

Exam Questions SC-200

Microsoft Security Operations Analyst

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



NEW QUESTION 1

HOTSPOT - (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:

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

	▼
0	<input checked="" type="checkbox"/>
1	<input type="checkbox"/>
2	<input type="checkbox"/>
3	<input type="checkbox"/>

Query element required to correlate data between tenants:

	▼
extend	
project	
workspace	<input checked="" type="checkbox"/>

NEW QUESTION 2

HOTSPOT - (Topic 1)

You need to create an advanced hunting query to investigate the executive team issue.

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

NOTE: Each correct selection is worth one point.

	▼
CloudAppEvents	
DeviceFileEvents	
DeviceProcessEvents	

| where TimeStamp > ago(2d)

| summarize activityCount =

ActionType, AccountDisplayName

| where activityCount > 5

	▼
avg()	
count()	
sum()	

by FolderPath, FileName,

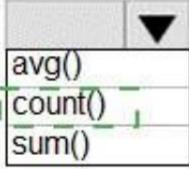
- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

```

| where TimeStamp > ago(2d)

| summarize activityCount =  by FolderPath, FileName,
ActionType, AccountDisplayName

| where activityCount > 5
    
```

NEW QUESTION 3

- (Topic 1)
 The issue for which team can be resolved by using Microsoft Defender for Office 365?

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

Answer: B

Explanation:

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

NEW QUESTION 4

- (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 5

- (Topic 1)
 The issue for which team can be resolved by using Microsoft Defender for Endpoint?

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

Answer: B

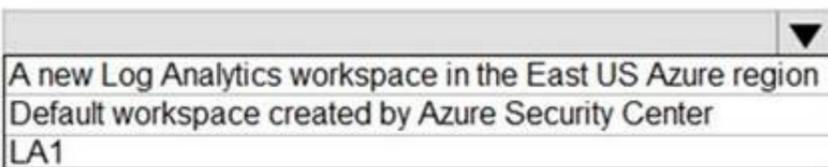
Explanation:

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

NEW QUESTION 6

HOTSPOT - (Topic 2)
 You need to implement Microsoft Defender for Cloud to meet the Microsoft Defender for Cloud 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.

Answer Area

Log Analytics workspace to use: 

Windows security events to collect: 

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

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

NEW QUESTION 7

HOTSPOT - (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:

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

NEW QUESTION 8

- (Topic 2)

You need to modify the anomaly detection policy settings to meet the Microsoft Defender for Cloud Apps requirements and resolve the reported problem. Which policy should you modify?

- A. Activity from suspicious IP addresses
- B. Risky sign-in
- C. Activity from anonymous IP addresses
- D. Impossible travel

Answer: D

NEW QUESTION 9

HOTSPOT - (Topic 2)

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

NOTE: Each correct selection is worth one point.

In the Cloud App Security portal:

▼
Add a security extension
Configure app connectors
Configure log collectors

From Azure Sentinel in the Azure portal:

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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

In the Cloud App Security portal:

▼
Add a security extension
Configure app connectors
Configure log collectors

From Azure Sentinel in the Azure portal:

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

NEW QUESTION 10

- (Topic 2)

Which rule setting should you configure to meet the Microsoft Sentinel requirements?

- A. From Set rule logic, turn off suppression.
- B. From Analytic rule details, configure the tactics.
- C. From Set rule logic, map the entities.
- D. From Analytic rule details, configure the severity.

Answer: C

NEW QUESTION 10

- (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 14

- (Topic 2)

You need to create the test rule to meet the Azure Sentinel requirements. What should you do when you create the rule?

- A. From Set rule logic, turn off suppression.
- B. From Analytics rule details, configure the tactics.
- C. From Set rule logic, map the entities.
- D. From Analytics rule details, configure the severity.

Answer: C

Explanation:

Reference:

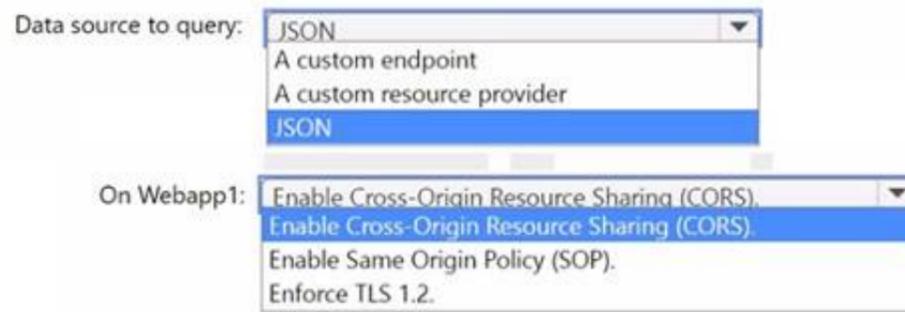
<https://docs.microsoft.com/en-us/azure/sentinel/tutorial-detect-threats-custom>

NEW QUESTION 18

HOTSPOT - (Topic 3)

You need to implement the query for Workbook1 and Webapp1. The solution must meet the Microsoft Sentinel requirements. How should you configure the query? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Answer Area

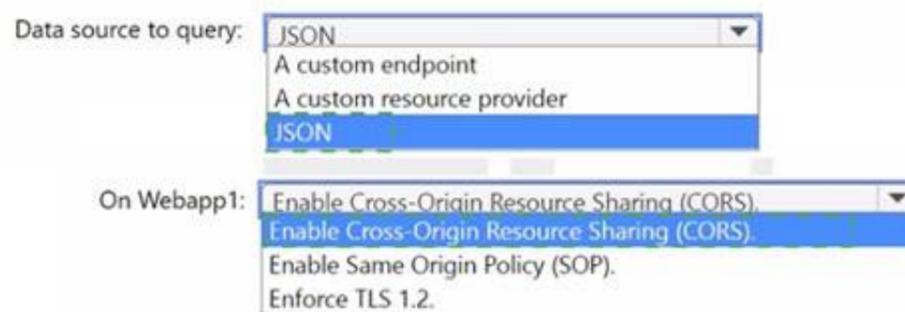


- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area



NEW QUESTION 19

- (Topic 3)

You need to configure event monitoring for Server1. The solution must meet the Microsoft Sentinel requirements. What should you create first?

- A. a Microsoft Sentinel automation rule
- B. a Microsoft Sentinel scheduled query rule
- C. a Data Collection Rule (DCR)
- D. an Azure Event Grid topic

Answer: C

NEW QUESTION 21

- (Topic 3)

You need to ensure that the Group1 members can meet the Microsoft Sentinel requirements. Which role should you assign to Group1?

- A. Microsoft Sentinel Automation Contributor
- B. Logic App Contributor
- C. Automation Operator
- D. Microsoft Sentinel Playbook Operator

Answer: D

NEW QUESTION 25

HOTSPOT - (Topic 3)

You need to implement the Microsoft Sentinel NRT rule for monitoring the designated break glass account. The solution must meet the Microsoft Sentinel requirements.

