

Exam Questions SC-200

Microsoft Security Operations Analyst

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



NEW QUESTION 1

- (Exam Topic 1)

You need to remediate active attacks to meet the technical requirements. What should you include in the solution?

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

Answer: B

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/sentinel/automate-responses-with-playbooks>

NEW QUESTION 2

- (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:	<div><div></div><div>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.</div></div>
External threat:	<div><div></div><div>Implement Azure Firewall. Modify the Key Vault firewall settings. Modify the network security groups (NSGs).</div></div>

- 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 3

- (Exam Topic 1)

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

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

Answer: B

Explanation:

Reference:

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

NEW QUESTION 4

- (Exam Topic 2)

You need to create the analytics rule 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.

Answer Area

Create the rule of type:

Fusion

Microsoft incident creation

Scheduled

Configure the playbook to include:

Diagnostics settings

A service principal

A trigger

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

Create the rule of type:

Fusion

Microsoft incident creation

Scheduled

Configure the playbook to include:

Diagnostics settings

A service principal

A trigger

NEW QUESTION 5

- (Exam Topic 2)
You need to add notes to the events to meet the Azure Sentinel requirements.

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

Actions

Add a bookmark and map an entity.

From Azure Monitor, run a Log Analytics query.

Add the query to favorites.

Select a query result.

From the Azure Sentinel workspace, run a Log Analytics query.

Answer Area

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Graphical user interface, text, application Description automatically generated
Reference:

Passing Certification Exams Made Easy

visit - https://www.2PassEasy.com

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

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 DC1 to meet the business requirements.
Which four actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

Actions

Provide domain administrator credentials to the litware.com Active Directory domain.

Create an instance of Microsoft Defender for Identity.

Provide global administrator credentials to the litware.com Azure AD tenant.

Install the sensor on DC1.

Install the standalone sensor on DC1.

Answer Area

⬅️

➡️

⬆️

⬆️

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:
Text Description automatically generated with medium confidence
Step 1: log in to <https://portal.atp.azure.com> as a global admin Step 2: Create the instance
Step 3. Connect the instance to Active Directory Step 4. Download and install the sensor. Reference:
<https://docs.microsoft.com/en-us/defender-for-identity/install-step1> <https://docs.microsoft.com/en-us/defender-for-identity/install-step4>

NEW QUESTION 8

- (Exam Topic 2)
You need to implement Azure Defender to meet the Azure Defender requirements and the business 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.

Log Analytics workspace to use:

A new Log Analytics workspace in the East US Azure region

Default workspace created by Azure Security Center

LA1

Windows security events to collect:

All Events

Common

Minimal

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Graphical user interface, application Description automatically generated

NEW QUESTION 9

- (Exam Topic 2)

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

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

Answer: C

Explanation:

Reference:

