

Microsoft

Exam Questions SC-200

Microsoft Security Operations Analyst



NEW QUESTION 1

- (Exam Topic 1)

You need to complete the query for failed sign-ins to meet the technical requirements. Where can you find the column name to complete the where clause?

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

Answer: D

NEW QUESTION 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)

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 4

- (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 5

- (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 6

- (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 7

- (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 8

- (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 9

- (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

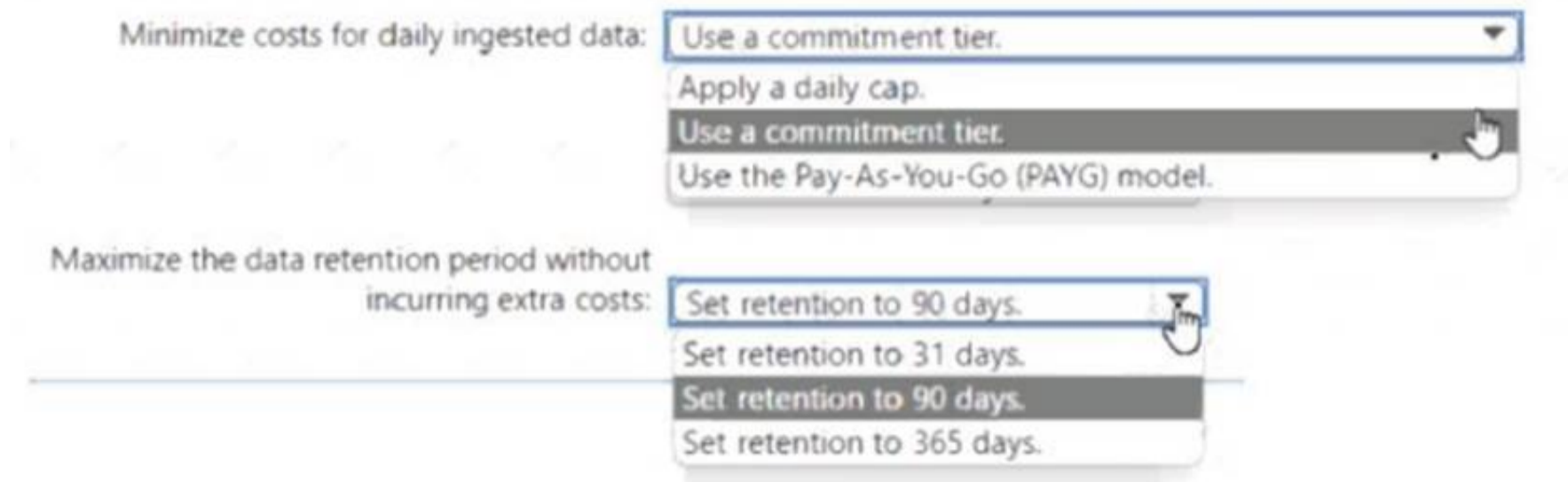
Explanation:
Graphical user interface, application Description automatically generated

NEW QUESTION 10

- (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.

