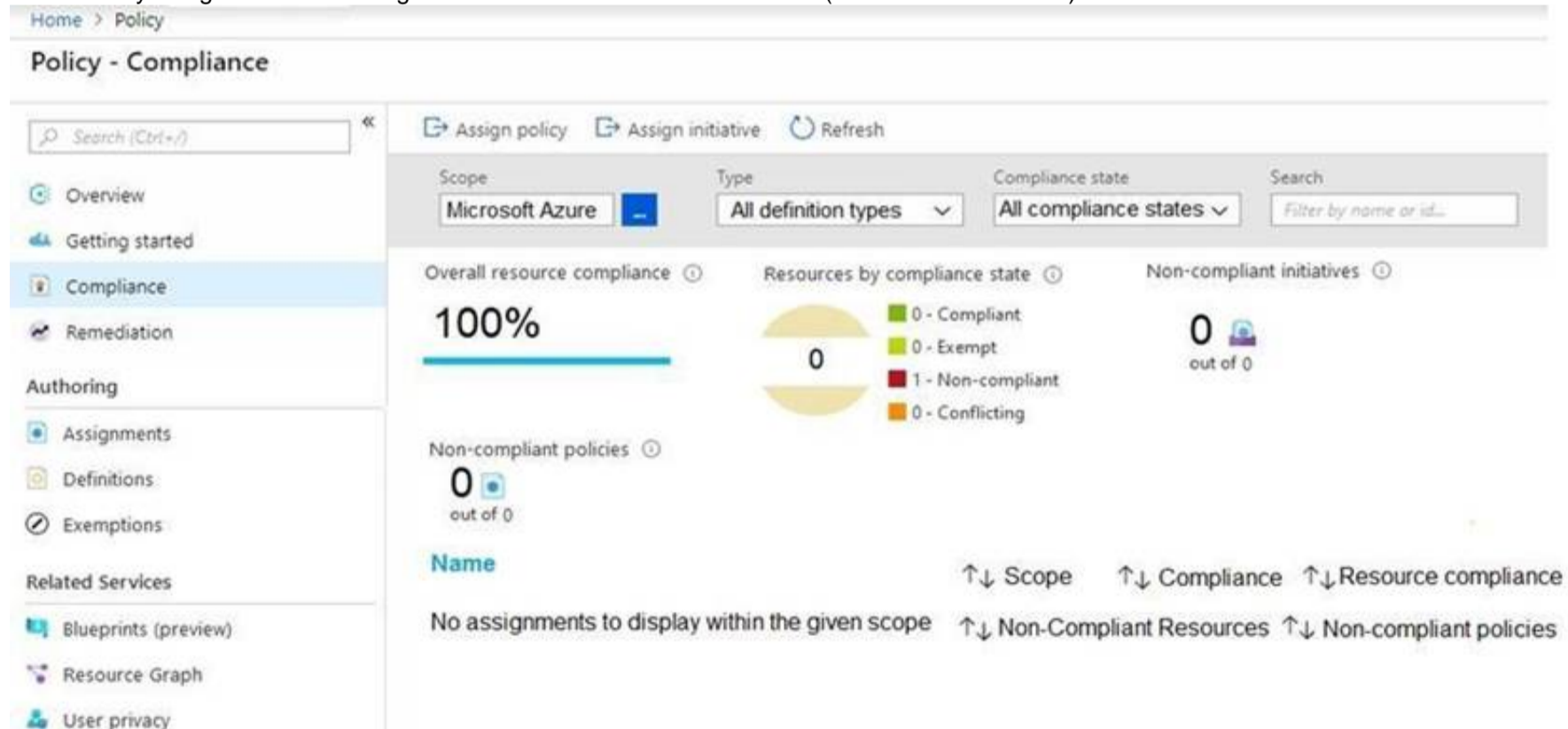
Reference:
<https://docs.microsoft.com/en-us/azure/sentinel/connect-cef-agent?tabs=rsyslog>

NEW QUESTION 10

- (Exam Topic 3)
You manage the security posture of an Azure subscription that contains two virtual machines name vm1 and vm2.
The secure score in Azure Security Center is shown in the Security Center exhibit. (Click the Security Center tab.)



Azure Policy assignments are configured as shown in the Policies exhibit. (Click the Policies tab.)