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

NEW QUESTION 10

- (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 10

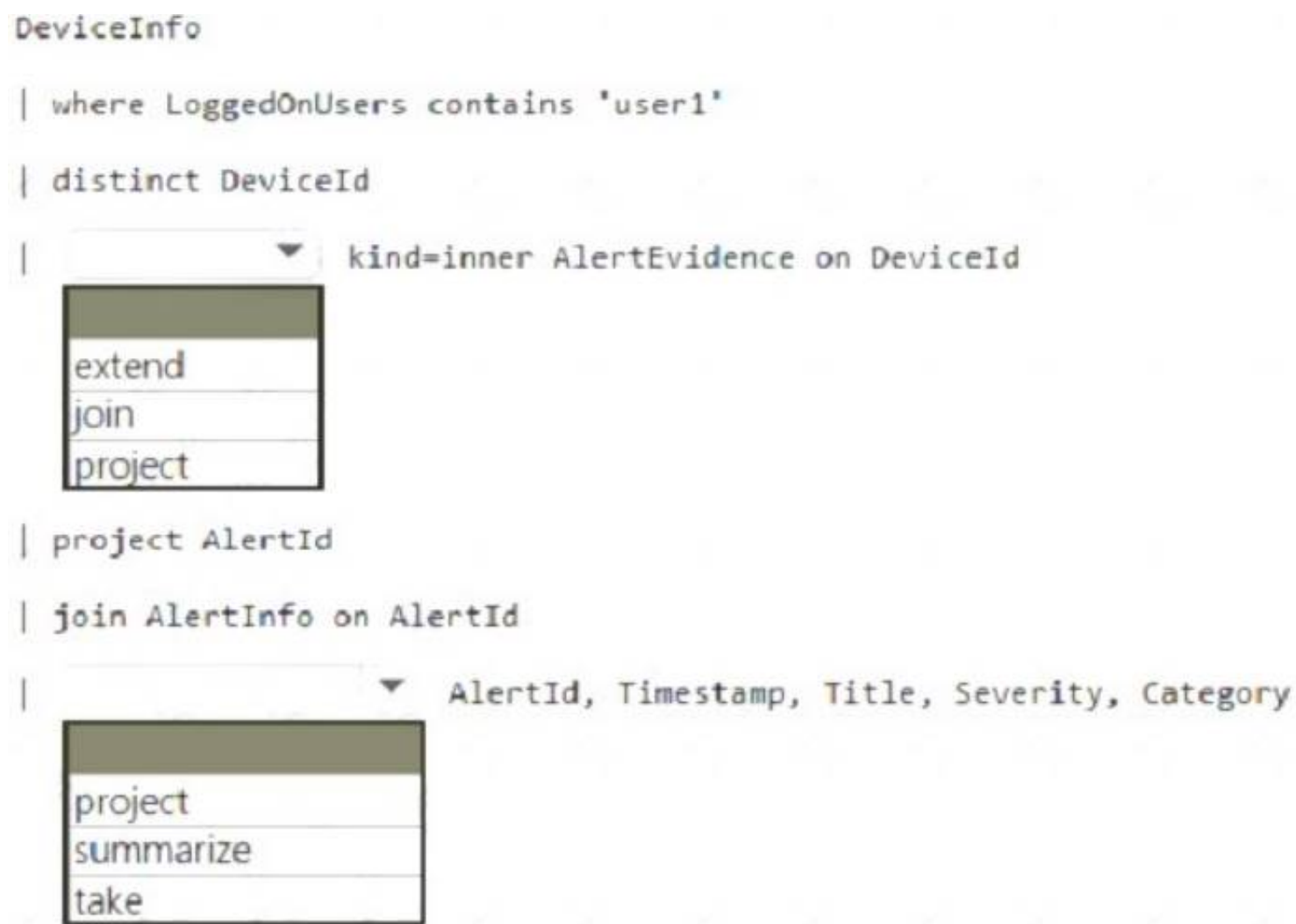
- (Exam Topic 3)

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.



- 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 14

- (Exam Topic 3)

You have a Microsoft Sentinel workspace named Workspace1.

You need to exclude a built-in, source-specific Advanced Security information Model (ASIM) parse from a built-in unified ASIM parser.

What should you create in Workspace1?

- A. a watch list
- B. an analytic rule
- C. a hunting query
- D. a workbook

Answer: A

NEW QUESTION 19

- (Exam Topic 3)

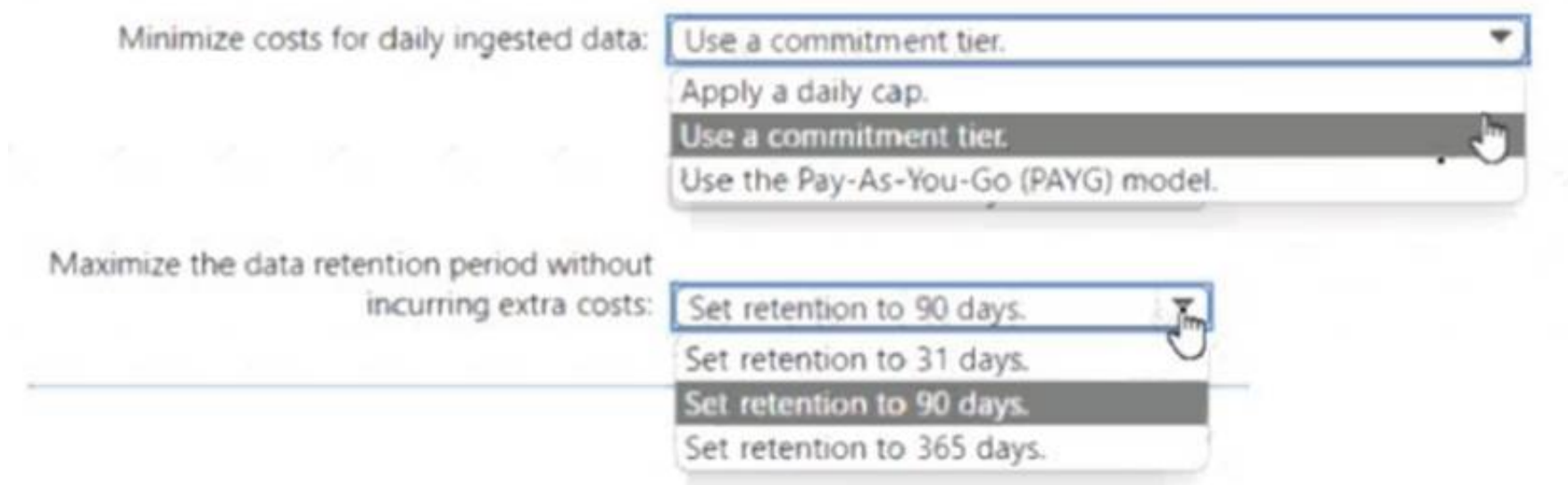
You have an Azure subscription.