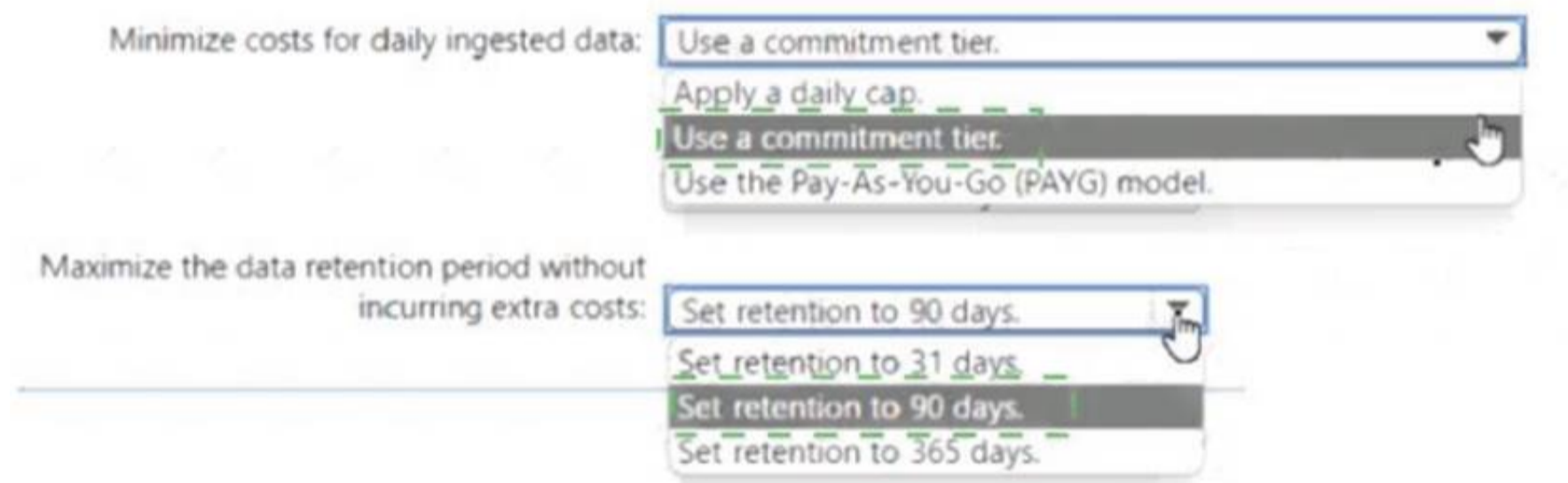
What should you do for each requirement? To answer, select the appropriate options in the answer area. NOTE Each correct selection is worth one point.



- A. Mastered
- B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 10

- (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 13

- (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 18

- (Exam Topic 3)

You have a Microsoft Sentinel workspace named Workspaces

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

What should you create in Workspace1?

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

Answer: D

Explanation:

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

NEW QUESTION 20

- (Exam Topic 3)

You create a hunting query in Azure Sentinel.

You need to receive a notification in the Azure portal as soon as the hunting query detects a match on the query. The solution must minimize effort.

What should you use?

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

Answer: C

Explanation:

Use livestream to run a specific query constantly, presenting results as they come in. Reference:

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

NEW QUESTION 24

- (Exam Topic 3)

You have a third-party security information and event management (SIEM) solution.

You need to ensure that the SIEM solution can generate alerts for Azure Active Directory (Azure AD) sign-events in near real time.

What should you do to route events to the SIEM solution?

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

Answer: B

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/overview-monitoring>

NEW QUESTION 29

- (Exam Topic 3)

You have an Azure Sentinel workspace.

You need to test a playbook manually in the Azure portal. From where can you run the test in Azure Sentinel?

- A. Playbooks
- B. Analytics
- C. Threat intelligence
- D. Incidents

Answer: D

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/sentinel/tutorial-respond-threats-playbook#run-a-playbook-on-demand>

NEW QUESTION 32

- (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 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 38

- (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 use Azure Security Center.

You receive a security alert in Security Center.

You need to view recommendations to resolve the alert in Security Center. Solution: From Regulatory compliance, you download the report.

Does this meet the goal?

- A. Yes
- B. No

Answer: B

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/security-center/security-center-managing-and-responding-alerts>

NEW QUESTION 42

- (Exam Topic 3)

You are investigating an incident by using Microsoft 365 Defender.

You need to create an advanced hunting query to count failed sign-in authentications on three devices named CFOLaptop, CEOLaptop, and COOLaptop.

How should you complete the query? To answer, select the appropriate options in the answer area. NOTE Each correct selection is worth one point

| Values | Answer Area |
|--|-------------|
| project LogonFailures=count() | |
| summarize LogonFailures=count() by DeviceName, LogonType | |
| where ActionType == FailureReason | |
| where DeviceName in ("CFOLaptop", "CEOLaptop", "COOLaptop") | and |
| ActionType == "LogonFailed" | |
| ActionType == FailureReason | |
| DeviceEvents | |
| DeviceLogonEvents | |

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

| Values | Answer Area |
|--|--|
| project LogonFailures=count() | |
| summarize LogonFailures=count() by DeviceName, LogonType | |
| where ActionType == FailureReason | DeviceLogonEvents |
| where DeviceName in ("CFOLaptop", "CEOLaptop", "COOLaptop") | where DeviceName in ("CFOLaptop", "CEOLaptop", "COOLaptop") and |
| ActionType == "LogonFailed" | ActionType == FailureReason |
| ActionType == FailureReason | summarize LogonFailures=count() by DeviceName, LogonType |
| DeviceEvents | |
| DeviceLogonEvents | |

NEW QUESTION 45

- (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 50

- (Exam Topic 3)

You use Azure Security Center. You receive a security alert in Security Center.

