

Exam Questions SC-200

Microsoft Security Operations Analyst

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



NEW QUESTION 1

- (Exam Topic 1)

You need to implement Azure Sentinel queries for Contoso and Fabrikam to meet the technical requirements. What should you include in the solution? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Minimum number of Log Analytics workspaces required in the Azure subscription of Fabrikam:

0

1

2

3

Query element required to correlate data between tenants:

extend

project

workspace

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

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

NEW QUESTION 2

- (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 3

- (Exam Topic 2)

You need to add notes to the events to meet the Azure Sentinel requirements.

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

Actions

Add a bookmark and map an entity.

From Azure Monitor, run a Log Analytics query.

Add the query to favorites.

Select a query result.

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

Answer Area

⬅

➡

⬆

⬇

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Graphical user interface, text, application Description automatically generated

Reference:

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

NEW QUESTION 4

- (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 5

- (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.

Minimize costs for daily ingested data:

- ☐ Use a commitment tier.
- ☐ Apply a daily cap.
- ☒ Use a commitment tier.
- ☐ Use the Pay-As-You-Go (PAYG) model.

Maximize the data retention period without incurring extra costs:

- ☐ Set retention to 90 days.
- ☐ Set retention to 31 days.
- ☒ Set retention to 90 days.
- ☐ Set retention to 365 days.

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Minimize costs for daily ingested data:

- ☐ Use a commitment tier.
- ☐ Apply a daily cap.
- ☒ Use a commitment tier.
- ☐ Use the Pay-As-You-Go (PAYG) model.

Maximize the data retention period without incurring extra costs:

- ☐ Set retention to 90 days.
- ☐ Set retention to 31 days.
- ☒ Set retention to 90 days.
- ☐ Set retention to 365 days.

NEW QUESTION 6

- (Exam Topic 3)

You have a Microsoft subscription that has Microsoft Defender for Cloud enabled You configure the Azure logic apps shown in the following table.

Name	Trigger	Action
LogicApp1	When a Defender for Cloud recommendation is created or triggered	Send an email
LogicApp2	When a Defender for Cloud alert is created or triggered	Send an email

You need to configure an automatic action that will run if a Suspicious process executed alert is triggered. The solution must minimize administrative effort. 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

Configure the Suppress similar alerts settings.

Configure the Mitigate the threat settings.

Filter by alert title.

Select **Take action**.

Configure the Prevent future attacks settings.

Configure the Trigger automated response settings.

>

<

Answer Area

1

2

3

- A. Mastered
 B. Not Mastered

Answer: A

Explanation:

- * A. Configure the Trigger automated response settings in the Azure Security Center or Azure Logic App,
- * B. Filter by alert title (e.g. "Suspicious process executed").
- * C. Select "Take action" (e.g. "Mitigate the threat").

NEW QUESTION 7

- (Exam Topic 3)

You need to use an Azure Resource Manager template to create a workflow automation that will trigger an automatic remediation when specific security alerts are received by Azure Security Center.

How should you complete the portion of the template that will provision the required Azure resources? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

```

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

```

Microsoft.Automation

Microsoft.Logic

Microsoft.Security

Microsoft.Automation

Microsoft.Logic

Microsoft.Security

- A. Mastered
 B. Not Mastered

Answer: A

Explanation:

Graphical user interface, text, application Description automatically generated

Reference:

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

NEW QUESTION 8

- (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:

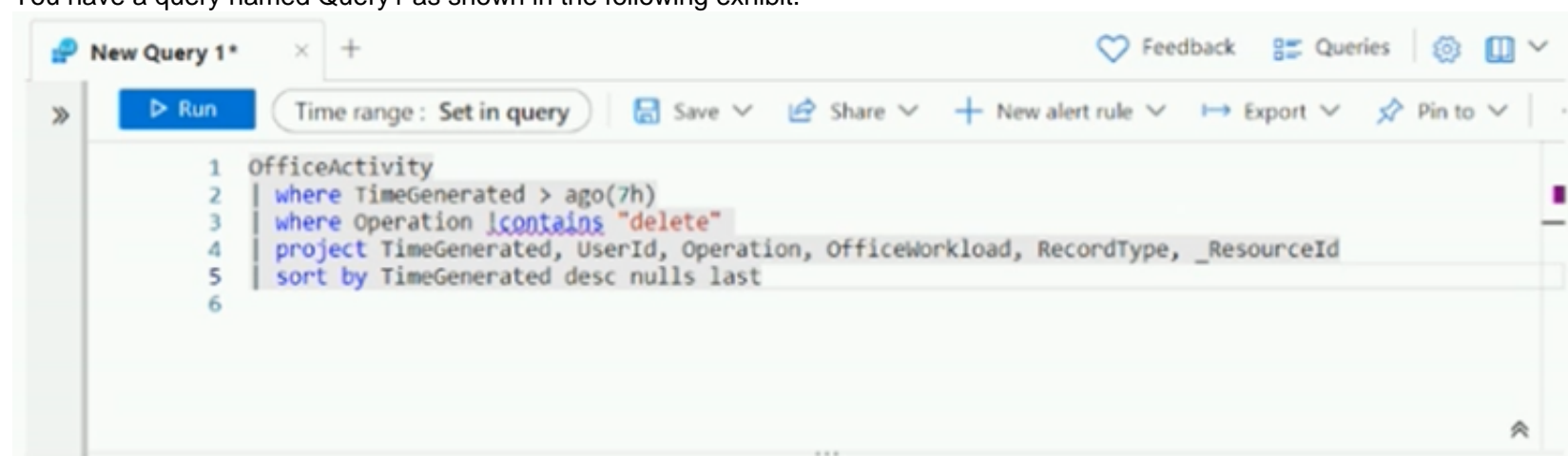
<https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/manage-alerts>

NEW QUESTION 9

- (Exam Topic 3)

You have a Microsoft Sentinel workspace.

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



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

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

Answer: C

Explanation:

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

NEW QUESTION 10

- (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 10

- (Exam Topic 3)

You are configuring Azure Sentinel.

You need to send a Microsoft Teams message to a channel whenever an incident representing a sign-in risk event is activated in Azure Sentinel.

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

NOTE: Each correct selection is worth one point.

- A. Enable Entity behavior analytics.
- B. Associate a playbook to the analytics rule that triggered the incident.
- C. Enable the Fusion rule.
- D. Add a playbook.
- E. Create a workbook.

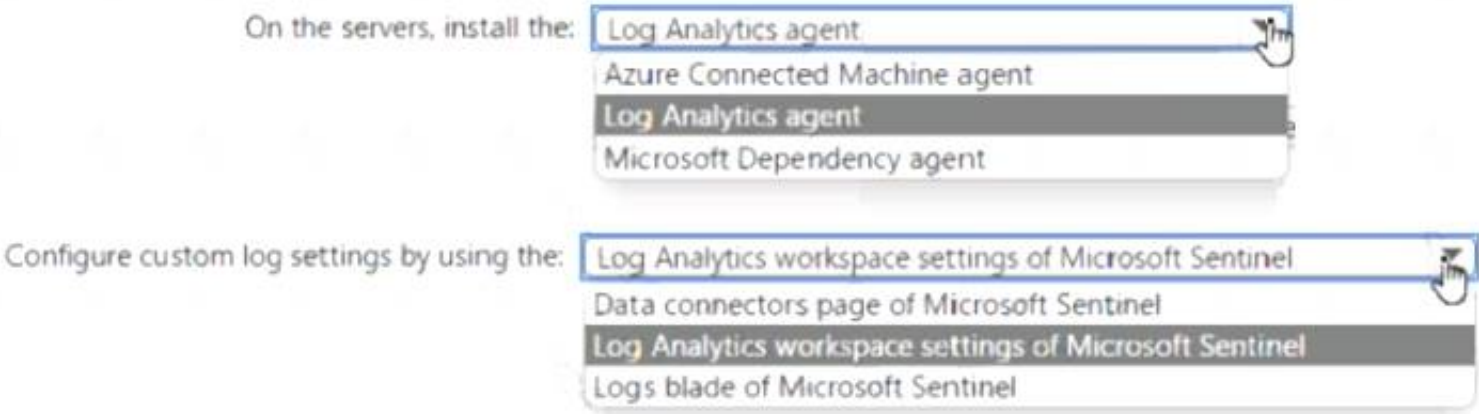
Answer: AB

Explanation:

Reference:
<https://docs.microsoft.com/en-us/azure/sentinel/enable-entity-behavior-analytics> <https://docs.microsoft.com/en-us/azure/sentinel/automate-responses-with-playbooks>

NEW QUESTION 12

- (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.