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

Answer Area

Statements	Yes	No
Both virtual machines have inbound rules that allow access from either Any or Internet ranges.	<input type="radio"/>	<input type="radio"/>
Both virtual machines have management ports exposed directly to the internet.	<input type="radio"/>	<input type="radio"/>
If you enable just-in-time network access controls on all virtual machines, you will increase the secure score by four point.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:
Reference:
<https://techcommunity.microsoft.com/t5/azure-security-center/security-control-restrict-unauthorized-network-ac> <https://techcommunity.microsoft.com/t5/azure-security-center/security-control-secure-management-ports/ba-p/1>

NEW QUESTION 14

- (Exam Topic 3)
You are investigating an incident in Azure Sentinel that contains more than 127 alerts. You discover eight alerts in the incident that require further investigation. You need to escalate the alerts to another Azure Sentinel administrator. What should you do to provide the alerts to the administrator?

- A. Create a Microsoft incident creation rule
- B. Share the incident URL
- C. Create a scheduled query rule
- D. Assign the incident

Answer: D

Explanation:
Reference:
<https://docs.microsoft.com/en-us/azure/sentinel/investigate-cases>

NEW QUESTION 18

- (Exam Topic 3)
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": "

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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Graphical user interface, text, application Description automatically generated

Reference:

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

NEW QUESTION 19

- (Exam Topic 3)

Your company uses Microsoft Defender for Endpoint.

The company has Microsoft Word documents that contain macros. The documents are used frequently on the devices of the company's accounting team.

You need to hide false positive in the Alerts queue, while maintaining the existing security posture. Which three actions should you perform? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

- A. Resolve the alert automatically.
- B. Hide the alert.
- C. Create a suppression rule scoped to any device.
- D. Create a suppression rule scoped to a device group.
- E. Generate the alert.

Answer: BCE

Explanation:

Reference:

<https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/manage-alerts>

NEW QUESTION 21

- (Exam Topic 3)

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:

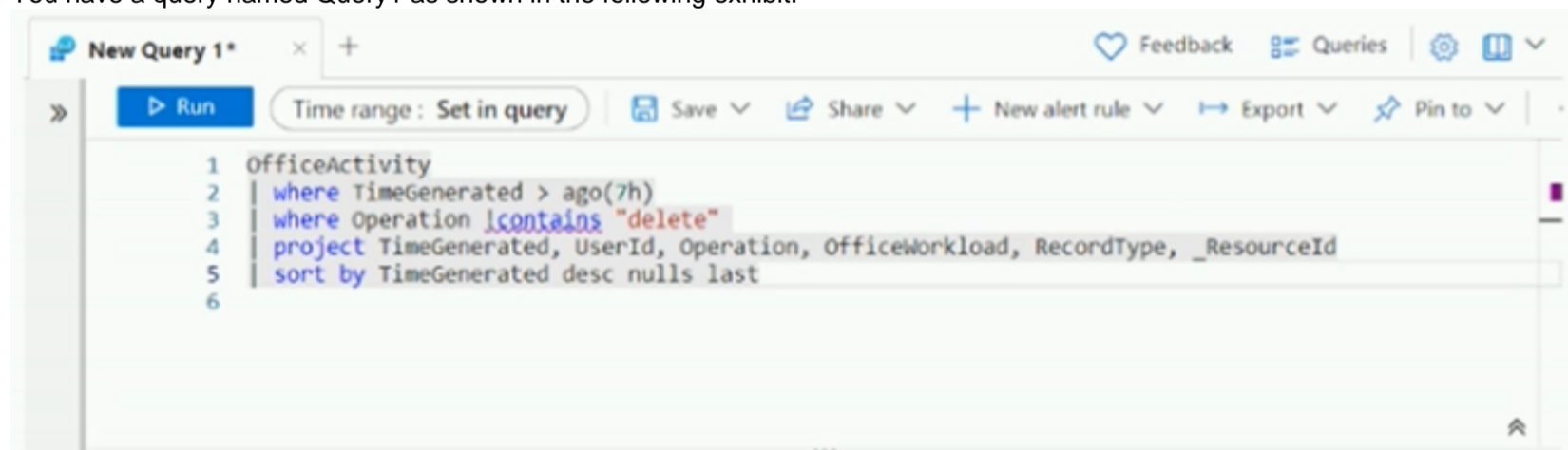
<https://docs.microsoft.com/en-us/azure/sentinel/connect-data-sources>

NEW QUESTION 24

- (Exam Topic 3)

You have a Microsoft Sentinel workspace.