You plan to implement an Microsoft Sentinel workspace. You anticipate that you will ingest 20 GB of security log data per day.

You need to configure storage for the workspace. The solution must meet the following requirements:

- Minimize costs for daily ingested data.
- Maximize the data retention period without incurring extra costs.

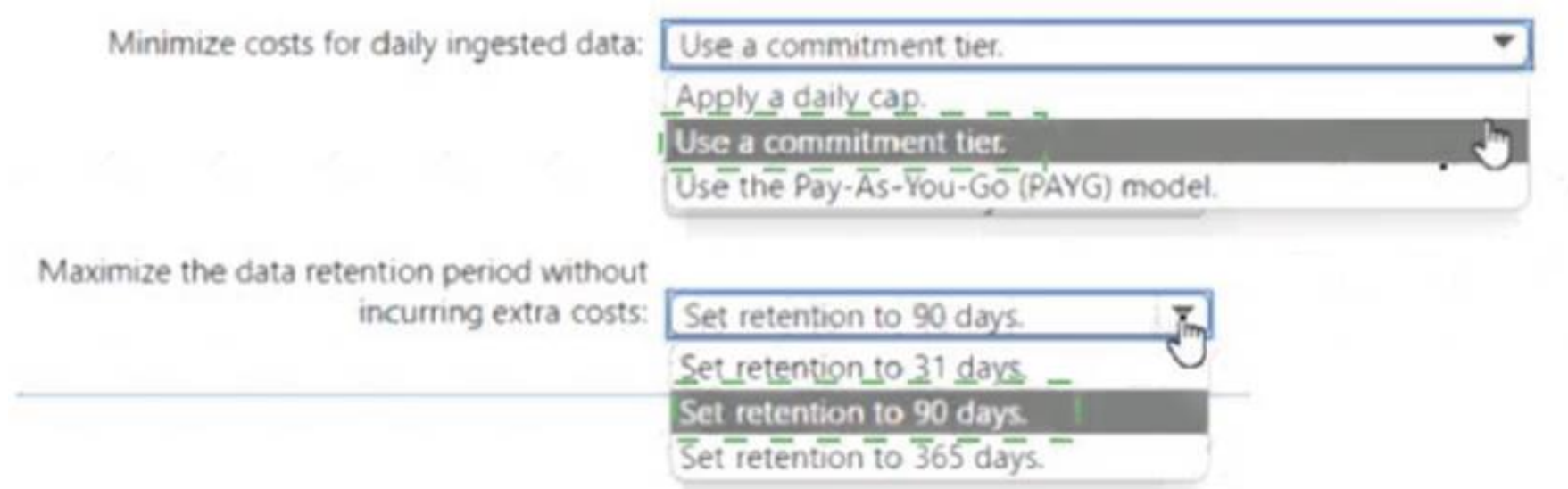
What should you do for each requirement? To answer, select the appropriate options in the answer area. NOTE Each correct selection is worth one point.



- A. Mastered
- B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 21

- (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 from 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 25

- (Exam Topic 3)

You have a Microsoft 365 subscription that uses Azure Defender. You have 100 virtual machines in a resource group named RG1.

You assign the Security Admin roles to a new user named SecAdmin1.

You need to ensure that SecAdmin1 can apply quick fixes to the virtual machines by using Azure Defender. The solution must use the principle of least privilege. Which role should you assign to SecAdmin1?

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

Answer: C

NEW QUESTION 27

- (Exam Topic 3)

You have five on-premises Linux servers.

You have an Azure subscription that uses Microsoft Defender for Cloud. You need to use Defender for Cloud to protect the Linux servers.

What should you install on the servers first?

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

Answer: B

Explanation:

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

* Collect logs and performance data from Azure virtual machines or hybrid machines hosted outside of Azure

* Etc. Reference:

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

<https://docs.microsoft.com/en-us/azure/azure-monitor/agents/agents-overview#log-analytics-agent>

NEW QUESTION 30

- (Exam Topic 3)

You have an Azure subscription.