- 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 16

- (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 17

- (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.

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

```

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 18

- (Exam Topic 3)

A company wants to analyze by using Microsoft 365 Apps.

You need to describe the connected experiences the company can use.

Which connected experiences should you describe? To answer, drag the appropriate connected experiences to the correct description. Each connected experience may be used once, more than once, or not at all. You may need to drag the split between panes or scroll to view content.

NOTE: Each correct selection is worth one point.



- A. Mastered
 B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 23

- (Exam Topic 3)

You receive an alert from Azure Defender for Key Vault.

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

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

What should you do first?

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

Answer: B

Explanation:

Reference:

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

NEW QUESTION 25

- (Exam Topic 3)

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

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

You are configuring Azure Sentinel.

You need to create an incident in Azure Sentinel when a sign-in to an Azure virtual machine from a malicious IP address is detected.

Solution: You create a Microsoft incident creation rule for a data connector.

Does this meet the goal?

- A. Yes
 B. No

Answer: A

Explanation:

Reference:

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

NEW QUESTION 26

- (Exam Topic 3)

Your company deploys the following services:

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

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

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

NOTE: Each correct selection is worth one point.

- A. the Compliance Data Administrator in Azure Active Directory (Azure AD)

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

Answer: BD

Explanation:

Reference:

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