You need to view recommendations to resolve the alert in Security Center. What should you do?

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

Answer: B

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/security-center/security-center-managing-and-responding-alerts>

NEW QUESTION 52

- (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 53

- (Exam Topic 3)

You have a Microsoft Sentinel workspace that contains the following incident. Brute force attack against Azure Portal analytics rule has been triggered.

You need to identify the geolocation information that corresponds to the incident. What should you do?

- A. From Overview, review the Potential malicious events map.
- B. From Incidents, review the details of the iPCustomEntity entity associated with the incident.
- C. From Incidents, review the details of the AccouncCuscomEntity entity associated with the incident.
- D. From Investigation, review insights on the incident entity.

Answer: A

Explanation:

Potential malicious events: When traffic is detected from sources that are known to be malicious, Microsoft Sentinel alerts you on the map. If you see orange, it is inbound traffic: someone is trying to access your organization from a known malicious IP address. If you see Outbound (red) activity, it means that data from your network is being streamed out of your organization to a known malicious IP address.

NEW QUESTION 57

- (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    },

```

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

NEW QUESTION 61

- (Exam Topic 3)

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

You need to review new attack techniques discovered by Microsoft and identify vulnerable resources in the subscription. The solution must minimize administrative effort

Which blade should you use in the Microsoft 365 Defender portal?

- A. Advanced hunting
- B. Threat analytics
- C. Incidents & alerts
- D. Learning hub

Answer: B

Explanation:

To review new attack techniques discovered by Microsoft and identify vulnerable resources in the subscription, you should use the Threat Analytics blade in the

Microsoft 365 Defender portal. The Threat Analytics blade provides insights into attack techniques, configuration vulnerabilities, and suspicious activities, and it can help you identify risks and prioritize threats in your environment.

Reference: <https://docs.microsoft.com/en-us/microsoft-365/security/mtp/microsoft-365-defender-threat-analyti>

NEW QUESTION 62

- (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 63

- (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 use Azure Security Center.

You receive a security alert in Security Center.

You need to view recommendations to resolve the alert in Security Center.

Solution: From Security alerts, you select the alert, select Take Action, and then expand the Prevent future attacks section.

Does this meet the goal?

- A. Yes
- B. No

Answer: B

Explanation:

You need to resolve the existing alert, not prevent future alerts. Therefore, you need to select the 'Mitigate the threat' option.

Reference:

<https://docs.microsoft.com/en-us/azure/security-center/security-center-managing-and-responding-alerts>

NEW QUESTION 68

- (Exam Topic 3)

You have a Microsoft 365 tenant that uses Microsoft Exchange Online and Microsoft Defender for Office 365. What should you use to identify whether zero-hour auto purge (ZAP) moved an email message from the mailbox of a user?