You need to delegate permissions to meet the following requirements:

➤ Enable and disable Azure Defender.

➤ Apply security recommendations to resource.

The solution must use the principle of least privilege.

Which Azure Security Center role should you use for each requirement? To answer, drag the appropriate roles to the correct requirements. Each role may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

Roles	Answer Area
Security Admin	
Resource Group Owner	
Subscription Contributor	
Subscription Owner	

Enable and disable Azure Defender:	Role
Apply security recommendations to a resource:	Role

- 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/security-center-permissions>

NEW QUESTION 31

- (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",
    "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', 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 33

- (Exam Topic 3)

You have an Azure Functions app that generates thousands of alerts in Azure Security Center each day for normal activity. You need to hide the alerts automatically in Security Center.

Which three actions should you perform in sequence in Security Center? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

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

- A. Mastered
B. Not Mastered

Answer: A

Explanation:

Reference:

<https://techcommunity.microsoft.com/t5/azure-security-center/suppression-rules-for-azure-security-center-alerts>

NEW QUESTION 34

- (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:

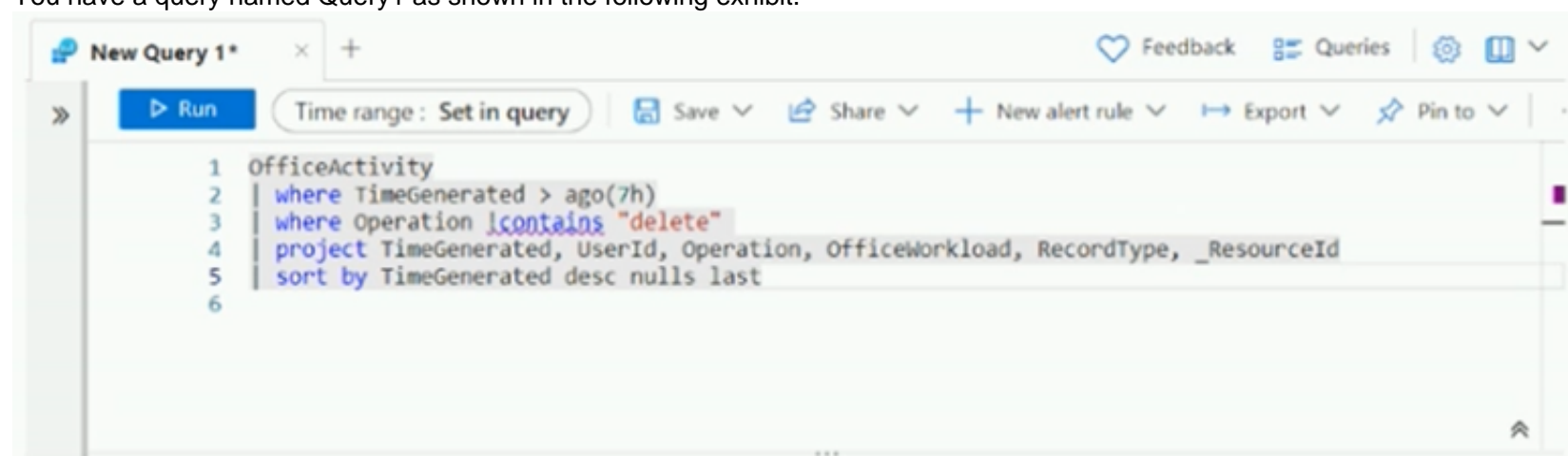
<https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/manage-alerts>

NEW QUESTION 39

- (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 41

- (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 46

- (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 47

- (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:

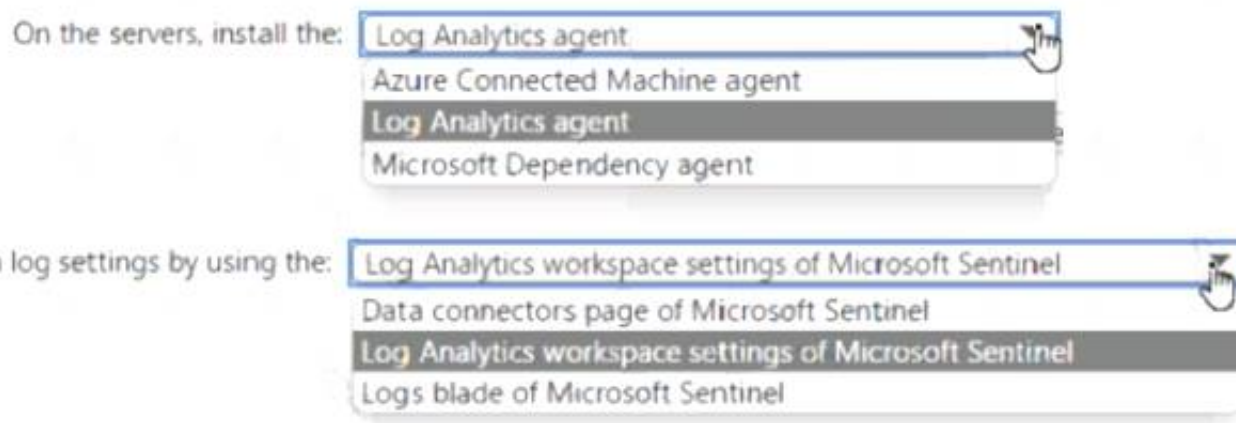
<https://docs.microsoft.com/en-us/azure/sentinel/notebook-get-started> <https://msticpy.readthedocs.io/en/latest/>

NEW QUESTION 49

- (Exam Topic 3)

Your on-premises network contains 100 servers that run Windows Server. You have an Azure subscription that uses Microsoft Sentinel.

You need to upload custom logs from the on-premises servers to Microsoft Sentinel. What should you do? To answer, select the appropriate options in the answer area.



- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

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

NEW QUESTION 53

- (Exam Topic 3)

You plan to create a custom Azure Sentinel query that will provide a visual representation of the security alerts generated by Azure Security Center.

You need to create a query that will be used to display a bar graph. What should you include in the query?

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

Answer: C

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/azure-monitor/visualize/workbooks-chart-visualizations>

NEW QUESTION 56

- (Exam Topic 3)

You provision a Linux virtual machine in a new Azure subscription.

You enable Azure Defender and onboard the virtual machine to Azure Defender.

You need to verify that an attack on the virtual machine triggers an alert in Azure Defender.

Which two Bash commands should you run on the virtual machine? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

A. `cp /bin/echo ./asc_alerttest_662jfi039n`

B. `./alerttest testing eicar pipe`

C. `cp /bin/echo ./alerttest`

D. `./asc_alerttest_662jfi039n testing eicar pipe`

Answer: AD

Explanation:

Reference:

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

NEW QUESTION 59

- (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

Answer Area

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



A. Mastered

B. Not Mastered

Answer: A

Explanation:

Step 1: From Logic App Designer, create a logic app.

Create a logic app and define when it should automatically run

* 1. From Defender for Cloud's sidebar, select Workflow automation.

* 2. To define a new workflow, click Add workflow automation. The options pane for your new automation opens.

Dashboard > Microsoft Defender for Cloud

Microsoft Defender for Cloud | Workflow automation

Showing 73 subscriptions

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

General

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
yoafTes...	Disabled	ASC DEM
EnabeA...	Enabled	ASC Mu
Encrypt...	Enabled	ASC Mu
KerenN...	Enabled	ASC DEM
KerenSh...	Enabled	ASC DEM
KerenTe...	Enabled	ASC DEM
MorAuto	Enabled	ASC DEM
NewDes...	Enabled	ASCDEM

1 Workflow automation

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    },

```

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

NEW QUESTION 64

- (Exam Topic 3)

You receive an alert from Azure Defender for Key Vault.

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

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

What should you do first?

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

Answer: B

Explanation:

Reference:

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

NEW QUESTION 68

- (Exam Topic 3)

You create a new Azure subscription and start collecting logs for Azure Monitor.

You need to configure Azure Security Center to detect possible threats related to sign-ins from suspicious IP addresses to Azure virtual machines. The solution must validate the configuration.

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

Actions	Answer Area
Change the alert severity threshold for emails to Medium .	
Copy an executable file on a virtual machine and rename the file as ASC_AlertTest_662jfi039N.exe.	
Enable Azure Defender for the subscription.	⬅️ ⬆️
Change the alert severity threshold for emails to Low .	➡️ ⬇️
Run the executable file and specify the appropriate arguments.	
Rename the executable file as AlertTest.exe.	

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Reference:

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

NEW QUESTION 71

- (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 75

- (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 Microsoft incident creation rule for a data connector.

Does this meet the goal?

- A. Yes
- B. No

Answer: A

Explanation:

Reference:

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

NEW QUESTION 77

- (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 80

- (Exam Topic 3)

A security administrator receives email alerts from Azure Defender for activities such as potential malware uploaded to a storage account and potential successful brute force attacks.

The security administrator does NOT receive email alerts for activities such as antimalware action failed and suspicious network activity. The alerts appear in Azure Security Center.

You need to ensure that the security administrator receives email alerts for all the activities. What should you configure in the Security Center settings?

- A. the severity level of email notifications
- B. a cloud connector
- C. the Azure Defender plans
- D. the integration settings for Threat detection

Answer: A

Explanation:

Reference:

<https://techcommunity.microsoft.com/t5/microsoft-365-defender/get-email-notifications-on-new-incidents-from>

NEW QUESTION 83

- (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 85

- (Exam Topic 3)

You have a Microsoft Sentinel workspace named sws1.

You need to create a hunting query to identify users that list storage keys of multiple Azure Storage accounts. The solution must exclude users that list storage keys for a single storage account.

How should you complete the query? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.