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



- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area



NEW QUESTION 29

- (Topic 3)

You need to implement the Defender for Cloud requirements. What should you configure for Server2?

- A. the Microsoft Antimalware extension
- B. an Azure resource lock
- C. an Azure resource tag
- D. the Azure Automanage machine configuration extension for Windows

Answer: D

NEW QUESTION 34

HOTSPOT - (Topic 3)

You need to implement the ASIM query for DNS requests. The solution must meet the Microsoft Sentinel requirements. How should you configure the query? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Answer Area

ASIM parser:

Filter:

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

ASIM parser:

Filter:

NEW QUESTION 39

HOTSPOT - (Topic 3)

You need to monitor the password resets. The solution must meet the Microsoft 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



- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area



NEW QUESTION 40

- (Topic 4)

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

- (Topic 4)

Your company uses Azure Sentinel.

A new security analyst reports that she cannot assign and dismiss incidents in Azure Sentinel. You need to resolve the issue for the analyst. The solution must use the principle of least privilege. Which role should you assign to the analyst?

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

Answer: A

Explanation:

Reference:

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

NEW QUESTION 47

- (Topic 4)

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 51

DRAG DROP - (Topic 4)

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

- 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.

Answer area

⏪
⏩

⏴
⏵

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Actions

- 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.

Answer area

Select Security policy.

Select Suppression rules, and then select Create new suppression rule.

Select Azure Resource as the entity type and specify the ID.

⏪
⏩

⏴
⏵

NEW QUESTION 53

HOTSPOT - (Topic 4)

You have a Microsoft 365 subscription that uses Microsoft 365 Defender and contains a user named User1.

You are notified that the account of User1 is compromised.

You need to review the alerts triggered on the devices to which User1 signed in.

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

NOTE: Each correct selection is worth one point.

DeviceInfo

```
| where LoggedOnUsers contains 'user1'
| distinct DeviceId
| [dropdown] kind=inner AlertEvidence on DeviceId
| [dropdown]
| project AlertId
| join AlertInfo on AlertId
| [dropdown] AlertId, Timestamp, Title, Severity, Category
| [dropdown]
```

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Box 1: join An inner join.

This query uses kind=inner to specify an inner-join, which prevents deduplication of left side values for DeviceId.

This query uses the DeviceInfo table to check if a potentially compromised user (<account- name>) has logged on to any devices and then lists the alerts that have been triggered on those devices.

DeviceInfo

//Query for devices that the potentially compromised account has logged onto

| where LoggedOnUsers contains '<account-name>'

| distinct DeviceId

//Crosscheck devices against alert records in AlertEvidence and AlertInfo tables

| join kind=inner AlertEvidence on DeviceId

| project AlertId

//List all alerts on devices that user has logged on to

| join AlertInfo on AlertId

| project AlertId, Timestamp, Title, Severity, Category

DeviceInfo LoggedOnUsers AlertEvidence "project AlertID" Box 2: project

NEW QUESTION 56

HOTSPOT - (Topic 4)

You have the following SQL query.

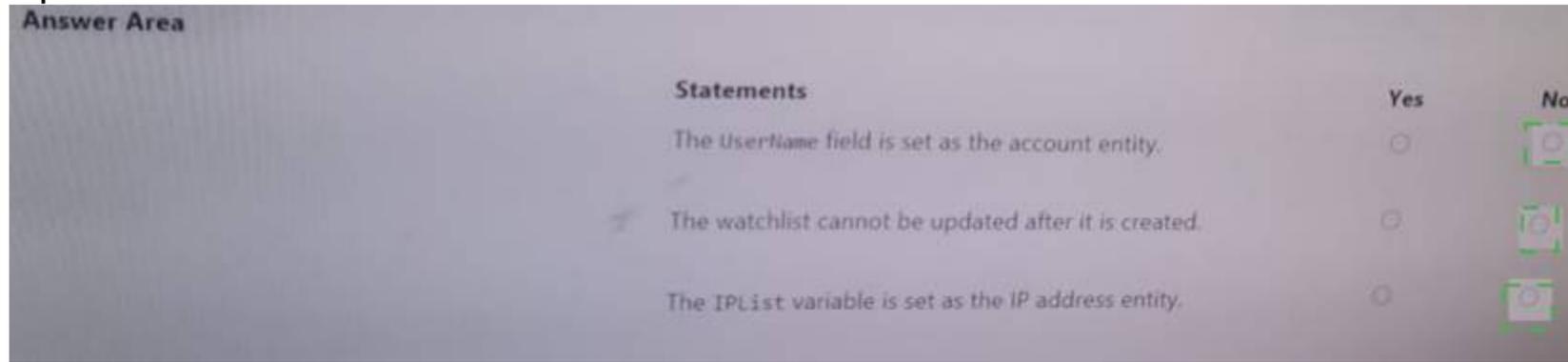
```
let IPList = _GetWatchlist('Bad_IPs');
Event
| where Source == "Microsoft-Windows-Sysmon"
| where EventID == 3
| extend EvData = parse_xml(EventData)
| extend EventDetail = EvData.DataItem.EventData.Data
| extend SourceIP = EventDetail.[9].["#text"], DestinationIP = EventDetail.[14].["#text"]
| where SourceIP in (IPList) or DestinationIP in (IPList)
| extend IPMatch = case( SourceIP in (IPList), "SourceIP", DestinationIP in (IPList), "DestinationIP", "None")
| extend timestamp = TimeGenerated, AccountCustomEntity = Username, HostCustomEntity = Computer, '
```

Answer Area

Statements	Yes	No
The Username field is set as the account entity.	<input type="radio"/>	<input 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:**NEW QUESTION 61**

- (Topic 4)

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: A

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 65

- (Topic 4)

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 livestream from a query. 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 69

- (Topic 4)

You have a Microsoft Sentinel workspace named Workspace1 and 200 custom Advanced Security Information Model (ASIM) parsers based on the DNS schema. You need to make the 200 parsers available in Workspace1. The solution must minimize administrative effort. What should you do first?

- A. Copy the parsers to the Azure Monitor Logs page.
- B. Create a JSON file based on the DNS template.
- C. Create an XML file based on the DNS template.
- D. Create a YAML file based on the DNS template.

Answer: A

NEW QUESTION 70

- (Topic 4)

You have a Microsoft Sentinel workspace that has user and Entity Behavior Analytics (UEBA) enabled for Signin Logs.

You need to ensure that failed interactive sign-ins are detected. The solution must minimize administrative effort.

What should you use?

- A. a scheduled alert query
- B. a UEBA activity template
- C. the Activity Log data connector
- D. a hunting query

Answer: B

NEW QUESTION 74

HOTSPOT - (Topic 4)

You have a Microsoft Sentinel workspace that contains a custom workbook.

You need to query the number of daily security alerts. The solution must meet the following requirements:

- Identify alerts that occurred during the last 30 days.
- Display the results in a timechart.