You have a query named Query1 as shown in the following exhibit.



You plan to create a custom parser named Parser 1. You need to use Query1 in Parser1. What should you do first?

- A. Remove line 2.
- B. In line 4. remove the TimeGenerated predicate.
- C. Remove line 5.
- D. In line 3, replace the 'contains operator with the !has operator.

Answer: C

Explanation:

This can be confirmed by referring to the official Microsoft documentation on creating custom log queries in Azure Sentinel, which states that the "has" operator should not be used in the query, and that it is unnecessary. Reference: <https://docs.microsoft.com/en-us/azure/sentinel/query-custom-logs>

NEW QUESTION 26

- (Exam Topic 3)

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-manag>

NEW QUESTION 31

- (Exam Topic 3)

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 34

- (Exam Topic 3)

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 36

- (Exam Topic 3)

You create a custom analytics rule to detect threats in Azure Sentinel. You discover that the rule fails intermittently.

What are two possible causes of the failures? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

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

Answer: AD

NEW QUESTION 40

- (Exam Topic 3)
You have an Azure subscription that uses Microsoft Defender for Cloud and contains a storage account named storage1. You receive an alert that there was an unusually high volume of delete operations on the blobs in storage1.
You need to identify which blobs were deleted. What should you review?

A. the Azure Storage Analytics logs
B. the activity logs of storage1
C. the alert details
D. the related entities of the alert

Answer: B

NEW QUESTION 44

- (Exam Topic 3)
You have an Azure subscription that has Microsoft Defender for Cloud enabled.
You have a virtual machine that runs Windows 10 and has the Log Analytics agent installed. You need to simulate an attack on the virtual machine that will generate an alert.
What should you do first?

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

Answer: A

NEW QUESTION 45

- (Exam Topic 3)
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

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.

Answer Area

- 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.

Dashboard > Microsoft Defender for Cloud

Microsoft Defender for Cloud | Workflow automation
 Showing 73 subscriptions

Search (Ctrl+/) **2** + Add workflow automation Refresh

General

Overview

Getting started

Recommendations

Security alerts

Inventory

Workbooks

Community

Diagnose and solve problems

Cloud Security

Secure Score

Regulatory compliance

Workload protections

Firewall Manager

Management

Environment settings

Security solutions

Workflow automation **1**

Filter by name S... E..

Name	Status	Scope
DuduTe...	Disabled	ASC DEM
DuduTe...	Disabled	ASC DEM
RonnyTest	Disabled	ASC DEM
rr_reg_c...	Disabled	ASC DEM
test	Disabled	private-b
yoafrTes...	Disabled	ASC DEM
EnabeA...	Enabled	ASC Mul
Encrypt...	Enabled	ASC Mul
KerenN...	Enabled	ASC DEM
KerenSh...	Enabled	ASC DEM
KerenTe...	Enabled	ASC DEM
MorAuto	Enabled	ASC DEM
NewDes...	Enabled	ASCDEM

Add workflow automation

General **3**

Name *

Description

Subscription

Resource group *

Trigger conditions

Choose the trigger conditions that will automatically trigger the configured action.

Defender for Cloud data type *

Alert name contains

Alert severity *

Actions

Configure the Logic App that will be triggered. Choose an existing Logic App or visit the Logic Apps page to create a new one

Show Logic App instances from the following subscriptions *

Logic App name

Refresh

Create Cancel

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.

Deploy Workflow Automation for Microsoft Defender for Cloud recommendations

Policy definition

Assign Edit definition Duplicate definition Delete definition Export definition

Essentials

Definition Assignments (0) Parameters

```

1 {
2   "properties": {
3     "displayName": "Deploy Workflow Automation for Microsoft Defender for Cloud recommendations",
4     "policyType": "BuiltIn",
5     "mode": "All",
6     "description": "Enable automation of Microsoft Defender for Cloud recommendations. This policy deploys",
7     "metadata": {
8       "version": "1.0.0",
9       "category": "Security Center"
10    }
11  }
12 }
```

Reference: <https://docs.microsoft.com/en-us/azure/defender-for-cloud/workflow-automation>

NEW QUESTION 50

- (Exam Topic 3)

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 53

- (Exam Topic 3)

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You have Linux virtual machines on Amazon Web Services (AWS). You deploy Azure Defender and enable auto-provisioning.

You need to monitor the virtual machines by using Azure Defender.