- A. the Threat Protection Status report in Microsoft Defender for Office 365
- B. the mailbox audit log in Exchange
- C. the Safe Attachments file types report in Microsoft Defender for Office 365
- D. the mail flow report in Exchange

Answer: A

Explanation:

To determine if ZAP moved your message, you can use either the Threat Protection Status report or Threat Explorer (and real-time detections).

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/zero-hour-auto-purge?view=o365-w>

NEW QUESTION 71

- (Exam Topic 3)

You have a Microsoft 365 E5 subscription that is linked to a hybrid Azure AD tenant.

You need to identify all the changes made to Domain Admins group during the past 30 days. What should you use?

- A. the Azure Active Directory Provisioning Analysis workbook
- B. the Overview settings of Insider risk management
- C. the Modifications of sensitive groups report in Microsoft Defender for Identity
- D. the identity security posture assessment in Microsoft Defender for Cloud Apps

Answer: C

NEW QUESTION 76

- (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 79

- (Exam Topic 3)

You create an Azure subscription.

You enable Microsoft Defender for Cloud for the subscription.

You need to use Defender for Cloud to protect on-premises computers. What should you do on the on-premises computers?

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

Answer: C

Explanation:

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

NEW QUESTION 84

- (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 89

- (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 93

- (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 =

EmailAttachementInfo

EmailEvents

IdentityLogonEvents

| where MalwareFilterVerdict == "Malware"

| project TimeEmail = Timestamp, Subject, SenderFromAddress, AccountName =

tostring(split (RecipientEmailAddress, "@") [0]);

MaliciousEmails

| join (

EmailAttachementInfo

EmailEvents

IdentityLogonEvents

| project LogonTime = Timestamp, AccountName, DeviceName

) on AccountName

| where (LogonTime - TimeEmail) between (0min.. 60min)

|

select 20

take 20

top 20

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

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 98

- (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 initiativesEdit security policiesEnable automatic provisioning |
| User2 | <ul style="list-style-type: none">View alerts and recommendationsApply security recommendationsDismiss alerts |

The solution must use the principle of least privilege.
Which role should you assign to each user? To answer, drag the appropriate roles to the correct users. Each role may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

Roles

Contributor

Owner

Security administrator

Security reader

Answer Area

User1:

User2:

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Box 1: Owner

Only the Owner can assign initiatives. Box 2: Contributor
Only the Contributor or the Owner can apply security recommendations.
Reference:
<https://docs.microsoft.com/en-us/azure/defender-for-cloud/permissions>

NEW QUESTION 102

- (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 104

- (Exam Topic 3)

You have 50 on-premises servers.