```

| where OperationNameValue == "microsoft.storage/storageaccounts/listkeys/action"
| where ActivityStatusValue == "Succeeded"
| join kind= inner (
    AzureActivity
    | where OperationNameValue == "microsoft.storage/storageaccounts/listkeys/action"
    | where ActivityStatusValue == "Succeeded"
    | project ExpectedIpAddress=CallerIpAddress, Caller
    | evaluate
        autocluster()
        bin()
        count()
) on Caller
| where CallerIpAddress != ExpectedIpAddress
| summarize ResourceIds = make_set(ResourceId), ResourceIdCount = dcount(ResourceId)
    by OperationNameValue, Caller, CallerIpAddress

```

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Box 1: AzureActivity

The AzureActivity table includes data from many services, including Microsoft Sentinel. To filter in only data from Microsoft Sentinel, start your query with the following code:

Box 2: autocluster()

Example: description: |

'Listing of storage keys is an interesting operation in Azure which might expose additional secrets and PII to callers as well as granting access to VMs. While there are many benign operations of this type, it would be interesting to see if the account performing this activity or the source IP address from which it is being done is anomalous. The query below generates known clusters of ip address per caller, notice that users which only had single operations do not appear in this list as we cannot learn from it their normal activity (only based on a single event). The activities for listing storage account keys is correlated with this learned clusters of expected activities and activity which is not expected is returned.'