Solution: You enable Azure Arc and onboard the virtual machines to Azure Arc. Does this meet the goal?

- A. Yes
- B. No

Answer: B

Explanation:

Reference:

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

NEW QUESTION 55

- (Exam Topic 3)

Your company uses Azure Sentinel to manage alerts from more than 10,000 IoT devices.

A security manager at the company reports that tracking security threats is increasingly difficult due to the large number of incidents.

You need to recommend a solution to provide a custom visualization to simplify the investigation of threats and to infer threats by using machine learning.

What should you include in the recommendation?

- A. built-in queries
- B. livestream
- C. notebooks
- D. bookmarks

Answer: C

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/sentinel/notebooks>

NEW QUESTION 60

- (Exam Topic 3)

Your company deploys the following services:

- Microsoft Defender for Identity
- Microsoft Defender for Endpoint
- Microsoft Defender for Office 365

You need to provide a security analyst with the ability to use the Microsoft 365 security center. The analyst must be able to approve and reject pending actions generated by Microsoft Defender for Endpoint. The solution must use the principle of least privilege.

Which two roles should assign to the analyst? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

- A. the Compliance Data Administrator in Azure Active Directory (Azure AD)
- B. the Active remediation actions role in Microsoft Defender for Endpoint
- C. the Security Administrator role in Azure Active Directory (Azure AD)
- D. the Security Reader role in Azure Active Directory (Azure AD)

Answer: BD

Explanation:

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/rbac?view=o365-worldwide>

NEW QUESTION 64

- (Exam Topic 3)

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-world>

NEW QUESTION 67

- (Exam Topic 3)

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 69

- (Exam Topic 3)

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.

```
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
```

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Graphical user interface, text, application Description automatically generated

Reference:

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

NEW QUESTION 72

- (Exam Topic 3)

You have an Azure subscription that uses Microsoft Defender for Cloud and contains a storage account named storage1. You receive an alert that there was an unusually high volume of delete operations on the blobs in storage1. You need to identify which blobs were deleted. What should you review?

- A. the activity logs of storage1
- B. the Azure Storage Analytics logs
- C. the alert details
- D. the related entities of the alert

Answer: A

Explanation:

To identify which blobs were deleted, you should review the activity logs of the storage account. The activity logs contain information about all the operations that have taken place in the storage account, including delete operations. These logs can be accessed in the Azure portal by navigating to the storage account, selecting "Activity log" under the "Monitoring" section, and filtering by the appropriate time range. You can also use Azure Monitor and Log Analytics to query and analyze the activity logs data.

References:

- > <https://docs.microsoft.com/en-us/azure/storage/common/storage-activity-logs>
- > <https://docs.microsoft.com/en-us/azure/azure-monitor/platform/activity-log-azure-storage>

NEW QUESTION 74

- (Exam Topic 3)

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 =
| where MalwareFilterVerdict == "Malware"
| project TimeEmail = Timestamp, Subject, SenderFromAddress, AccountName =
tostring(split (RecipientEmailAddress, "@") [0]);

MaliciousEmails
| join (
| 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:

Graphical user interface, text, application, email Description automatically generated
Reference:
<https://docs.microsoft.com/en-us/microsoft-365/security/defender/advanced-hunting-query-emails-devices?view>

NEW QUESTION 78

- (Exam Topic 3)

Your company has an on-premises network that uses Microsoft Defender for Identity. The Microsoft Secure Score for the company includes a security assessment associated with unsecure Kerberos delegation. You need remediate the security risk. What should you do?

- A. Install the Local Administrator Password Solution (LAPS) extension on the computers listed as exposed entities.
- B. Modify the properties of the computer objects listed as exposed entities.
- C. Disable legacy protocols on the computers listed as exposed entities.
- D. Enforce LDAP signing on the computers listed as exposed entities.

