

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

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

Answer: D

Explanation:

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

NEW QUESTION 6

- (Exam Topic 2)

You need to 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 7

- (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 8

- (Exam Topic 3)

You purchase a Microsoft 365 subscription.

You plan to configure Microsoft Cloud App Security.

You need to create a custom template-based policy that detects connections to Microsoft 365 apps that originate from a botnet network.

What should you use? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Policy template type:

	▼
Access policy	
Activity policy	
Anomaly detection policy	

Filter based on:

	▼
IP address tag	
Source	
User agent string	

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Graphical user interface, text, application, table Description automatically generated

Reference:

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

NEW QUESTION 9

- (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 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 10

- (Exam Topic 3)

You are investigating an incident in Azure Sentinel that contains more than 127 alerts. You discover eight alerts in the incident that require further investigation.

You need to escalate the alerts to another Azure Sentinel administrator. What should you do to provide the alerts to the administrator?

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

Answer: D

Explanation:

Reference:

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

NEW QUESTION 14

- (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)

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 22

- (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 24

- (Exam Topic 3)

You have an Azure subscription that uses Microsoft Defender for Endpoint.
You need to ensure that you can allow or block a user-specified range of IP addresses and URLs.
What should you enable first in the advanced features from the Endpoints Settings in the Microsoft 365 Defender portal?

- A. endpoint detection and response (EDR) in block mode
- B. custom network indicators
- C. web content filtering
- D. Live response for servers

Answer: A

NEW QUESTION 25

- (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 m the answer area.

On the servers, install the:

Log Analytics agent

Azure Connected Machine agent

Log Analytics agent

Microsoft Dependency agent

Configure custom log settings by using the:

Log Analytics workspace settings of Microsoft Sentinel

Data connectors page of Microsoft Sentinel

Log Analytics workspace settings of Microsoft Sentinel

Logs blade of Microsoft Sentinel

- 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 27

- (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
<code> project LogonFailures=count()</code>	
<code> summarize LogonFailures=count() by DeviceName, LogonType</code>	
<code> where ActionType == FailureReason</code>	
<code> where DeviceName in ("CFOLaptop", "CEOLaptop", "COOLaptop")</code>	
<code>ActionType == "LogonFailed"</code>	
<code>ActionType == FailureReason</code>	
<code>DeviceEvents</code>	
<code>DeviceLogonEvents</code>	

- A. Mastered

B. Not Mastered

Answer: A

Explanation:

Values

| project LogonFailures=count()

| summarize LogonFailures=count()
by DeviceName, LogonType

| where ActionType == FailureReason

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

ActionType == "LogonFailed"

ActionType == FailureReason

DeviceEvents

DeviceLogonEvents

Answer Area

DeviceLogonEvents

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

ActionType == FailureReason

| summarize LogonFailures=count()
by DeviceName, LogonType

NEW QUESTION 31

- (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 34

- (Exam Topic 3)

You are responsible for responding to Azure Defender for Key Vault alerts.

During an investigation of an alert, you discover unauthorized attempts to access a key vault from a Tor exit node.

What should you configure to mitigate the threat?

- A. Key Vault firewalls and virtual networks
- B. Azure Active Directory (Azure AD) permissions
- C. role-based access control (RBAC) for the key vault
- D. the access policy settings of the key vault

Answer: A

Explanation:

Reference:

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

NEW QUESTION 39

- (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

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.

Answer Area

<

>

↑

↓

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Reference:

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

NEW QUESTION 40

- (Exam Topic 3)

You are informed of a new common vulnerabilities and exposures (CVE) vulnerability that affects your environment.

You need to use Microsoft Defender Security Center to request remediation from the team responsible for the affected systems if there is a documented active exploit available.

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 Device Inventory, search for the CVE.

Open the Threat Protection report.

From Threat & Vulnerability Management, select **Weaknesses**, and search for the CVE.

From Advanced hunting, search for cveId in the DeviceTvmSoftwareInventoryVulnerabilitites table.

Create the remediation request.

Select **Security recommendations**.