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

```
SecurityAlert
| where TimeGenerated >= ago(30d)
| count() by ProviderName, (TimeGenerated, 1d)
| render timechart
```

Dropdown 1: lookup, project, summarize

Dropdown 2: bin, make series, range

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

```
SecurityAlert
| where TimeGenerated >= ago(30d)
| count() by ProviderName, (TimeGenerated, 1d)
| render timechart
```

Dropdown 1: lookup, project, summarize

Dropdown 2: bin, make series, range

NEW QUESTION 78

HOTSPOT - (Topic 4)

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 Azure Security Center.

View the window

You need to test LA1 in Security Center.

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

Answer Area

Set the LA1 trigger to:

- When an Azure Security Center Recommendation is created or triggered
- When an Azure Security Center Alert is created or triggered
- When a response to an Azure Security Center alert is triggered

Trigger the execution of LA1 from:

- Recommendations
- Workflow automation

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

Set the LA1 trigger to:

When an Azure Security Center Recommendation is created or triggered
When an Azure Security Center Alert is created or triggered
When a response to an Azure Security Center alert is triggered

Trigger the execution of LA1 from:

Recommendations
Workflow automation

NEW QUESTION 82

HOTSPOT - (Topic 4)

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

```

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

```

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

```

NEW QUESTION 84

- (Topic 4)

You have an Azure subscription that uses Microsoft Defender for Cloud and contains a resource group named RG1. RG1. You need to configure just in time (JIT) VM access for the virtual machines in RG1. The solution must meet the following

- Limit the maximum request time to two hours.
- Limit protocol access to Remote Desktop Protocol (RDP) only.
- Minimize administrative effort. What should you use?

- A. Azure AD Privileged Identity Management (PIM)
- B. Azure Policy
- C. Azure Front Door
- D. Azure Bastion

Answer: A

NEW QUESTION 87

- (Topic 4)

You have a Microsoft 365 subscription that uses Microsoft 365 Defender. You plan to create a hunting query from Microsoft Defender. You need to create a custom tracked query that will be used to assess the threat status of the subscription. From the Microsoft 365 Defender portal, which page should you use to create the query?

- A. Policies & rules
- B. Explorer
- C. Threat analytics
- D. Advanced Hunting

Answer: D

NEW QUESTION 88

- (Topic 4)

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 89

DRAG DROP - (Topic 4)

You have an Azure subscription.

You need to delegate permissions to meet the following requirements:

- Enable and disable advanced features of Microsoft Defender for Cloud.
- Apply security recommendations to a resource. The solution must use the principle of least privilege.

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

NOTE: Each correct selection is worth one point.

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

NEW QUESTION 90

- (Topic 4)

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 Microsoft Defender for Cloud.
- C. Create a Microsoft Cloud App Security connector.
- D. Create an Azure AD Identity Protection connector.

Answer: AB

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 94

- (Topic 4)

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 95

HOTSPOT - (Topic 4)

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.

```

in~ ("Microsoft.Network/networkSecurityGroups/securityRules/write")
| make-series dcount(ResourceId) default=0 on EventSubmissionTimestamp in range(ago(7d), now(), 1d) by Caller
| extend timestamp = todatetime(EventSubmissionTimestamp[0])
| extend AccountCustomEntity = Caller

```

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