Answer: B

Explanation:

To remediate the security risk associated with unsecure Kerberos delegation, you should modify the properties of the computer objects listed as exposed entities. Specifically, you should set the Kerberos delegation settings to either 'Trust this computer for delegation to any service' or 'Trust this computer for delegation to specified services only'. This will ensure that the computer is not allowed to use Kerberos delegation to access other computers on the network.
Reference: <https://docs.microsoft.com/en-us/windows/security/identity-protection/microsoft-defender-for-iden>

NEW QUESTION 83

- (Exam Topic 3)

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	<ul style="list-style-type: none"> Assign initiatives Edit security policies Enable automatic provisioning
User2	<ul style="list-style-type: none"> View alerts and recommendations Apply security recommendations 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	Answer Area
Contributor	User1: <div></div>
Owner	User2: <div></div>
Security administrator	
Security reader	

- 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.
Reference:
<https://docs.microsoft.com/en-us/azure/defender-for-cloud/permissions>

NEW QUESTION 88

- (Exam Topic 3)
You have a Microsoft 365 E5 subscription that uses Microsoft SharePoint Online. You delete users from the subscription. You need to be notified if the deleted users downloaded numerous documents from SharePoint Online sites during the month before their accounts were deleted. What should you use?

- A. a file policy in Microsoft Defender for Cloud Apps
- B. an access review policy
- C. an alert policy in Microsoft Defender for Office 365
- D. an insider risk policy

Answer: C

Explanation:

Alert policies let you categorize the alerts that are triggered by a policy, apply the policy to all users in your organization, set a threshold level for when an alert is triggered, and decide whether to receive email notifications when alerts are triggered. Default alert policies include:
Unusual external user file activity - Generates an alert when an unusually large number of activities are performed on files in SharePoint or OneDrive by users outside of your organization. This includes activities such as accessing files, downloading files, and deleting files. This policy has a High severity setting.
Reference: <https://docs.microsoft.com/en-us/microsoft-365/compliance/alert-policies>

NEW QUESTION 93

- (Exam Topic 3)
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.	<input type="radio"/>	<input checked="" type="radio"/>
The watchlist cannot be updated after it is created.	<input type="radio"/>	<input checked="" type="radio"/>
The IPList variable is set as the IP address entity.	<input type="radio"/>	<input checked="" type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

Statements	Yes	No
The Username field is set as the account entity.	<input type="radio"/>	<input type="checkbox"/>
The watchlist cannot be updated after it is created.	<input type="radio"/>	<input type="checkbox"/>
The IPList variable is set as the IP address entity.	<input type="radio"/>	<input type="checkbox"/>

NEW QUESTION 96

- (Exam Topic 3)

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

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

Answer: C

Explanation:

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

NEW QUESTION 100

- (Exam Topic 3)

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

Answer Area

SW1

CEF1

Server1

Server2

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:

Graphical user interface, text Description automatically generated

Reference:

<https://docs.microsoft.com/en-us/azure/sentinel/connect-log-forwarder?tabs=rsyslog>

NEW QUESTION 105

- (Exam Topic 3)

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 109

- (Exam Topic 3)

You have two Azure subscriptions that use Microsoft Defender for Cloud.

You need to ensure that specific Defender for Cloud security alerts are suppressed at the root management group level. The solution must minimize administrative effort.

What should you do in the Azure portal?

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

Answer: D

Explanation:

You can use alerts suppression rules to suppress false positives or other unwanted security alerts from Defender for Cloud.

Note: To create a rule directly in the Azure portal:

* 1. From Defender for Cloud's security alerts page:

Select the specific alert you don't want to see anymore, and from the details pane, select Take action.

Or, select the suppression rules link at the top of the page, and from the suppression rules page select Create new suppression rule:

* 2. In the new suppression rule pane, enter the details of your new rule.

Your rule can dismiss the alert on all resources so you don't get any alerts like this one in the future.

Your rule can dismiss the alert on specific criteria - when it relates to a specific IP address, process name, user account, Azure resource, or location.

* 3. Enter details of the rule.

* 4. Save the rule.

Reference: <https://docs.microsoft.com/en-us/azure/defender-for-cloud/alerts-suppression-rules>

NEW QUESTION 113

- (Exam Topic 3)

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 114

- (Exam Topic 3)
You have an Azure Sentinel deployment.
You need to query for all suspicious credential access activities.
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

From Azure Sentinel, select **Hunting**.

Select **Run All Queries**.

Select **New Query**.

Filter by tactics.

From Azure Sentinel, select **Notebooks**.

Answer Area

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Actions

From Azure Sentinel, select **Hunting**.

Select **Run All Queries**.

Select **New Query**.

Filter by tactics.

From Azure Sentinel, select **Notebooks**.

Answer Area

NEW QUESTION 119

- (Exam Topic 3)
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 121

- (Exam Topic 3)

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 122

- (Exam Topic 3)

Your company uses Azure Security Center and Azure Defender.