NEW QUESTION 27

- (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 32

- (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 33

- (Exam Topic 3)

You need to create a query for a workbook. The query must meet the following requirements:

- > List all incidents by incident number.
- > Only include the most recent log for each incident.

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

NOTE: Each correct selection is worth one point.

SecurityIncident

project	arg_max	(LasModifiedTime,*) by IncidentNumber
sort	limit	
summarize	top	

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Graphical user interface Description automatically generated

Reference:

<https://www.drware.com/whats-new-soc-operational-metrics-now-available-in-sentinel/>

NEW QUESTION 37

- (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 42

- (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 (
    | 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 47

- (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 51

- (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		Answer Area	
From the Data controller settings in the Azure portal, create an Azure Arc data controller.	<div> <div>></div> <div><</div> </div>	1	<div> <div>↑</div> <div>↓</div> </div>
On the on-premises servers, install the Azure Monitor agent.		2	
From the Add servers with Azure Arc settings in the Azure portal, generate an installation script.		3	
On the on-premises servers, install the Azure Connected Machine agent.			
On the on-premises servers, install the Log Analytics agent.			

- 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 54

- (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 56

- (Exam Topic 3)

You have an Azure subscription that has Azure Defender enabled for all supported resource types. You create an Azure logic app named LA1.

You plan to use LA1 to automatically remediate security risks detected in Defenders for Cloud. You need to test LA1 in Defender for Cloud.

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

NOTE: Each correct selection is worth one point.

Set the LA1 trigger to:

- When a Defender for Cloud Recommendation is created or triggered
- When a Defender for Cloud Recommendation is created or triggered