```

in~ ("Microsoft.Network/networkSecurityGroups/securityRules/write")
| make-series dcount(ResourceId) default=0 on EventSubmissionTimestamp in range(ago(7d), now(), 1d) by Caller
| extend timestamp = todatetime(EventSubmissionTimestamp[0])
| extend AccountCustomEntity = Caller

```

NEW QUESTION 100

- (Topic 4)

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 103

HOTSPOT - (Topic 4)

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:

Microsoft Teams:

	▼
Custom	
Office 365	
Security Events	
Syslog	

Linux virtual machines in Azure:

	▼
Custom	
Office 365	
Security Events	
Syslog	

NEW QUESTION 108

- (Topic 4)

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 171.23.34.32- 171.23.34.63. 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 171.23.34.32-171.23.34.63.
- 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 range.
- E. Select Import and import the file.

Answer: D

Explanation:

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

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

NEW QUESTION 112

- (Topic 4)

Your company uses line-of-business apps that contain Microsoft Office VBA macros.

You plan to enable protection against downloading and running additional payloads from the Office VBA macros as additional child processes.

You need to identify which Office VBA macros might be affected.

Which two commands can you run to achieve the goal? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

- A. Add-MpPreference -AttackSurfaceReductionRules_Ids D4F940AB -401B -4EFC -AADC -AD5F3C50688A -AttackSurfaceReductionRules_Actions Enabled
- B. Set-MpPreference -AttackSurfaceReductionRules_Ids D4F940AB -401B -4EFC -AADC -AD5F3C50688A -AttackSurfaceReductionRules_Actions AuditMode
- C. Add-MpPreference -AttackSurfaceReductionRules_Ids D4F940AB -401B -4EFC -AADC -AD5F3C50688A -AttackSurfaceReductionRules_Actions AuditMode
- D. Set-MpPreference -AttackSurfaceReductionRules_Ids D4F940AB -401B -4EFC -AADC -AD5F3C50688A -AttackSurfaceReductionRules_Actions Enabled

- A. Option A
- B. Option B
- C. Option C
- D. Option D

Answer: BC

Explanation:

Reference:

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

NEW QUESTION 115

DRAG DROP - (Topic 4)

You are investigating an incident by using Microsoft 365 Defender.

You need to create an advanced hunting query to detect 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>	

and

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Values	Answer Area
<code> project LogonFailures=count()</code>	<code> summarize LogonFailures=count() by DeviceName, LogonType</code>
<code> summarize LogonFailures=count() by DeviceName, LogonType</code>	<code> where DeviceName in ("CFOLaptop, "CEOlaptop", "COOLaptop")</code>
<code> where ActionType == FailureReason</code>	<code> where ActionType == FailureReason</code>
<code> where DeviceName in ("CFOLaptop, "CEOlaptop", "COOLaptop")</code>	<code>ActionType == "LogonFailed"</code>
<code>ActionType == "LogonFailed"</code>	<code> project LogonFailures=count()</code>

and

NEW QUESTION 119

- (Topic 4)

You have a Microsoft Sentinel workspace.

You receive multiple alerts for failed sign in attempts to an account. You identify that the alerts are false positives.

You need to prevent additional failed sign-in alerts from being generated for the account. The solution must meet the following requirements.

- Ensure that failed sign-in alerts are generated for other accounts.
- Minimize administrative effort What should do?

- A. Create an automation rule.
- B. Create a watchlist.
- C. Modify the analytics rule.
- D. Add an activity template to the entity behavior.

Answer: A

Explanation:

An automation rule will allow you to specify which alerts should be suppressed, ensuring that failed sign-in alerts are generated for other accounts while minimizing administrative effort. To create an automation rule, navigate to the Automation Rules page in the Microsoft Sentinel workspace and configure the rule parameters to suppress the false positive alerts.

NEW QUESTION 122

- (Topic 4)

You have 50 Microsoft Sentinel workspaces.

You need to view all the incidents from all the workspaces on a single page in the Azure portal. The solution must minimize administrative effort.

Which page should you use in the Azure portal?

- A. Microsoft Sentinel - Incidents
- B. Microsoft Sentinel - Workbooks
- C. Microsoft Sentinel
- D. Log Analytics workspaces

Answer: D

NEW QUESTION 123

- (Topic 4)

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: CE

Explanation:

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

NEW QUESTION 128

- (Topic 4)

You need to identify which mean time metrics to use to meet the Microsoft Sentinel requirements. Which workbook should you use?

- A. Analytics Efficiency
- B. Security Operations Efficiency
- C. Event Analyzer
- D. Investigation insights

Answer: C

NEW QUESTION 133

- (Topic 4)

You have an existing Azure logic app that is used to block Azure Active Directory (Azure AD) users. The logic app is triggered manually.

You deploy Azure Sentinel.

You need to use the existing logic app as a playbook in Azure Sentinel. What should you do first?

- A. Add a new scheduled query rule.
- B. Add a data connector to Azure Sentinel.
- C. Configure a custom Threat Intelligence connector in Azure Sentinel.
- D. Modify the trigger in the logic app.

Answer: D

Explanation:

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

NEW QUESTION 136

- (Topic 4)

You have a Microsoft 365 E5 subscription that contains 100 Linux devices. The devices are onboarded to Microsoft Defender 365. You need to initiate the collection of investigation packages from the devices by using the Microsoft 365 Defender portal. Which response action should you use?

- A. Run antivirus scan
- B. Initiate Automated Investigation
- C. Collect investigation package
- D. Initiate Live Response Session

Answer: D

NEW QUESTION 137

- (Topic 4)

You have an Azure subscription that use Microsoft Defender for Cloud and contains a user named User1.

You need to ensure that User1 can modify Microsoft Defender for Cloud security policies. The solution must use the principle of least privilege. Which role should you assign to User1?

- A. Security operator
- B. Security Admin
- C. Owner
- D. Contributor

Answer: B

NEW QUESTION 139

- (Topic 4)

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-events?view=o365-worldwide>

NEW QUESTION 142

HOTSPOT - (Topic 4)

You manage the security posture of an Azure subscription that contains two virtual machines name vm1 and vm2.

The secure score in Azure Security Center is shown in the Security Center exhibit. (Click the Security Center tab.)



Resource exemption (preview)

Now you can exempt irrelevant resources so they do not affect your secure score. [Learn more](#)

Each security control below represents a security risk you should mitigate. Address the recommendations in each control, focusing on the controls worth the most points. To get the max score, fix all recommendations for all resources in a control. [Learn more](#)

Search recommendations:

Control status: **2 Selected** Recommendation status: **2 Selected**

Recommendation maturity: **All** Resource type: **All** Quick fix available: **All**

Contains exemptions: **All** [Reset filters](#) Group by controls: On

Controls	Potential score increase	Unhealthy resources	Resource Health
> Restrict unauthorized network access	+9% (4 points)	2 of 2 resources	
> Secure management ports	+9% (4 points)	1 of 2 resources	
> Enable encryption at rest	+9% (4 points)	2 of 2 resources	
> Remediate security configurations	+4% (2 points)	1 of 2 resources	
> Apply adaptive application control	+3% (2 points)	1 of 2 resources	
> Apply system updates Completed	+0% (0 points)	None	
> Enable endpoint protection Completed	+0% (0 points)	None	
> Remediate vulnerabilities Completed	+0% (0 points)	None	
> Implement security best practices Completed	+0% (0 points)	None	
> Enable MFA Completed	+0% (0 points)	None	
> Manage access and permissions Completed	+0% (0 points)	None	

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

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

Answer Area

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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

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

NEW QUESTION 143

DRAG DROP - (Topic 4)

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
<input type="text" value="SW1"/>	From the Syslog configuration, remove the facilities that send CEF messages. <input type="text"/>
<input type="text" value="CEF1"/>	
<input type="text" value="Server1"/>	From the Log Analytics agent, disable Syslog synchronization. <input type="text"/>
<input type="text" value="Server2"/>	

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

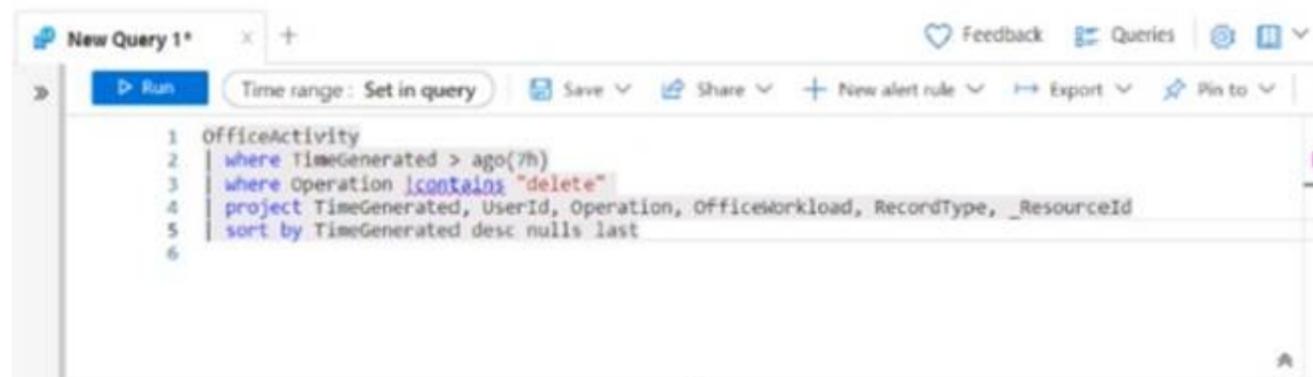
Resources	Answer Area
<input type="text" value="SW1"/>	From the Syslog configuration, remove the facilities that send CEF messages. <input type="text" value="Server1"/>
<input type="text" value="CEF1"/>	
<input type="text" value="Server1"/>	From the Log Analytics agent, disable Syslog synchronization. <input type="text" value="CEF1"/>
<input type="text" value="Server2"/>	

NEW QUESTION 146

- (Topic 4)

You have a Microsoft Sentinel workspace.

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