```

| where OperationNameValue =~ "microsoft.storage/storageaccounts/listkeys/action"
| where ActivityStatusValue == "Succeeded"
| join kind= inner ( AzureActivity
| where OperationNameValue =~ "microsoft.storage/storageaccounts/listkeys/action"
| where ActivityStatusValue == "Succeeded"
| project ExpectedIpAddress=CallerIpAddress, Caller
| evaluate autocluster()
) on Caller
| where CallerIpAddress != ExpectedIpAddress
| summarize StartTime = min(TimeGenerated), EndTime = max(TimeGenerated), ResourceIds = make_set(ResourceId), ResourceIdCount = dcount(ResourceId)
by OperationNameValue, Caller, CallerIpAddress
| extend timestamp = StartTime, AccountCustomEntity = Caller, IPCustomEntity = CallerIpAddress
Reference:
https://github.com/Azure/Azure-Sentinel/blob/master/Hunting%20Queries/AzureActivity/Anomalous\_Listing\_O

```

NEW QUESTION 90

- (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 Entity tags, you add the accounts as Honeytoken accounts. Does this meet the goal?

- A. Yes
- B. No

Answer: A

Explanation:

Reference:

<https://docs.microsoft.com/en-us/defender-for-identity/manage-sensitive-honeytoken-accounts>

NEW QUESTION 92

- (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 94

- (Exam Topic 3)

You use Azure Sentinel.

You need to receive an immediate alert whenever Azure Storage account keys are enumerated. Which two actions should you perform? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

A. Create a livestream

B. Add a data connector

C. Create an analytics rule

D. Create a hunting query.

E. Create a bookmark.

Answer: BC

Explanation:

B: To add a data connector, you would use the Azure Sentinel data connectors feature to connect to your Azure subscription and to configure log data collection for Azure Storage account key enumeration events.

C: After adding the data connector, you need to create an analytics rule to analyze the log data from the Azure storage connector, looking for the specific event of Azure storage account keys enumeration. This rule will trigger an alert when it detects the specific event, allowing you to take immediate action.

NEW QUESTION 98

- (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 99

- (Exam Topic 3)

You plan to create a custom Azure Sentinel query that will track anomalous Azure Active Directory (Azure AD) sign-in activity and present the activity as a time chart aggregated by day.

You need to create a query that will be used to display the time chart. What should you include in the query?

- A. extend
- B. bin
- C. makeset
- D. workspace

Answer: B

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/azure-monitor/logs/get-started-queries>

NEW QUESTION 103

- (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: <input type="text"/>
Owner	User2: <input type="text"/>
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 104

- (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 106

- (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

SW1

CEF1

Server1

Server2

Answer Area

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

From the Log Analytics agent, disable Syslog synchronization.

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Graphical user interface, text Description automatically generated

Reference:

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

NEW QUESTION 110

- (Exam Topic 3)

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

You have Microsoft SharePoint Online sites that contain sensitive documents. The documents contain customer account numbers that each consists of 32 alphanumeric characters.

You need to create a data loss prevention (DLP) policy to protect the sensitive documents. What should you use to detect which documents are sensitive?

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

Answer: C

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/information-protection/what-is-information-protection>

NEW QUESTION 115

- (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 119

- (Exam Topic 3)

You have an Azure subscription named Sub1 and a Microsoft 365 subscription. Sub1 is linked to an Azure Active Directory (Azure AD) tenant named contoso.com. You create an Azure Sentinel workspace named workspace1. In workspace1, you activate an Azure AD connector for contoso.com and an Office 365 connector for the Microsoft 365 subscription.

You need to use the Fusion rule to detect multi-staged attacks that include suspicious sign-ins to contoso.com followed by anomalous Microsoft Office 365 activity. Which two actions should you perform? Each correct answer present part of the solution.

NOTE: Each correct selection is worth one point.

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

Answer: AD

Explanation:

To use the Fusion rule to detect multi-staged attacks that include suspicious sign-ins to contoso.com followed by anomalous Microsoft Office 365 activity, you should perform the following two actions:

- Create an Azure AD Identity Protection connector. This will allow you to monitor suspicious activities in your Azure AD tenant and detect malicious sign-ins.
- Create a custom rule based on the Office 365 connector templates. This will allow you to monitor and detect anomalous activities in the Microsoft 365 subscription.

Reference: <https://docs.microsoft.com/en-us/azure/sentinel/fusion-rules>

NEW QUESTION 121

- (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 122

- (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 123

- (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

From Azure Sentinel, select Hunting.

Filter by tactics.

Select Run All Queries.

NEW QUESTION 127

- (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 129

- (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 134

- (Exam Topic 3)

You have a Microsoft Sentinel workspace named workspace1 and an Azure virtual machine named VM1. You receive an alert for suspicious use of PowerShell on VM1.

You need to investigate the incident, identify which event triggered the alert, and identify whether the following actions occurred on VM1 after the alert:

- > The modification of local group memberships
- > The purging of event logs

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

Actions

From the details pane of the incident, select **Investigate**.

From the Investigation blade, select the entity that represents VM1.

From the Investigation blade, select the entity that represents powershell.exe.

From the Investigation blade, select **Timeline**.

From the Investigation blade, select **Info**.

From the Investigation blade, select **Insights**.

Answer Area

>

<

^

v

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Step 1: From the Investigation blade, select Insights

The Investigation Insights Workbook is designed to assist in investigations of Azure Sentinel Incidents or individual IP/Account/Host/URL entities.

Step 2: From the Investigation blade, select the entity that represents VM1.

The Investigation Insights workbook is broken up into 2 main sections, Incident Insights and Entity Insights. Incident Insights

The Incident Insights gives the analyst a view of ongoing Sentinel Incidents and allows for quick access to their associated metadata including alerts and entity information.

Entity Insights

The Entity Insights allows the analyst to take entity data either from an incident or through manual entry and explore related information about that entity. This workbook presently provides view of the following entity types:

IP Address Account Host

URL

Step 3: From the details pane of the incident, select Investigate. Choose a single incident and click View full details or Investigate. Reference:

<https://github.com/Azure/Azure-Sentinel/wiki/Investigation-Insights---Overview> <https://docs.microsoft.com/en-us/azure/sentinel/investigate-cases>

NEW QUESTION 138

- (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 139

- (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-intellige>

NEW QUESTION 144

- (Exam Topic 3)

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.

Azure Sentinel Contributor	
Azure Sentinel Responder	Create and run playbooks:
Azure Sentinel Reader	Create workbooks and analytic rules:
Logic App Contributor	

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

A picture containing graphical user interface Description automatically generated

Reference:

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

NEW QUESTION 147

- (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 151

- (Exam Topic 3)

You have a Microsoft 365 E5 subscription that contains 200 Windows 10 devices enrolled in Microsoft Defender for Endpoint.

You need to ensure that users can access the devices by using a remote shell connection directly from the Microsoft 365 Defender portal. The solution must use the principle of least privilege.

What should you do in the Microsoft 365 Defender portal? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

To configure Microsoft Defender for Endpoint:

Turn on endpoint detection and response (EDR) in block mode
Turn on Live Response
Turn off Tamper Protection

To configure the devices:

Add a network assessment job
Create a device group that contains the devices and set Automation level to Full
Create a device group that contains the devices and set Automation level to No automated response

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Box 1: Turn on Live Response

Live response is a capability that gives you instantaneous access to a device by using a remote shell connection. This gives you the power to do in-depth investigative work and take immediate response actions.

Box: 2 : Add a network assessment job

Network assessment jobs allow you to choose network devices to be scanned regularly and added to the device inventory.

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/respond-machine-alerts?view=o365-> <https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/network-devices?view=o365-worldw>

NEW QUESTION 152

- (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 157

- (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 160

- (Exam Topic 3)

You have resources in Azure and Google cloud.

You need to ingest Google Cloud Platform (GCP) data into Azure Defender.

In which order should you perform the actions? To answer, move all actions from the list of actions to the answer area and arrange them in the correct order.

Actions

Answer Area

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



- A. Mastered
B. Not Mastered

Answer: A

Explanation:

Reference:
<https://docs.microsoft.com/en-us/azure/security-center/quickstart-onboard-gcp>

NEW QUESTION 165

- (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 170

- (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;

imAuthentication
imNetworkSession
imProcessCreate
imWebSession

| 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
) by TargetUserId, TargetUserPrincipalName, TargetUserType

| 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( SrcGeoCountry ) by TargetUserId, TargetUserPrincipalName, TargetUserType

| where NumOfCountries >= threshold
| extend timestamp = StartTime, AccountCustomEntity = TargetUserPrincipalName
```