- When a Defender for Cloud Alert is created or triggered
- When a response to a Defender for Cloud alert is triggered

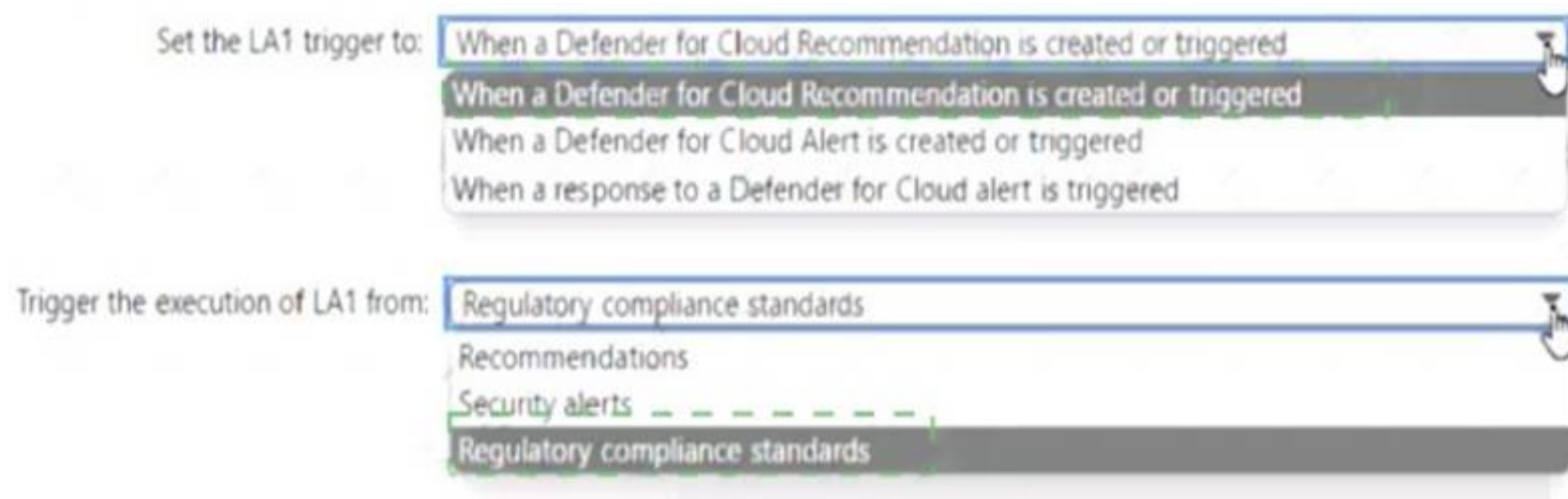
Trigger the execution of LA1 from:

- Regulatory compliance standards
- Recommendations
- Security alerts
- Regulatory compliance standards

- A. Mastered
 B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 58

- (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 63

- (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 67

- (Exam Topic 3)

Your company uses Azure Security Center and Azure Defender.

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

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

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

Answer: C

Explanation:

Reference:

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

NEW QUESTION 70

- (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:

<input type="checkbox"/> Turn on endpoint detection and response (EDR) in block mode <input type="checkbox"/> Turn on Live Response <input type="checkbox"/> Turn off Tamper Protection

To configure the devices:

<input type="checkbox"/> Add a network assessment job <input type="checkbox"/> Create a device group that contains the devices and set Automation level to Full <input type="checkbox"/> 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 75

- (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 76

- (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 77

- (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 80

- (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 83

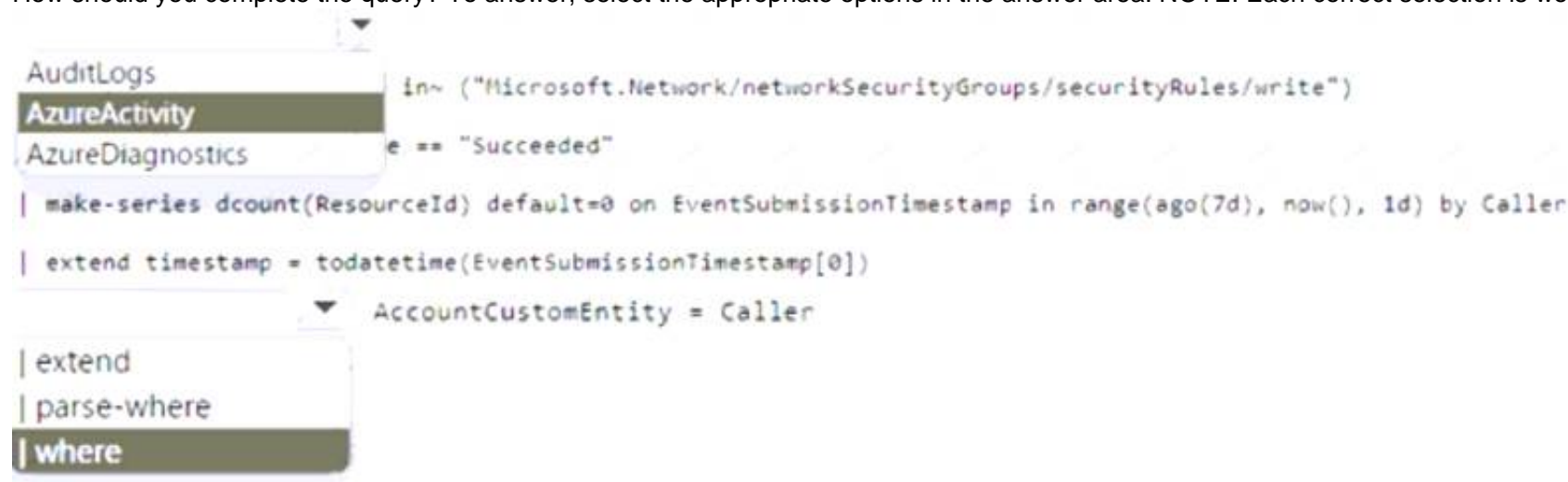
- (Exam Topic 3)

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

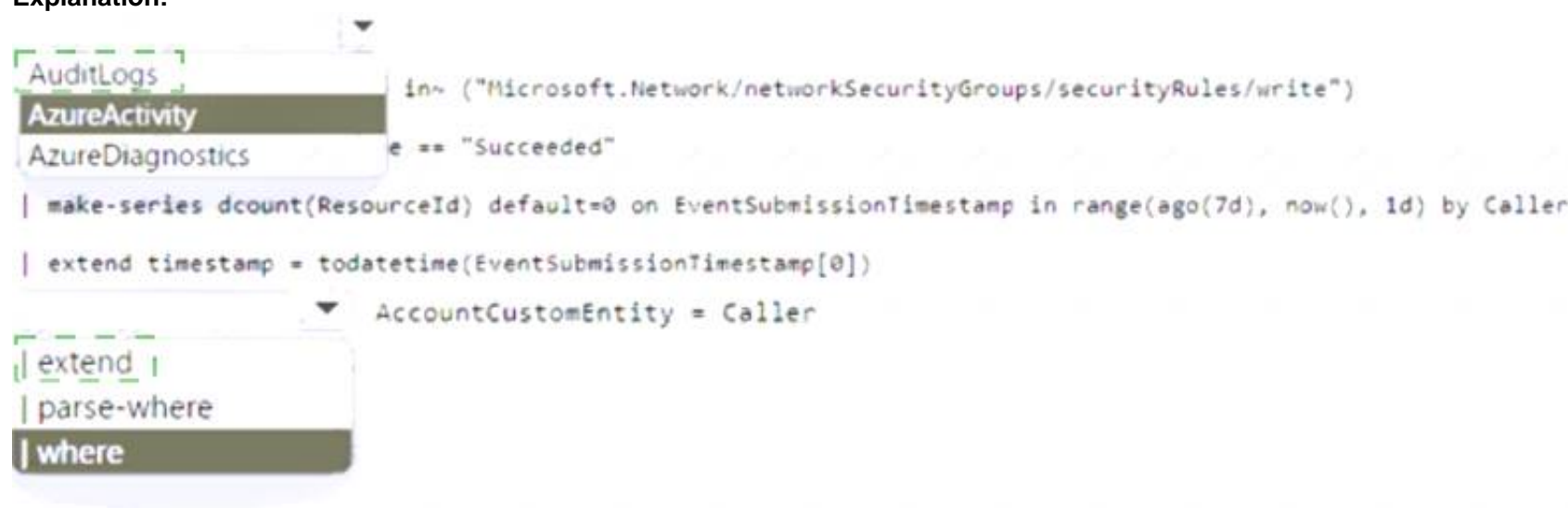
How should you complete the query? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.



- A. Mastered
- B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 85

.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

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

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

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

Money Back Guarantee

SC-200 Practice Exam Features:

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