```
1 OfficeActivity
2 | where TimeGenerated > ago(7h)
3 | where Operation !contains "delete"
4 | project TimeGenerated, UserId, Operation, OfficeWorkload, RecordType, _ResourceId
5 | sort by TimeGenerated desc nulls last
6
```

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: A

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 151

- (Topic 4)

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 155

- (Topic 4)

You have a Microsoft Sentinel workspace that uses the Microsoft 365 Defender data connector.

From Microsoft Sentinel, you investigate a Microsoft 365 incident.

You need to update the incident to include an alert generated by Microsoft Defender for Cloud Apps.

What should you use?

- A. the entity side panel of the Timeline card in Microsoft Sentinel
- B. the investigation graph on the Incidents page of Microsoft Sentinel
- C. the Timeline tab on the Incidents page of Microsoft Sentinel
- D. the Alerts page in the Microsoft 365 Defender portal

Answer: A

NEW QUESTION 156

- (Topic 4)

You need to meet the Microsoft Sentinel requirements for App1. What should you configure for App1?

- A. an API connection
- B. a trigger
- C. an connector
- D. authorization

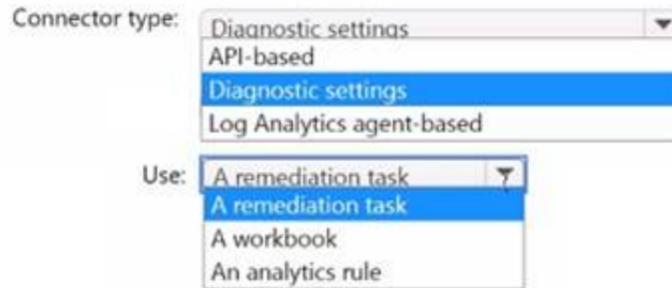
Answer: B

NEW QUESTION 159

HOTSPOT - (Topic 4)

You have four Azure subscriptions. One of the subscriptions contains a Microsoft Sentinel workspace.
 You need to deploy Microsoft Sentinel data connectors to collect data from the subscriptions by using Azure Policy. The solution must ensure that the policy will apply to new and existing resources in the subscriptions.
 Which type of connectors should you provision, and what should you use to ensure that all the resources are monitored? To answer, select the appropriate options in the answer area.
 NOTE: Each correct selection is worth one point.

Answer Area

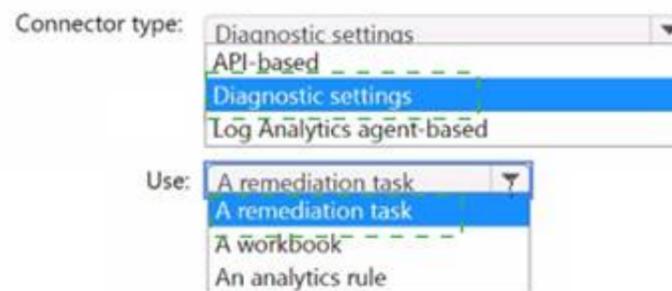


- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area



NEW QUESTION 164

HOTSPOT - (Topic 4)

You need to assign role-based access control (RBAQ roles to Group1 and Group2 to meet The Microsoft Defender for Cloud requirements and the business requirements Which role should you assign to each group? To answer, select the appropriate options in the answer area NOTE Each correct selection is worth one point.

Answer Area

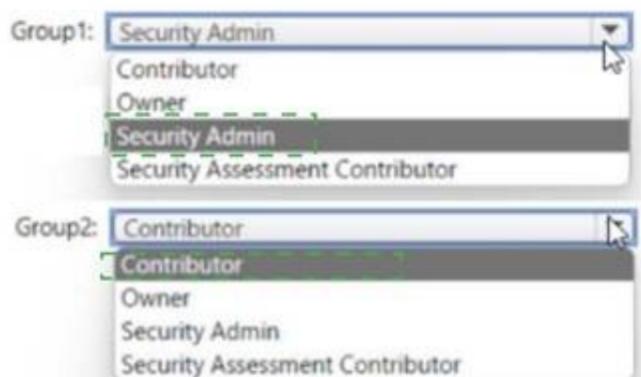


- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

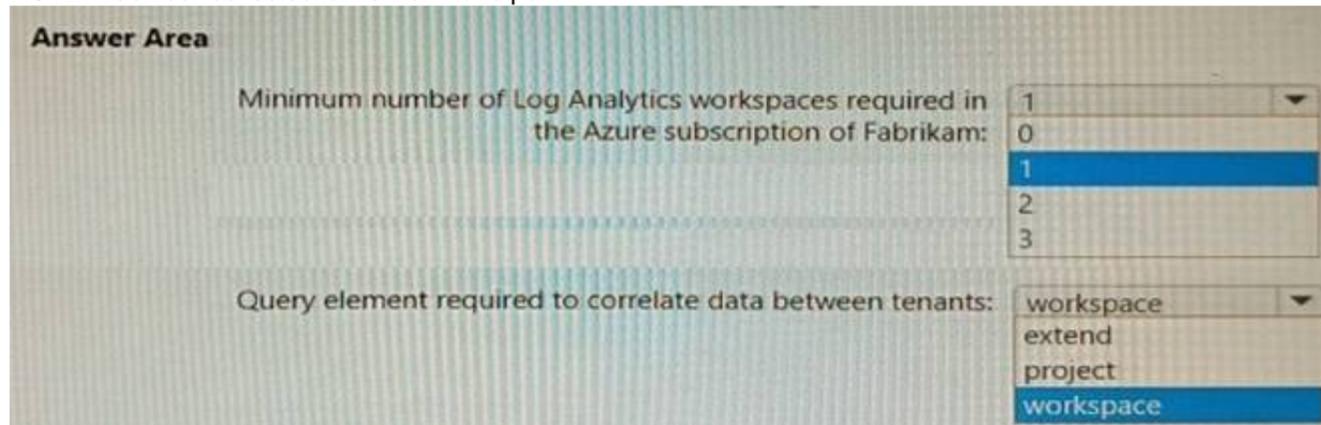


NEW QUESTION 168

HOTSPOT - (Topic 4)

You need to implement Microsoft 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.

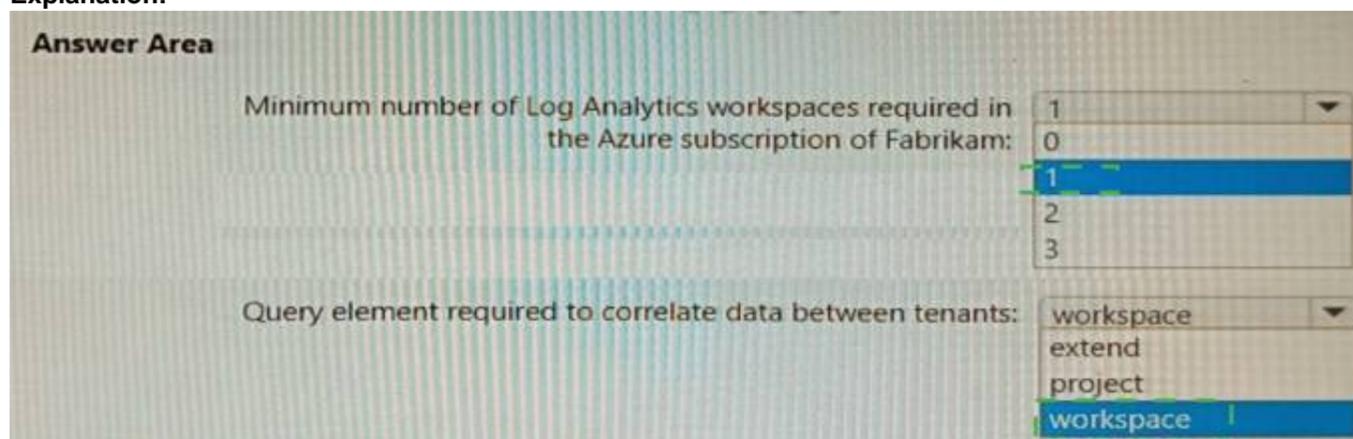
NOTE: Each correct selection is worth one point.



- A. Mastered
- B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 171

- (Topic 4)

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 176

- (Topic 4)

You have five on-premises Linux servers.

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

What should you install on the servers first?

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

Answer: B

Explanation:

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

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

* Etc.

Reference:

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

NEW QUESTION 177

- (Topic 4)

You have an Azure subscription that uses resource type for Cloud. You need to filter the security alerts view to show the following alerts:

- Unusual user accessed a key vault
- Log on from an unusual location
- Impossible travel activity Which severity should you use?

- A. Informational
- B. Low
- C. Medium
- D. High

Answer: C

NEW QUESTION 182

DRAG DROP - (Topic 4)

Your network contains an on-premises Active Directory Domain Services (AD DS) domain that syncs with an Azure AD tenant.

You have a Microsoft Sentinel workspace named Sentinel1.

You need to enable User and Entity Behavior Analytics (UEBA) for Sentinel1 and collect security events from the AD DS domain.

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 Sentinel1, collect the AD DS security events by using the Legacy Agent connector.
- For the AD DS domain, configure Windows Event Forwarding.
- For Sentinel1, configure the Windows Forwarded Events connector.
- To the AD DS domain, deploy Microsoft Defender for Identity.
- For Sentinel1, configure the Microsoft Defender for Identity connector.
- For Sentinel1, enable UEBA.

Answer Area

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Actions

- From Sentinel1, collect the AD DS security events by using the Legacy Agent connector.
- For the AD DS domain, configure Windows Event Forwarding.
- For Sentinel1, configure the Windows Forwarded Events connector.
- To the AD DS domain, deploy Microsoft Defender for Identity.
- For Sentinel1, configure the Microsoft Defender for Identity connector.
- For Sentinel1, enable UEBA.

Answer Area

To the AD DS domain, deploy Microsoft Defender for Identity.

For Sentinel1, configure the Microsoft Defender for Identity connector.

For Sentinel1, enable UEBA.

NEW QUESTION 186

HOTSPOT - (Topic 4)

Your network contains an on-premises Active Directory Domain Services (AD DS) domain that syncs with Azure AD.

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

You need to identify all the interactive authentication attempts by the users in the finance department of your company.

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

NOTE: Each correct selection is worth one point.

Answer Area