NEW QUESTION 174

- (Exam Topic 3)

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

```
DeviceProcessEvents
| where Timestamp > ago (24h)
and InitiatingProcessFileName =~ 'runsl132.exe'
and InitiatingProcessCommandLine !contains " " and InitiatingProcessCommandLine != ""
and FileName in~ ('schtasks.exe')
and ProcessCommandLine has 'Change' and ProcessCommandLine has 'SystemRestore'
and ProcessCommandLine has 'disable'
| project Timestamp, AccountName, ProcessCommandLine
```

You need to receive an alert when any process disables System Restore on a device managed by Microsoft Defender during the last 24 hours. Which two actions should you perform? Each correct answer presents part of the solution. NOTE: Each correct selection is worth one point.

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

Answer: AE

Explanation:

Reference:

<https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/custom-detection-rules>

NEW QUESTION 178

- (Exam Topic 3)

You have the following environment:

- > Azure Sentinel
- > A Microsoft 365 subscription
- > Microsoft Defender for Identity
- > An Azure Active Directory (Azure AD) tenant

You configure Azure Sentinel to collect security logs from all the Active Directory member servers and domain controllers.

You deploy Microsoft Defender for Identity by using standalone sensors.

You need to ensure that you can detect when sensitive groups are modified in Active Directory. Which two actions should you perform? Each correct answer presents part of the solution. NOTE: Each correct selection is worth one point.

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

Answer: AD

Explanation:

Reference:

<https://docs.microsoft.com/en-us/defender-for-identity/configure-windows-event-collection> <https://docs.microsoft.com/en-us/defender-for-identity/configure-event-collection>

NEW QUESTION 180

- (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 in 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 185

- (Exam Topic 3)

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

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

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

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

NOTE: Each correct selection is worth one point.

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

Answer: AD

NEW QUESTION 187

- (Exam Topic 3)

You need to receive a security alert when a user attempts to sign in from a location that was never used by the other users in your organization to sign in.

Which anomaly detection policy should you use?

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

Answer: C

Explanation:

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

Reference:

<https://docs.microsoft.com/en-us/cloud-app-security/anomaly-detection-policy>

NEW QUESTION 189

- (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
- What should you use?

- 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 191

- (Exam Topic 3)

You use Azure Sentinel.

You need to use a built-in role to provide a security analyst with the ability to edit the queries of custom Azure Sentinel workbooks. The solution must use the principle of least privilege.

Which role should you assign to the analyst?

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

Answer: A

Explanation:

Azure Sentinel Contributor can create and edit workbooks, analytics rules, and other Azure Sentinel resources. Reference:

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

NEW QUESTION 192

.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

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

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

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

Money Back Guarantee

SC-200 Practice Exam Features:

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