You have an Azure subscription that uses Microsoft Defender for Cloud. The Defender for Cloud deployment has Microsoft Defender for Servers and automatic provisioning enabled.

You need to configure Defender for Cloud to support the on-premises servers. The solution must meet the following requirements:

- Provide threat and vulnerability management.
- Support data collection rules.

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 the Data controller settings in the Azure portal, create an Azure Arc data controller.

On the on-premises servers, install the Azure Monitor agent.

From the Add servers with Azure Arc settings in the Azure portal, generate an installation script.

On the on-premises servers, install the Azure Connected Machine agent.

On the on-premises servers, install the Log Analytics agent.

>

<

1

2

3

Answer Area

⬆

⬇

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

To configure Defender for Cloud to support the on-premises servers, you should perform the following three actions in sequence:

- On the on-premises servers, install the Azure Connected Machine agent.
- On the on-premises servers, install the Log Analytics agent.
- From the Data controller settings in the Azure portal, create an Azure Arc data controller.

Once these steps are completed, the on-premises servers will be able to communicate with the Azure Defender for Cloud deployment and will be able to support threat and vulnerability management as well as data collection rules.

Reference: <https://docs.microsoft.com/en-us/azure/security-center/deploy-azure-security-center#on-premises-d>

NEW QUESTION 109

- (Exam Topic 3)

Your company stores the data for every project in a different Azure subscription. All the subscriptions use the same Azure Active Directory (Azure AD) tenant. Every project consists of multiple Azure virtual machines that run Windows Server. The Windows events of the virtual machines are stored in a Log Analytics workspace in each machine's respective subscription.

You deploy Azure Sentinel to a new Azure subscription.

You need to perform hunting queries in Azure Sentinel to search across all the Log Analytics workspaces of all the subscriptions.

Which two actions should you perform? Each correct answer presents part of the solution. NOTE: Each correct selection is worth one point.

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

Answer: BE

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

NEW QUESTION 112

- (Exam Topic 3)
You use Azure Defender.
You have an Azure Storage account that contains sensitive information.
You need to run a PowerShell script if someone accesses the storage account from a suspicious IP address. Which two actions should you perform? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

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

Answer: AC

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

NEW QUESTION 115

- (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 checked="" type="radio"/> | <input 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 116

- (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 117

- (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 | From the Syslog configuration, remove the facilities that send CEF messages. | <input type="text"/> |
| CEF1 | | |
| Server1 | From the Log Analytics agent, disable Syslog synchronization. | <input type="text"/> |
| Server2 | | |