The security operations team at the company informs you that it does NOT receive email notifications for security alerts.

What should you configure in Security Center to enable the email notifications?

- A. Security solutions
- B. Security policy
- C. Pricing & settings
- D. Security alerts
- E. Azure Defender

Answer: C

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/security-center/security-center-provide-security-contact-details>

NEW QUESTION 126

- (Exam Topic 3)

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 127

- (Exam Topic 3)

You have a Microsoft 365 subscription that uses Microsoft Defender for Endpoint.

You need to add threat indicators for all the IP addresses in a range of 171.23.3432-171.2334.63. The solution must minimize administrative effort.

What should you do in the Microsoft 365 Defender portal?

- A. Create an import file that contains the IP address of 171.23.34.32/27. Select Import and import the file.
- B. Select Add indicator and set the IP address to 171.2334.32-171.23.34.63.
- C. Select Add indicator and set the IP address to 171.23.34.32/27
- D. Create an import file that contains the individual IP addresses in the rang
- E. Select Import and import the file.

Answer: C

Explanation:

This will add all the IP addresses in the range of 171.23.34.32/27 as threat indicators. This is the simplest and most efficient way to add all the IP addresses in the range.

Reference:

[1] <https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/threat-intelligence>

NEW QUESTION 130

- (Exam Topic 3)

You have a Microsoft 365 subscription that uses Microsoft 365 Defender. You need to identify all the entities affected by an incident. Which tab should you use in the Microsoft 365 Defender portal?

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

Answer: C

Explanation:

The Evidence and Response tab shows all the supported events and suspicious entities in the alerts in the incident.

Reference: <https://docs.microsoft.com/en-us/microsoft-365/security/defender/investigate-incidents>

NEW QUESTION 133

- (Exam Topic 3)

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:

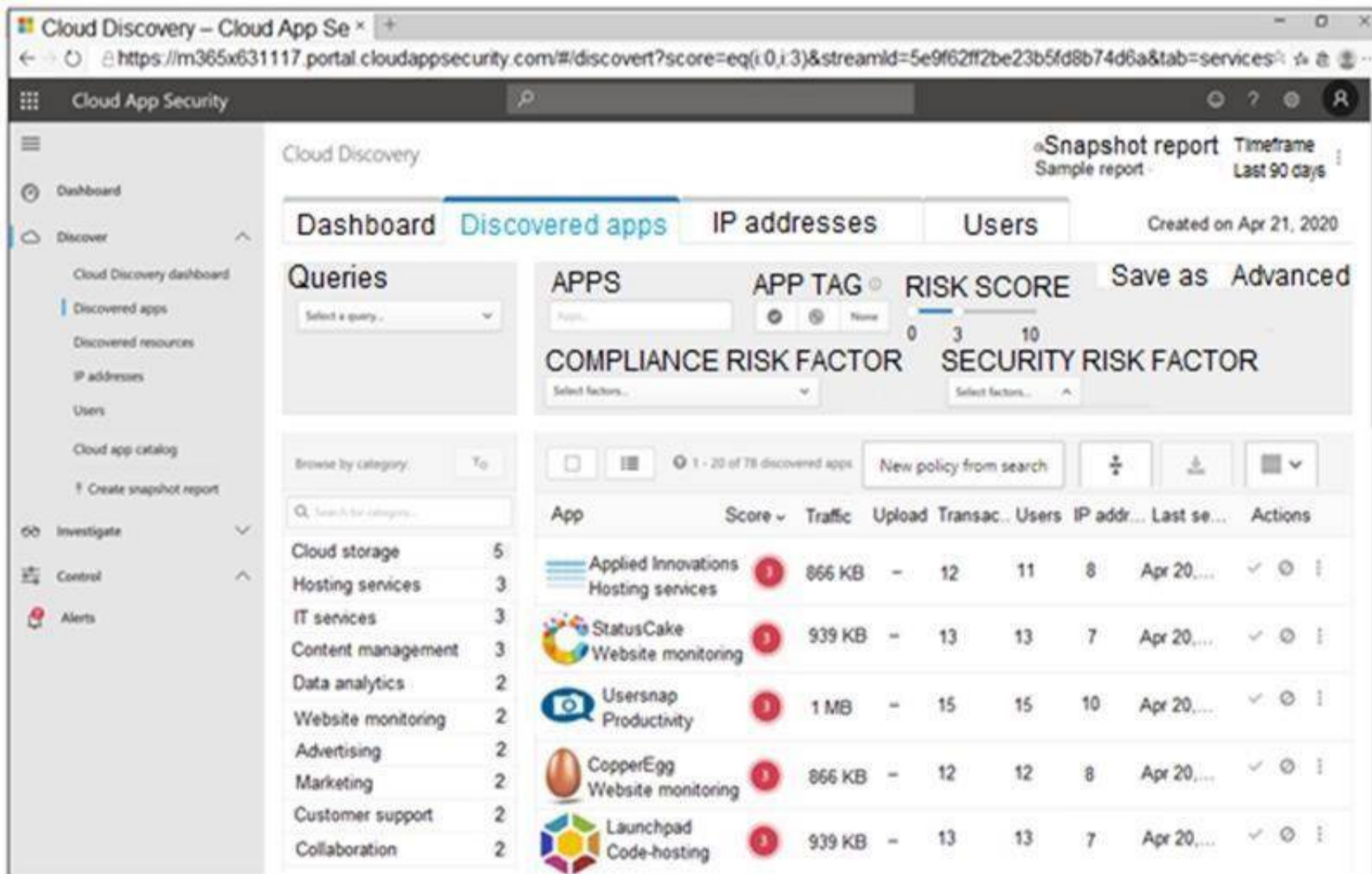
Reference:

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

NEW QUESTION 134

- (Exam Topic 3)

You open the Cloud App Security portal as shown in the following exhibit.



You need to remediate the risk for the Launchpad app.

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

Actions

Tag the app as **Unsanctioned**.

Run the script on the source appliance.

Run the script in Azure Cloud Shell.

Select the app.

Tag the app as **Sanctioned**.

Generate a block script.

Answer Area

⏪

⏩

⏴

⏵

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:
Reference:
<https://docs.microsoft.com/en-us/cloud-app-security/governance-discovery>

NEW QUESTION 138
- (Exam Topic 3)
You have a Microsoft Sentinel workspace named Workspaces
You configure Workspace1 to collect DNS events and deploy the Advanced Security information Model (ASIM) unifying parser for the DNS schema.
You need to query the ASIM DNS schema to list all the DNS events from the last 24 hours that have a response code of 'NXDOMAIN' and were aggregated by the source IP address in 15-minute intervals. The solution must maximize query performance.
How should you complete the query? To answer, select the appropriate options in the answer area NOTE: Each correct selection is worth one point.

_Im_Dns

Dns

imDns

(starttime=ago(1d), responsecodename='NXDOMAIN')

| where TimeGenerated > ago(1d) | where ResponseCodeName =~ "NXDOMAIN"

| where ResponseCodeName == "NXDOMAIN" | where TimeGenerated > ago(1d)

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

_Im_Dns

Dns

imDns

(starttime=ago(1d), responsecodename='NXDOMAIN')

| where TimeGenerated > ago(1d) | where ResponseCodeName =~ "NXDOMAIN"

| where ResponseCodeName == "NXDOMAIN" | where TimeGenerated > ago(1d)

NEW QUESTION 142
- (Exam Topic 3)
You deploy Azure Sentinel.
You need to implement connectors in Azure Sentinel to monitor Microsoft Teams and Linux virtual machines in Azure. The solution must minimize administrative

effort.
Which data connector type should you use for each workload? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Microsoft Teams:

▼

Custom

Office 365

Security Events

Syslog

Linux virtual machines in Azure:

▼

Custom

Office 365

Security Events

Syslog

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:
Graphical user interface, text, application Description automatically generated
Reference:
<https://docs.microsoft.com/en-us/azure/sentinel/connect-office-365> <https://docs.microsoft.com/en-us/azure/sentinel/connect-syslog>

NEW QUESTION 143

- (Exam Topic 3)
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 144

- (Exam Topic 3)
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:

Graphical user interface, text, application Description automatically generated

Reference:

https://docs.microsoft.com/en-us/azure/governance/policy/concepts/effects https://docs.microsoft.com/en-us/azure/security-center/workflow-automation

NEW QUESTION 148

- (Exam Topic 3)

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.	<input type="radio"/>	<input type="radio"/>
The watchlist cannot be updated after it is created.	<input type="radio"/>	<input type="radio"/>
The IPList variable is set as the IP address entity.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Statements	Yes	No
The Username field is set as the account entity.	<input checked="" type="radio"/>	<input type="radio"/>
The watchlist cannot be updated after it is created.	<input checked="" type="radio"/>	<input type="radio"/>
The IPList variable is set as the IP address entity.	<input type="radio"/>	<input checked="" type="radio"/>

NEW QUESTION 151

- (Exam Topic 3)

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 154

- (Exam Topic 3)

You have a Microsoft Sentinel workspace.