Answer Area

<

>

↑

↓

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Reference:

<https://techcommunity.microsoft.com/t5/core-infrastructure-and-security/microsoft-defender-atp-remediate-apps>

NEW QUESTION 43

- (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 48

- (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 52

- (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 53

- (Exam Topic 3)

You have an Azure subscription that has Azure Defender enabled for all supported resource types.

You need to configure the continuous export of high-severity alerts to enable their retrieval from a third-party security information and event management (SIEM) solution.

To which service should you export the alerts?

- A. Azure Cosmos DB
- B. Azure Event Grid
- C. Azure Event Hubs
- D. Azure Data Lake

Answer: C

Explanation:

Reference: <https://docs.microsoft.com/en-us/azure/security-center/continuous-export?tabs=azure-portal>

NEW QUESTION 58

- (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 61

- (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 63

- (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 66

- (Exam Topic 3)

Your company has an on-premises network that uses Microsoft Defender for Identity.

The Microsoft Secure Score for the company includes a security assessment associated with unsecure Kerberos delegation.

You need remediate the security risk. What should you do?

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

Answer: B

Explanation:

To remediate the security risk associated with unsecure Kerberos delegation, you should modify the properties of the computer objects listed as exposed entities. Specifically, you should set the Kerberos delegation settings to either 'Trust this computer for delegation to any service' or 'Trust this computer for delegation to specified services only'. This will ensure that the computer is not allowed to use Kerberos delegation to access other computers on the network.

Reference: <https://docs.microsoft.com/en-us/windows/security/identity-protection/microsoft-defender-for-iden>

NEW QUESTION 71

- (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 each account as a Sensitive account. Does this meet the goal?

- A. Yes
- B. No

Answer: B

Explanation:

Reference:

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

NEW QUESTION 73

- (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.

➤

➤

Answer Area

1

2

3

⬆

⬇

- 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 74

- (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 76

- (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 80

- (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 82

- (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 85

- (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 90

- (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 94

- (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 99

- (Exam Topic 3)

You have an Azure Sentinel deployment in the East US Azure region.

You create a Log Analytics workspace named LogsWest in the West US Azure region.

You need to ensure that you can use scheduled analytics rules in the existing Azure Sentinel deployment to generate alerts based on queries to LogsWest.

What should you do first?

A. Deploy Azure Data Catalog to the West US Azure region.

B. Modify the workspace settings of the existing Azure Sentinel deployment

C. Add Microsoft Sentinel to a workspace.

D. Create a data connector in Azure Sentinel.

Answer: C

Explanation:

Reference:

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

NEW QUESTION 102

- (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 Mitigate the threat section.

Does this meet the goal?

A. Yes

B. No

Answer: A

Explanation:

Reference:

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

NEW QUESTION 107

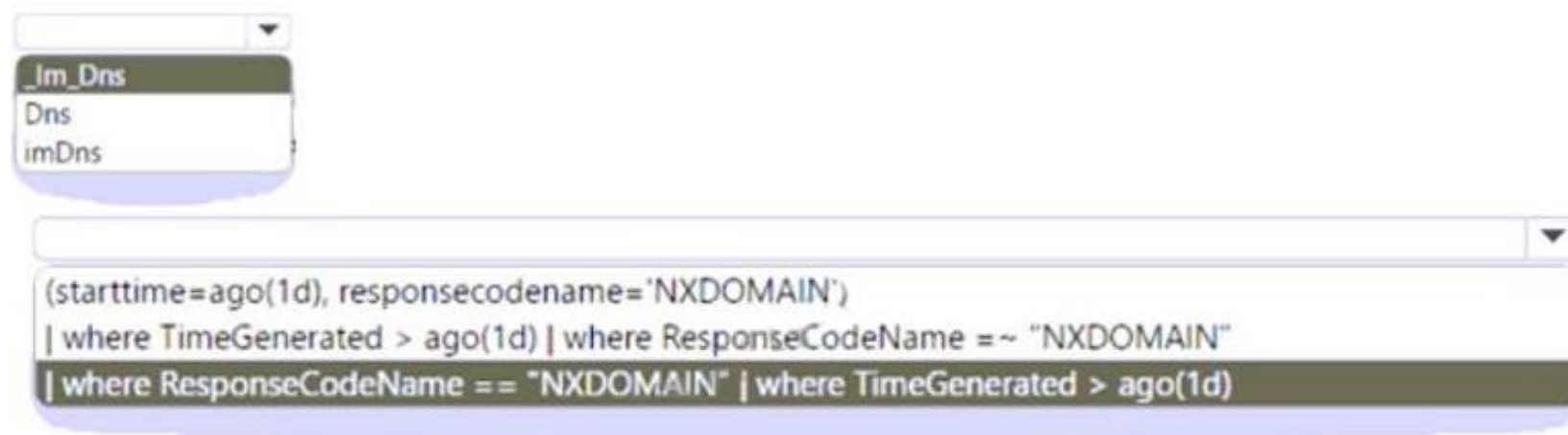
- (Exam Topic 3)

