



## **Microsoft**

### **Exam Questions SC-200**

Microsoft Security Operations Analyst

## About ExamBible

### *Your Partner of IT Exam*

## Found in 1998

ExamBible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, ExamBible has its unique advantages that other companies could not achieve.

## Our Advances

### \* 99.9% Uptime

All examinations will be up to date.

### \* 24/7 Quality Support

We will provide service round the clock.

### \* 100% Pass Rate

Our guarantee that you will pass the exam.

### \* Unique Gurantee

If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

**NEW QUESTION 1**

- (Exam Topic 1)

You need to recommend remediation actions for the Azure Defender alerts for Fabrikam.

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

**Answer Area**

Internal threat:  ▼

- Add resource locks to the key vault.
- Modify the access policy settings for the key vault.
- Modify the role-based access control (RBAC) settings for the key vault.

External threat:  ▼

- Implement Azure Firewall.
- Modify the Key Vault firewall settings.
- Modify the network security groups (NSGs).

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

Reference:

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

**NEW QUESTION 2**

- (Exam Topic 1)

You need to recommend a solution to meet the technical requirements for the Azure virtual machines. What should you include in the recommendation?

- A. just-in-time (JIT) access
- B. Azure Defender
- C. Azure Firewall
- D. Azure Application Gateway

**Answer:** B

**Explanation:**

Reference:

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

**NEW QUESTION 3**

- (Exam Topic 1)

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

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

**Answer:** B

**Explanation:**

Reference:

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

**NEW QUESTION 4**

- (Exam Topic 2)

You need to restrict cloud apps running on CLIENT1 to meet the Microsoft Defender for Endpoint requirements.

Which two configurations should you modify? Each correct answer present part of the solution.

NOTE: Each correct selection is worth one point.

- A. the Onboarding settings from Device management in Microsoft Defender Security Center
- B. Cloud App Security anomaly detection policies
- C. Advanced features from Settings in Microsoft Defender Security Center
- D. the Cloud Discovery settings in Cloud App Security

**Answer:** CD

**Explanation:**

All Cloud App Security unsanctioned apps must be blocked on the Windows 10 computers by using Microsoft Defender for Endpoint.

Reference:

<https://docs.microsoft.com/en-us/cloud-app-security/mde-govern>

**NEW QUESTION 5**

- (Exam Topic 2)

You need to configure DC1 to meet the business requirements.

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

**Actions**

**Answer Area**

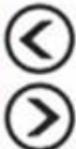
Provide domain administrator credentials to the litware.com Active Directory domain.

Create an instance of Microsoft Defender for Identity.

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

Install the sensor on DC1.

Install the standalone sensor on DC1.



- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

Text Description automatically generated with medium confidence

Step 1: log in to <https://portal.atp.azure.com> as a global admin Step 2: Create the instance

Step 3. Connect the instance to Active Directory Step 4. Download and install the sensor. Reference:

<https://docs.microsoft.com/en-us/defender-for-identity/install-step1> <https://docs.microsoft.com/en-us/defender-for-identity/install-step4>

**NEW QUESTION 6**

- (Exam Topic 2)

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

NOTE: Each correct selection is worth one point.

In the Cloud App Security portal:

▼

Add a security extension

Configure app connectors

Configure log collectors

From Azure Sentinel in the Azure portal:

▼

Add a data connector

Add a workbook

Configure the Logs settings

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

Graphical user interface, text, application Description automatically generated

Reference:

<https://docs.microsoft.com/en-us/cloud-app-security/siem-sentinel>

**NEW QUESTION 7**

- (Exam Topic 3)

You purchase a Microsoft 365 subscription.

You plan to configure Microsoft Cloud App Security.

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

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

NOTE: Each correct selection is worth one point.

Policy template type:  ▼

Access policy
Activity policy
Anomaly detection policy

Filter based on:  ▼

IP address tag
Source
User agent string

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

Graphical user interface, text, application, table Description automatically generated  
 Reference:  
<https://docs.microsoft.com/en-us/cloud-app-security/anomaly-detection-policy>

**NEW QUESTION 8**

- (Exam Topic 3)

You have a Microsoft Sentinel workspace named Workspace1.

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

What should you create in Workspace1?

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

**Answer:** A

**NEW QUESTION 9**

- (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:  ▼

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 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 10**

- (Exam Topic 3)

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

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

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

Which role should you assign to SecAdmin1?