You need to create a KQL query that will identify successful sign-ins from multiple countries during the last three hours.

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 timeframe = ago(3h);
let threshold = 5;

[
  | where TimeGenerated > timeframe
  | where EventType=='Logon' and EventResult=='Success'
  | where isnotempty(SrcGeoCountry)
  | summarize StartTime = min(TimeGenerated), EndTime = max(TimeGenerated), Vendors=make_set(EventVendor), Products=make_set(EventProduct), '
  NumOfCountries = dcount( [ DstGeoCountry
                           SrcGeoCountry
                           SrcGeoRegion
                         ]
  | where NumOfCountries >= threshold
  | extend timestamp = StartTime, AccountCustomEntity = TargetUserPrincipalName
```

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

```
let timeframe = ago(3h);
let threshold = 5;

[
  | where TimeGenerated > timeframe
  | where EventType=='Logon' and EventResult=='Success'
  | where isnotempty(SrcGeoCountry)
  | summarize StartTime = min(TimeGenerated), EndTime = max(TimeGenerated), Vendors=make_set(EventVendor), Products=make_set(EventProduct), '
  NumOfCountries = dcount( [ SrcGeoRegion
                           DstGeoCountry
                           SrcGeoCountry
                           SrcGeoRegion
                         ]
  | where NumOfCountries >= threshold
  | extend timestamp = StartTime, AccountCustomEntity = TargetUserPrincipalName
```

NEW QUESTION 156

- (Exam Topic 3)

You have a Microsoft 365 subscription that uses Microsoft 365 Defender A remediation action for an automated investigation quarantines a file across multiple devices. You need to mark the file as safe and remove the file from quarantine on the devices. What should you use m the Microsoft 365 Defender portal?

- A. From Threat tracker, review the queries.
- B. From the History tab in the Action center, revert the actions.
- C. From the investigation page, review the AIR processes.
- D. From Quarantine from the Review page, modify the rules.

Answer: B

NEW QUESTION 161

- (Exam Topic 3)

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.

QUESTION 165

Blades

Hunting blade

Incident blade

Logs blade

Answer Area

Create a bookmark by using the:

Associate a bookmark with the incident by using the:

- 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 166

- (Exam Topic 3)

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 171

- (Exam Topic 3)

You have a Microsoft 365 subscription that contains 1,000 Windows 10 devices. The devices have Microsoft Office 365 installed.

You need to mitigate the following device threats:

- > Microsoft Excel macros that download scripts from untrusted websites
- > Users that open executable attachments in Microsoft Outlook
- > Outlook rules and forms exploits

- A. Microsoft Defender Antivirus
- B. attack surface reduction rules in Microsoft Defender for Endpoint
- C. Windows Defender Firewall
- D. adaptive application control in Azure Defender

Answer: B

Explanation:

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/overview-attack-surface-reduction?v>

NEW QUESTION 174

- (Exam Topic 3)

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)

| 

|         |   |
|---------|---|
|         | ▼ |
| extend  |   |
| join    |   |
| project |   |
| union   |   |

 (

DeviceFileEvents

| 

|         |   |
|---------|---|
|         | ▼ |
| extend  |   |
| join    |   |
| project |   |
| union   |   |

 FileName, SHA256

) on SHA256

| 

|         |   |
|---------|---|
|         | ▼ |
| extend  |   |
| join    |   |
| project |   |
| union   |   |

 Timestamp, FileName, SHA256, DeviceName, DeviceId,

NetworkMessageId, SenderFromAddress, RecipientEmailAddress
```

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:
Reference:
<https://docs.microsoft.com/en-us/microsoft-365/security/mtp/advanced-hunting-query-emails-devices?view=o36>

NEW QUESTION 177
.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questions and Answers in PDF Format

SC-200 Practice Exam Features:

- * SC-200 Questions and Answers Updated Frequently
- * SC-200 Practice Questions Verified by Expert Senior Certified Staff
- * SC-200 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- * SC-200 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

100% Actual & Verified — Instant Download, Please Click
[Order The SC-200 Practice Test Here](#)