```

IdentityQueryEvents
| where Department == 'Finance'
| project-rename objid = AccountObjectId
| join

```

IdentityQueryEvents

- BehaviorAnalytics
- IdentityInfo
- IdentityQueryEvents

on \$left.objid == \$right.AccountObjectId

AuditLogs

- AuditLogs
- IdentityLogonEvents
- SigninLogs

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

```

IdentityQueryEvents
BehaviorAnalytics
IdentityInfo
IdentityQueryEvents
| where Department == 'Finance'
| project-rename objid = AccountObjectId
| join AuditLogs on $left.objid == $right.AccountObjectId
AuditLogs
IdentityLogonEvents
SigninLogs
    
```

NEW QUESTION 191

DRAG DROP - (Topic 4)

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")

ActionType == "LogonFailed"

ActionType == FailureReason

DeviceEvents

DeviceLogonEvents

and

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Values

Answer Area

| project LogonFailures=count()

| summarize LogonFailures=count()
by DeviceName, LogonType

| where ActionType == FailureReason

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

ActionType == "LogonFailed"

ActionType == FailureReason

DeviceEvents

DeviceLogonEvents

DeviceLogonEvents

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

ActionType == FailureReason

| summarize LogonFailures=count()
by DeviceName, LogonType

NEW QUESTION 192

DRAG DROP - (Topic 4)

You plan to connect an external solution that will send Common Event Format (CEF) messages to Azure Sentinel.

You need to deploy the log forwarder.

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

Actions

Answer Area

Deploy an OMS Gateway on the network.

Set the syslog daemon to forward the events directly to Azure Sentinel.

Configure the syslog daemon. Restart the syslog daemon and the Log Analytics agent.

Download and install the Log Analytics agent.

Set the Log Analytics agent to listen on port 25226 and forward the CEF messages to Azure Sentinel.



- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Actions

Answer Area

Deploy an OMS Gateway on the network.

Set the syslog daemon to forward the events directly to Azure Sentinel.

Configure the syslog daemon. Restart the syslog daemon and the Log Analytics agent.

Download and install the Log Analytics agent.

Set the Log Analytics agent to listen on port 25226 and forward the CEF messages to Azure Sentinel.



Download and install the Log Analytics agent.

Set the Log Analytics agent to listen on port 25226 and forward the CEF messages to Azure Sentinel.

Configure the syslog daemon. Restart the syslog daemon and the Log Analytics agent.

NEW QUESTION 195

DRAG DROP - (Topic 4)

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	Answer Area
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 <code>cveId</code> in the <code>DeviceTvmSoftwareInventoryVulnerabilitites</code> table.	
Create the remediation request.	
Select Security recommendations .	

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Actions	Answer Area
From Device Inventory, search for the CVE.	From Threat & Vulnerability Management, select Weaknesses , and search for the CVE.
Open the Threat Protection report.	Select Security recommendations .
From Threat & Vulnerability Management, select Weaknesses , and search for the CVE.	Create the remediation request.
From Advanced hunting, search for <code>cveId</code> in the <code>DeviceTvmSoftwareInventoryVulnerabilitites</code> table.	
Create the remediation request.	
Select Security recommendations .	

NEW QUESTION 197

- (Topic 4)

You have a Microsoft 365 subscription that uses Microsoft Purview. Your company has a project named Project1. You need to identify all the email messages that have the word Project1 in the subject line. The solution must search only the mailboxes of users that worked on Project1.
 What should you do?

- A. Create a records management disposition.
- B. Perform a user data search.
- C. Perform an audit search.
- D. Perform a content search.