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:

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 108

- (Exam Topic 3)

You deploy Azure Sentinel.

You need to implement connectors in Azure Sentinel to monitor Microsoft Teams and Linux virtual machines in Azure. The solution must minimize administrative effort.

Which data connector type should you use for each workload? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Microsoft Teams:

Custom

Office 365

Security Events

Syslog

Linux virtual machines in Azure:

Custom

Office 365

Security Events

Syslog

- A. Mastered
B. Not Mastered

Answer: A

Explanation:

Graphical user interface, text, application Description automatically generated

Reference:

<https://docs.microsoft.com/en-us/azure/sentinel/connect-office-365> <https://docs.microsoft.com/en-us/azure/sentinel/connect-syslog>

NEW QUESTION 110

- (Exam Topic 3)

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

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

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

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

Solution: You manually install the Log Analytics agent on the virtual machines. Does this meet the goal?

- A. Yes
B. No

Answer: B

Explanation:

Reference:

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

NEW QUESTION 112

- (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 117

- (Exam Topic 3)
You have a Microsoft 365 subscription that has Microsoft 365 Defender enabled.
You need to identify all the changes made to sensitivity labels during the past seven days. What should you use?

- A. the Incidents blade of the Microsoft 365 Defender portal
- B. the Alerts settings on the Data Loss Prevention blade of the Microsoft 365 compliance center
- C. Activity explorer in the Microsoft 365 compliance center
- D. the Explorer settings on the Email & collaboration blade of the Microsoft 365 Defender portal

Answer: C

Explanation:
Labeling activities are available in Activity explorer. For example:
Sensitivity label applied
This event is generated each time an unlabeled document is labeled or an email is sent with a sensitivity label. It is captured at the time of save in Office native applications and web applications.
It is captured at the time of occurrence in Azure Information protection add-ins.
Upgrade and downgrade labels actions can also be monitored via the Label event type field and filter. Reference:
<https://docs.microsoft.com/en-us/microsoft-365/compliance/data-classification-activity-explorer-available-event>

NEW QUESTION 122

- (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 127

- (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 131

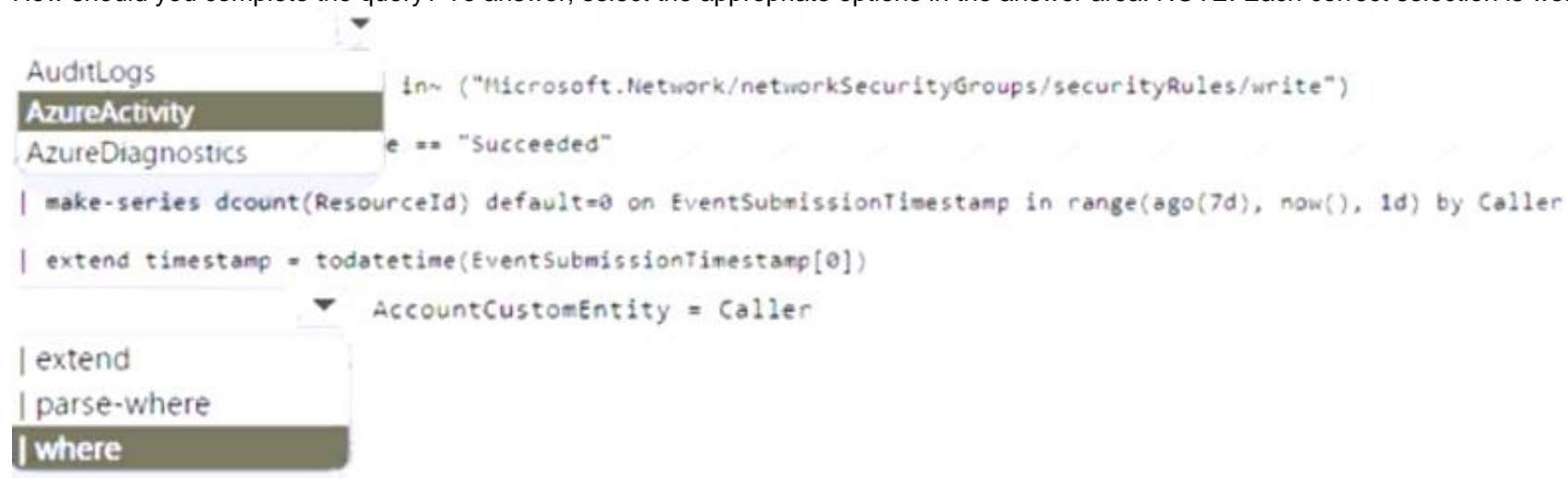
- (Exam Topic 3)