- 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 122

- (Exam Topic 3)

You are configuring Microsoft Cloud App Security.

You have a custom threat detection policy based on the IP address ranges of your company's United States-based offices.

You receive many alerts related to impossible travel and sign-ins from risky IP addresses. You determine that 99% of the alerts are legitimate sign-ins from your corporate offices. You need to prevent alerts for legitimate sign-ins from known locations.

Which two actions should you perform? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

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

Answer: AD

NEW QUESTION 127

- (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 131

- (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 135

- (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 136

- (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 140

- (Exam Topic 3)
You create an Azure subscription.
You enable Azure Defender for the subscription.
You need to use Azure Defender to protect on-premises computers. What should you do on the on-premises computers?

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

Answer: A

Explanation:

Security Center collects data from your Azure virtual machines (VMs), virtual machine scale sets, IaaS containers, and non-Azure (including on-premises) machines to monitor for security vulnerabilities and threats.
Data is collected using:
The Log Analytics agent, which reads various security-related configurations and event logs from the machine and copies the data to your workspace for analysis.

Examples of such data are: operating system type and version, operating system logs (Windows event logs), running processes, machine name, IP addresses, and logged in user.

Security extensions, such as the Azure Policy Add-on for Kubernetes, which can also provide data to Security Center regarding specialized resource types.

Reference:

<https://docs.microsoft.com/en-us/azure/security-center/security-center-enable-data-collection>

NEW QUESTION 145

- (Exam Topic 3)

Your company has a single office in Istanbul and a Microsoft 365 subscription.

The company plans to use conditional access policies to enforce multi-factor authentication (MFA). You need to enforce MFA for all users who work remotely.

What should you include in the solution?

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

Answer: C

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/location-condition>

NEW QUESTION 147

- (Exam Topic 3)

You need to visualize Azure Sentinel data and enrich the data by using third-party data sources to identify indicators of compromise (IoC).

What should you use?

- A. notebooks in Azure Sentinel
- B. Microsoft Cloud App Security
- C. Azure Monitor
- D. hunting queries in Azure Sentinel

Answer: A

Explanation:

Reference:

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

NEW QUESTION 152

- (Exam Topic 3)

Your company uses Microsoft Sentinel

A new security analyst reports that she cannot assign and resolve incidents in Microsoft Sentinel.

You need to ensure that the analyst can assign and resolve incidents. The solution must use the principle of least privilege.

Which role should you assign to the analyst?

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

Answer: A

Explanation:

The Microsoft Sentinel Responder role allows users to investigate, triage, and resolve security incidents, which includes the ability to assign incidents to other users. This role is designed to provide the necessary permissions for incident management and response while still adhering to the principle of least privilege. Other roles such as Logic App Contributor and Microsoft Sentinel Contributor would have more permissions than necessary and may not be suitable for the analyst's needs. Microsoft Sentinel Reader role is not sufficient as it doesn't have permission to assign and resolve incidents.

Reference: <https://docs.microsoft.com/en-us/azure/sentinel/role-based-access-control-rbac>

NEW QUESTION 157

- (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: You add the accounts to an Active Directory group and add the group as a Sensitive group. 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 160

- (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 163

- (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:

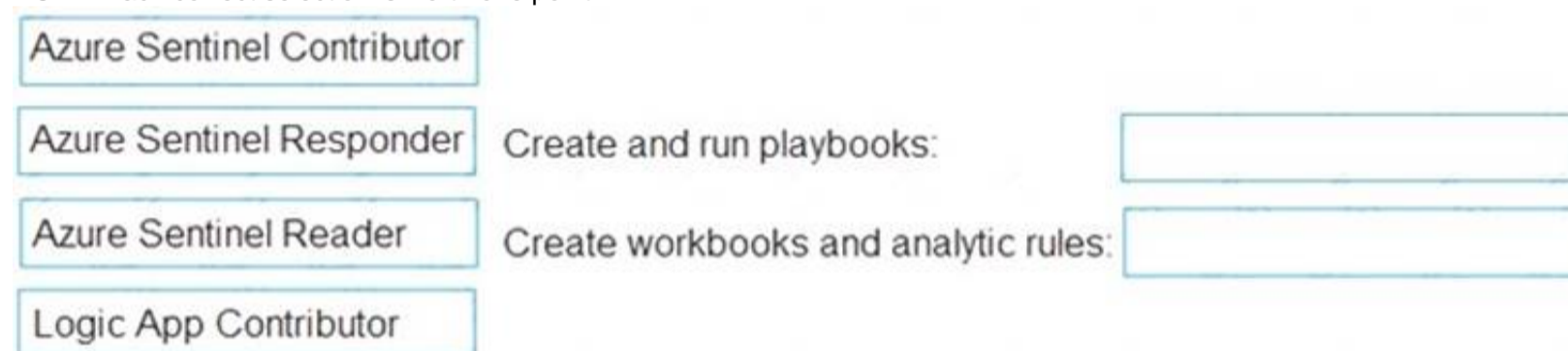
- > Create and run playbooks
- > Create workbooks and analytic rules.

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.



- 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 165

- (Exam Topic 3)

You have a Microsoft Sentinel workspace.

You need to prevent a built-in Advance Security information Model (ASIM) parse from being updated automatically.

What are two ways to achieve this goal? Each correct answer presents a complete solution. NOTE: Each correct selection is worth one point.

- A. Redeploy the built-in parse and specify a CallerContext parameter of any and a SourceSpecificParse parameter of any.
- B. Create a hunting query that references the built-in parse.
- C. Redeploy the built-in parse and specify a CallerContext parameter of built-in.
- D. Build a custom unify parse and include the build- parse version
- E. Create an analytics rule that includes the built-in parse

Answer: AD

NEW QUESTION 167

- (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 168

- (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:

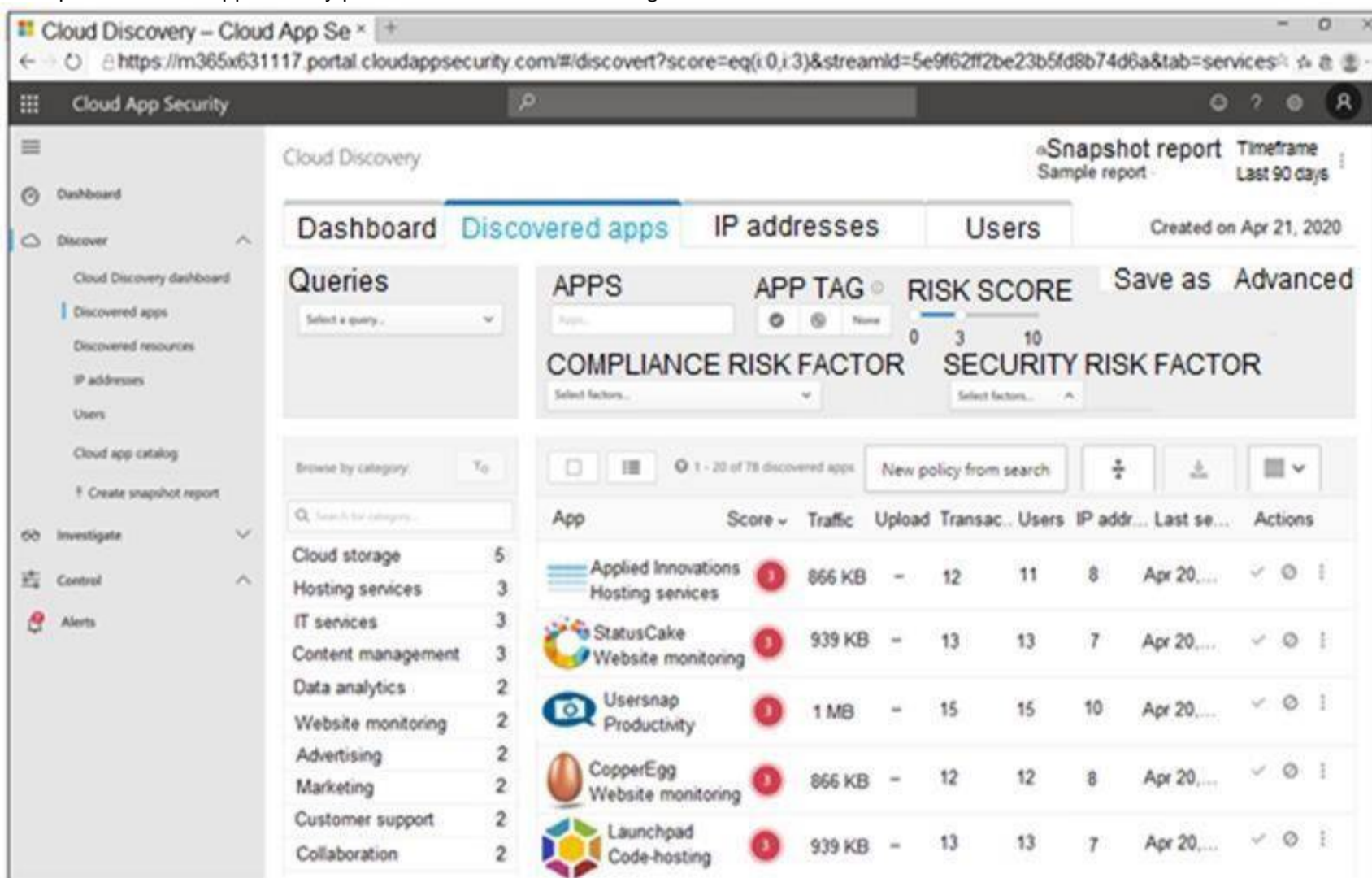
Reference:

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

NEW QUESTION 170

- (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

Answer Area

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.



A. Mastered

B. Not Mastered

Answer: A

Explanation:

Reference:

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

NEW QUESTION 171

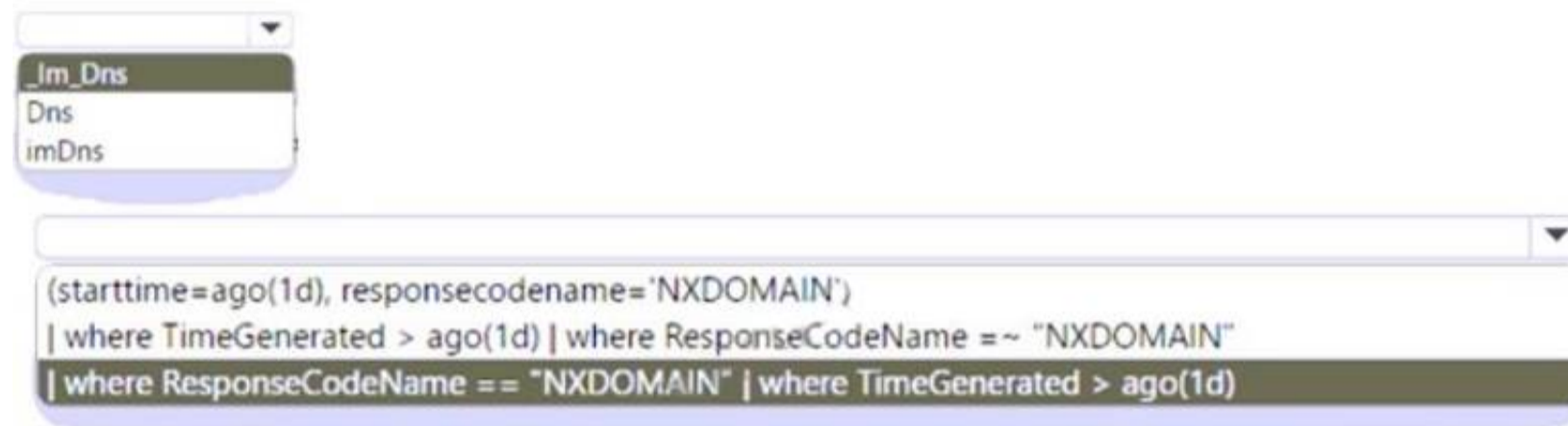
- (Exam Topic 3)

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.

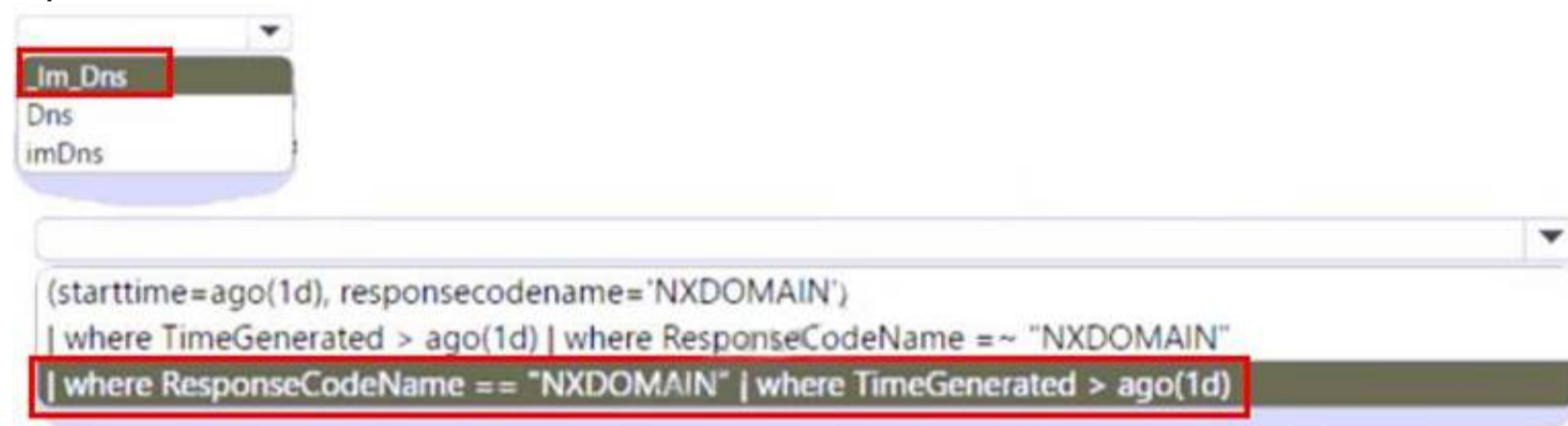


A. Mastered

B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 174

- (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 176

- (Exam Topic 3)

You have an Azure subscription that uses Microsoft Sentinel. You detect a new threat by using a hunting query.

You need to ensure that Microsoft Sentinel automatically detects the threat. The solution must minimize administrative effort.

What should you do?

A. Create a playbook.

B. Create a watchlist.

- C. Create an analytics rule.
- D. Add the query to a workbook.

Answer: C

Explanation:

By creating an analytics rule, you can set up a query that will automatically run and alert you when the threat is detected, without having to manually run the query. This will help minimize administrative effort, as you can set up the rule once and it will run on a schedule, alerting you when the threat is detected. Reference: <https://docs.microsoft.com/en-us/azure/sentinel/analytics-create-rule>

NEW QUESTION 181

- (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 184

- (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 <code>userName</code> field is set as the account entity. | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| The watchlist cannot be updated after it is created. | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| The <code>IPList</code> variable is set as the IP address entity. | <input type="checkbox"/> | <input checked="" type="checkbox"/> |

NEW QUESTION 188

- (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

Enable Security Health Analytics.

From Azure Security Center, add cloud connectors.

Configure the GCP Security Command Center.

Create a dedicated service account and a private key.

Enable the GCP Security Command Center API.

Answer Area

←

→

↑

↓

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Reference:

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

NEW QUESTION 189

- (Exam Topic 3)

You have an Azure subscription that uses Microsoft Sentinel.

You need to minimize the administrative effort required to respond to the incidents and remediate the security threats detected by Microsoft Sentinel.

Which two features should you use? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

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

Answer: CD

Explanation:

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

NEW QUESTION 194

- (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 198

- (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 203

- (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 in the Review page, modify the rules.

Answer: B

NEW QUESTION 208

- (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 209

- (Exam Topic 3)

You create an Azure subscription named sub1.

In sub1, you create a Log Analytics workspace named workspace1.

You enable Azure Security Center and configure Security Center to use workspace1.

You need to ensure that Security Center processes events from the Azure virtual machines that report to workspace1.

What should you do?

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

Answer: A

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/security-center/security-center-enable-data-collection>

NEW QUESTION 213

- (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 214

- (Exam Topic 3)

You have a custom analytics rule to detect threats in Azure Sentinel.

You discover that the analytics rule stopped running. The rule was disabled, and the rule name has a prefix of AUTO DISABLED.

What is a possible cause of the issue?

- A. There are connectivity issues between the data sources and Log Analytics.
- B. The number of alerts exceeded 10,000 within two minutes.
- C. The rule query takes too long to run and times out.
- D. Permissions to one of the data sources of the rule query were modified.

Answer: D

Explanation:

Reference:

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

NEW QUESTION 217

- (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 219

- (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 224

.....

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](#)