Answer: D

NEW QUESTION 202

- (Topic 4)

You have an Azure subscription that contains an Microsoft Sentinel workspace. You need to create a playbook that will run automatically in response to an Microsoft Sentinel alert.
 What should you create first?

- A. a trigger in Azure Functions

- B. an Azure logic app
- C. a hunting query in Microsoft Sentinel
- D. an automation rule in Microsoft Sentinel

Answer: D

NEW QUESTION 204

DRAG DROP - (Topic 4)

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.

- 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-deployment>

NEW QUESTION 208

HOTSPOT - (Topic 4)

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:

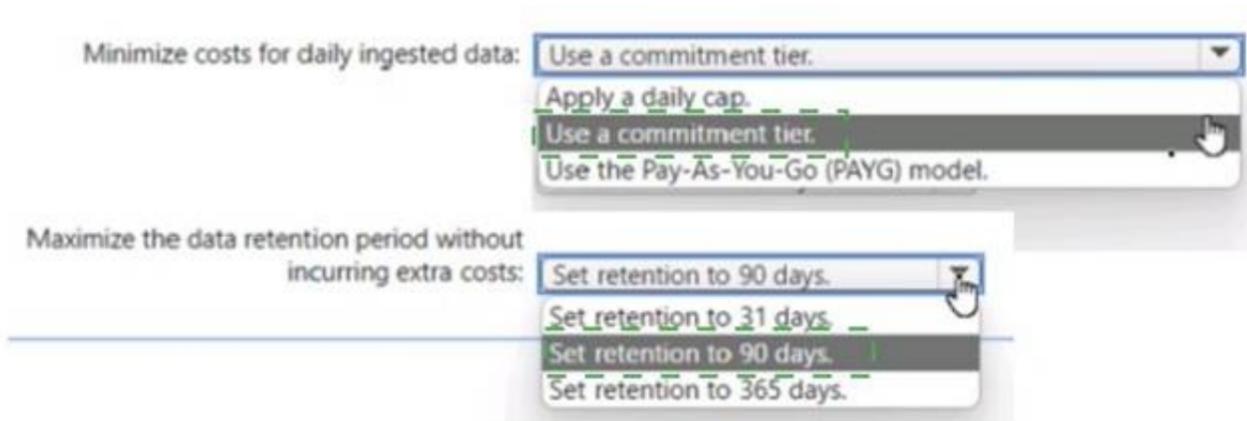
- Minimize costs for daily ingested data.
- Maximize the data retention period without incurring extra costs.

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:



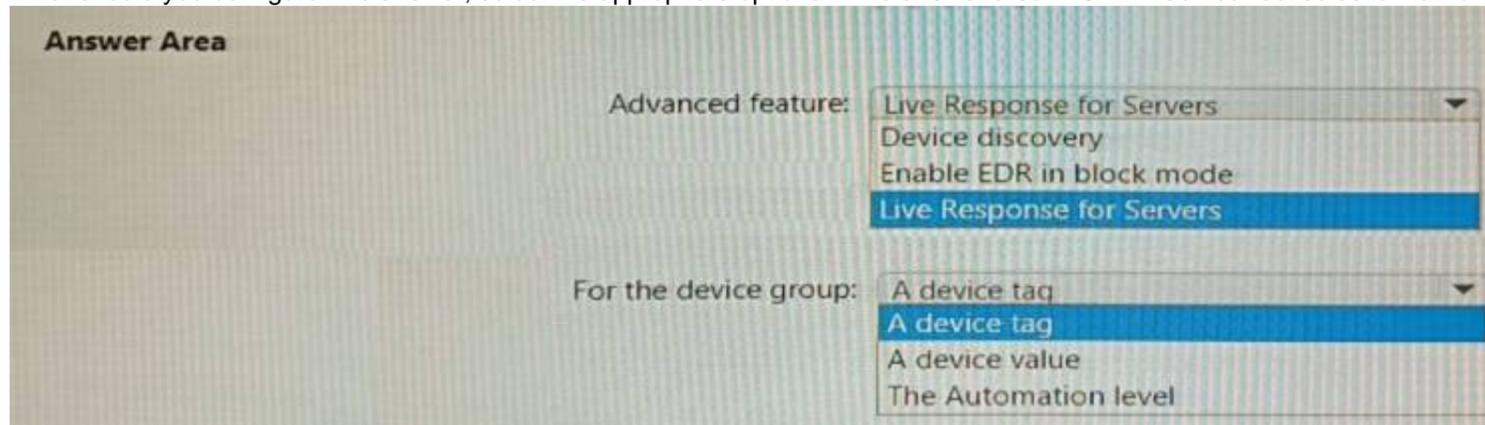
NEW QUESTION 212

HOTSPOT - (Topic 4)

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

You need to ensure that you can initiate remote shell connections to Windows servers by using the Microsoft 365 Defender portal.

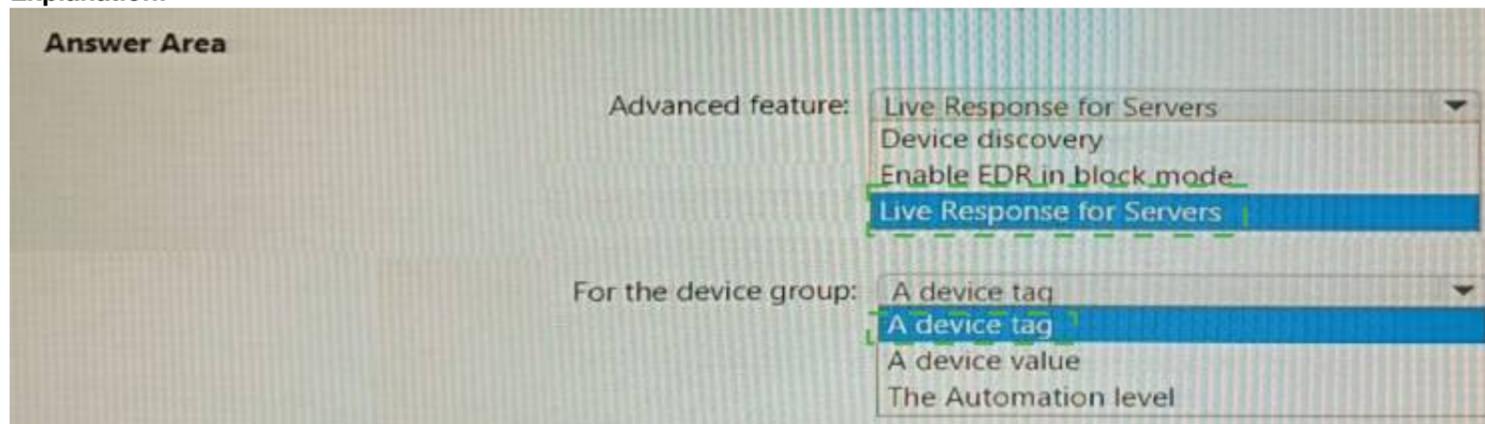
What should you configure? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.



- A. Mastered
- B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 217

- (Topic 4)

You have an Azure subscription that uses Microsoft Sentinel and contains 100 Linux virtual machines.

You need to monitor the virtual machines by using Microsoft Sentinel. The solution must meet the following requirements:

- Minimize administrative effort
 - Minimize the parsing required to read log data
- What should you configure?

- A. REST API integration
- B. a SysJog connector
- C. a Log Analytics Data Collector API
- D. a Common Event Format (CEF) connector

Answer: B

NEW QUESTION 220

- (Topic 4)

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 225

HOTSPOT - (Topic 4)

From Azure Sentinel, you open the Investigation pane for a high-severity incident as shown in the following exhibit.



Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.
 NOTE: Each correct selection is worth one point.

If you hover over the virtual machine named vm1, you can view **[answer choice]**.

- the inbound network security group (NSG) rules
- the last five Windows security log events
- the open ports on the host
- the running processes

If you select **[answer choice]**, you can navigate to the bookmarks related to the incident.

- Entities
- Info
- Insights
- Timeline

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

If you hover over the virtual machine named vm1, you can view **[answer choice]**.

- the inbound network security group (NSG) rules
- the last five Windows security log events
- the open ports on the host
- the running processes

If you select **[answer choice]**, you can navigate to the bookmarks related to the incident.

- Entities
- Info
- Insights
- Timeline

NEW QUESTION 227

- (Topic 4)

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 231

- (Topic 4)

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 234

- (Topic 4)

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

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

Answer: B

NEW QUESTION 235

- (Topic 4)

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 237

- (Topic 4)

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-center>

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

NEW QUESTION 239

HOTSPOT - (Topic 4)

You have a Microsoft Sentinel workspace.

You need to configure a report visual for a custom workbook. The solution must meet the following requirements:

- The count and usage trend of AppDisplayName must be included
- The TrendList column must be useable in a sparkline visual,

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

NOTE: Each correct selection is worth one point.

Answer Area