You have an Azure subscription that contains an Microsoft Sentinel workspace.

You need to create a hunting query using Kusto Query Language (KQL) that meets the following requirements:

- Identifies an anomalous number of changes to the rules of a network security group (NSG) made by the same security principal
- Automatically associates the security principal with an Microsoft Sentinel entity

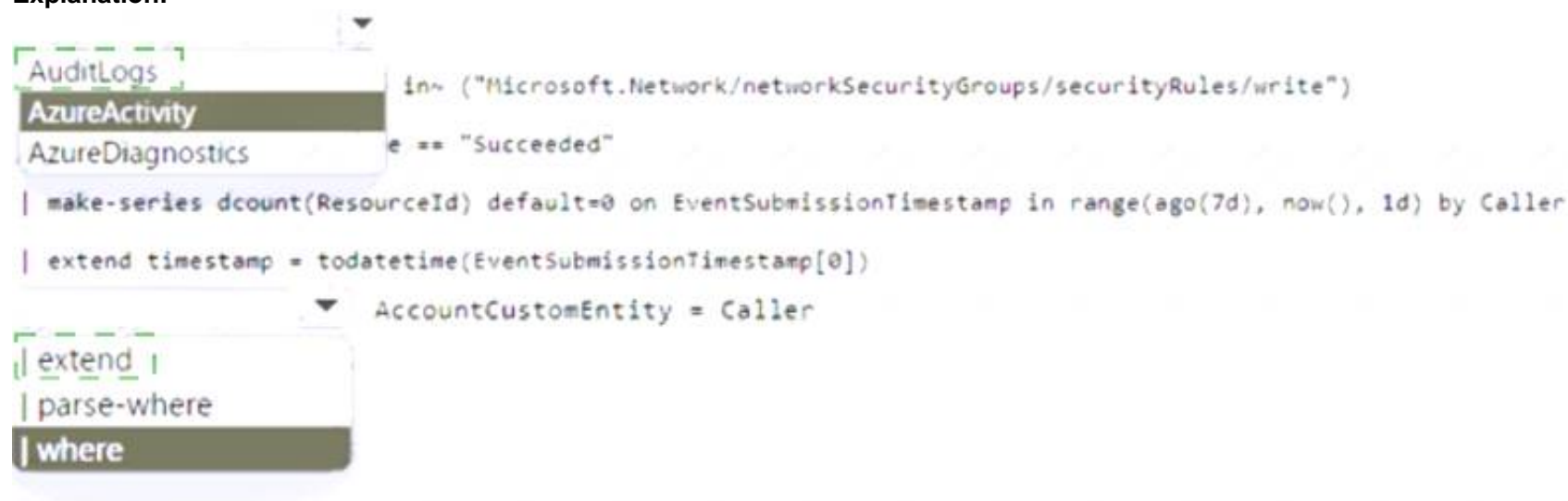
How should you complete the query? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.



- A. Mastered
- B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 132

- (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 134

- (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 136

- (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 141

- (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 144

- (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 149

.....

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](#)