```

SigninLogs
| where ResultType == 0 and AppDisplayName != ""
| summarize count() by AppDisplayName
| join (
  | let
  | lookup TrendList = count() on TimeGenerated in range({TimeRange:start}, {TimeRange:end}, 4h) by AppDisplayName
  | mv-expand
)
| top 10 by count_desc
SigninLogs
| make-series TrendList = count() on TimeGenerated in range({TimeRange:start}, {TimeRange:end}, 4h) by AppDisplayName
| make_bag()
| make-series
| mv-expand
| render
) on AppDisplayName
| top 10 by count_desc
  
```

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

```

SigninLogs
| where ResultType == 0 and AppDisplayName != ""
| summarize count() by AppDisplayName
| join (
  | let
  | lookup TrendList = count() on TimeGenerated in range({TimeRange:start}, {TimeRange:end}, 4h) by AppDisplayName
  | mv-expand
)
| top 10 by count_desc
SigninLogs
| make-series TrendList = count() on TimeGenerated in range({TimeRange:start}, {TimeRange:end}, 4h) by AppDisplayName
| make_bag()
| make-series
| mv-expand
| render
) on AppDisplayName
| top 10 by count_desc
  
```

NEW QUESTION 240

- (Topic 4)

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 241

HOTSPOT - (Topic 4)

You have an Azure subscription that uses Microsoft Sentinel and contains a user named User1.

You need to ensure that User1 can enable User and Entity Behavior Analytics (UEBA) for entity behavior in Azure AD. The solution must use the principle of least privilege.

Which roles should you assign to User1? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Azure AD role: Security administrator
 Global administrator
 Identity Governance Administrator
 Security administrator
 Security operator

Azure role: Microsoft Sentinel Contributor
 Microsoft Sentinel Automation Contributor
 Microsoft Sentinel Contributor
 Security Admin
 Security Assessment Contributor

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

Azure AD role: Security administrator
 Global administrator
 Identity Governance Administrator
 Security administrator
 Security operator

Azure role: Microsoft Sentinel Contributor
 Microsoft Sentinel Automation Contributor
 Microsoft Sentinel Contributor
 Security Admin
 Security Assessment Contributor

NEW QUESTION 242

- (Topic 4)

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 246

HOTSPOT - (Topic 4)

You have a Microsoft 365 E5 subscription.

You need to create a hunting query that will return every email that contains an attachment named Document.pdf. The query must meet the following requirements:

- Only show emails sent during the last hour.
- Optimize 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.

Answer Area

EmailAttachmentInfo

```
| join DeviceFileEvents on SHA256
| join kind=inner (DeviceFileEvents | where Timestamp > ago(1h)) on SHA256
| where Timestamp > ago(1h)
| where Timestamp < ago(1h)
```

| where Subject == "Document Attachment" and FileName == "Document.pdf"

```
| join DeviceFileEvents on SHA256
| join kind=inner (DeviceFileEvents | where Timestamp > ago(1h)) on SHA256
| where Timestamp > ago(1h)
| where Timestamp < ago(1h)
```

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

EmailAttachmentInfo

```
| join DeviceFileEvents on SHA256
| join kind=inner (DeviceFileEvents | where Timestamp > ago(1h)) on SHA256
| where Timestamp > ago(1h)
| where Timestamp < ago(1h)
```

| where Subject == "Document Attachment" and FileName == "Document.pdf"

```
| join DeviceFileEvents on SHA256
| join kind=inner (DeviceFileEvents | where Timestamp > ago(1h)) on SHA256
| where Timestamp > ago(1h)
| where Timestamp < ago(1h)
```

NEW QUESTION 251

- (Topic 4)

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 252

- (Topic 4)

You have an Azure subscription that uses Microsoft Sentinel.

You need to create a custom report that will visualise sign-in information over time.

What should you create first?

- A. a workbook
- B. a hunting query
- C. a notebook
- D. a playbook

Answer: A

Explanation:

A workbook is a data-driven interactive report in Microsoft Sentinel. You can use workbooks to create custom reports based on data from your Azure subscription. Reference: <https://docs.microsoft.com/en-us/azure/sentinel/workbooks-overview>

NEW QUESTION 256

HOTSPOT - (Topic 4)

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:

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

NEW QUESTION 261

HOTSPOT - (Topic 4)

You have a Microsoft Sentinel workspace named sws1.

You plan to create an Azure logic app that will raise an incident in an on-premises IT service management system when an incident is generated in sws1.

You need to configure the Microsoft Sentinel connector credentials for the logic app. The solution must meet the following requirements:

- Minimize administrative effort.
- Use the principle of least privilege.

How should you configure the credentials? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Configure the connector to use:

A managed identity
A service principal
An Azure AD user account

Role to assign to the credentials:

Microsoft Sentinel Responder
Microsoft Sentinel Automation Contributor
Microsoft Sentinel Reader
Microsoft Sentinel Responder

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

Configure the connector to use:

- A managed identity
- A service principal
- An Azure AD user account

Role to assign to the credentials:

- Microsoft Sentinel Automation Contributor
- Microsoft Sentinel Reader
- Microsoft Sentinel Responder

NEW QUESTION 265

- (Topic 4)

You are investigating a potential attack that deploys a new ransomware strain.

You plan to perform automated actions on a group of highly valuable machines that contain sensitive information.

You have three custom device groups.

You need to be able to temporarily group the machines to perform actions on the devices. Which three actions should you perform? Each correct answer presents part of the solution. NOTE: Each correct selection is worth one point.

- A. Add a tag to the device group.
- B. Add the device users to the admin role.
- C. Add a tag to the machines.
- D. Create a new device group that has a rank of 1.
- E. Create a new admin role.
- F. Create a new device group that has a rank of 4.

Answer: ACD

Explanation:

<https://docs.microsoft.com/en-us/learn/modules/deploy-microsoft-defender-for-endpoints-environment/4-manage-access>

NEW QUESTION 266

.....

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