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

**Answer: C**

**NEW QUESTION 10**

- (Exam Topic 3)

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

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

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

**Answer: D**

**Explanation:**

Reference:

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

**NEW QUESTION 15**

- (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 19**

- (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": "[resourceId('Microsoft.Automation', parameters('resourceGroupName'), 'Microsoft.Automation', parameters('subscriptionId'))]"/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', parameters('subscriptionId')), parameters('appName'), 'manual', '2019-05-01').value)]"
        }
      ]
    }
  }
],

```

- A. Mastered
- B. Not Mastered

**Answer: A**

**Explanation:**

Graphical user interface, text, application Description automatically generated

Reference:

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

**NEW QUESTION 20**

- (Exam Topic 3)

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

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

NOTE: Each correct selection is worth one point.

### Actions

- 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:**

Reference:

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

**NEW QUESTION 25**

- (Exam Topic 3)

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

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

You have three custom device groups.

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

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

**Answer:** ACD

**Explanation:**

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

**NEW QUESTION 27**

- (Exam Topic 3)

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

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

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

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

NOTE: Each correct selection is worth one point.

- A. `cp /bin/echo ./asc_alerttest_662jfi039n`
- B. `./alerttest testing eicar pipe`
- C. `cp /bin/echo ./alerttest`
- D. `./asc_alerttest_662jfi039n testing eicar pipe`

**Answer:** AD

**Explanation:**

Reference:

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

**NEW QUESTION 31**

- (Exam Topic 3)

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

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

What should you configure to mitigate the threat?

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

**Answer:** A

**Explanation:**

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

**NEW QUESTION 34**

- (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 38**

- (Exam Topic 3)

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

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

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

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

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

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

**NEW QUESTION 40**

- (Exam Topic 3)

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 42**

- (Exam Topic 3)

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

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

You receive a security alert in Security Center.

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

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

Does this meet the goal?

- A. Yes
- B. No

**Answer:** B

**Explanation:**

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

Reference:

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

**NEW QUESTION 46**

- (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`

1

	▼
project	
sort	
summarize	

	▼
arg_max	
limit	
top	

`(LastModifiedTime,*) by IncidentNumber`

- 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 50**

- (Exam Topic 3)

You have an Azure subscription linked to an Azure Active Directory (Azure AD) tenant. The tenant contains two users named User1 and User2.

You plan to deploy Azure Defender.

You need to enable User1 and User2 to perform tasks at the subscription level as shown in the following table.

User	Task
User1	<ul style="list-style-type: none"> <li>• Assign initiatives</li> <li>• Edit security policies</li> <li>• Enable automatic provisioning</li> </ul>
User2	<ul style="list-style-type: none"> <li>• View alerts and recommendations</li> <li>• Apply security recommendations</li> <li>• Dismiss alerts</li> </ul>

The solution must use the principle of least privilege.

Which role should you assign to each user? To answer, drag the appropriate roles to the correct users. Each role may be used once, more than once, or not at all.

You may need to drag the split bar between panes or scroll to view content.

Roles	Answer Area
Contributor	User1: <input type="text"/>
Owner	User2: <input type="text"/>
Security administrator	
Security reader	

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

Box 1: Owner

Only the Owner can assign initiatives. Box 2: Contributor

Only the Contributor or the Owner can apply security recommendations.

Reference:

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

**NEW QUESTION 54**

- (Exam Topic 3)

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

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

You are configuring Microsoft Defender for Identity integration with Active Directory.

From the Microsoft Defender for identity portal, you need to configure several accounts for attackers to exploit.

Solution: You add each account as a Sensitive account. Does this meet the goal?

- A. Yes
- B. No

**Answer:** B

**Explanation:**

Reference:

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

**NEW QUESTION 55**

- (Exam Topic 3)

You receive a security bulletin about a potential attack that uses an image file.

You need to create an indicator of compromise (IoC) in Microsoft Defender for Endpoint to prevent the attack. Which indicator type should you use?

- A. a URL/domain indicator that has Action set to Alert only
- B. a URL/domain indicator that has Action set to Alert and block
- C. a file hash indicator that has Action set to Alert and block
- D. a certificate indicator that has Action set to Alert and block

**Answer:** C

**Explanation:**

Reference:

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

**NEW QUESTION 60**

- (Exam Topic 3)

You have an Azure subscription that contains a Log Analytics workspace.

You need to enable just-in-time (JIT) VM access and network detections for Azure resources. Where should you enable Azure Defender?

- A. at the subscription level
- B. at the workspace level
- C. at the resource level

**Answer:** A

**Explanation:**

Reference:

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

#### NEW QUESTION 61

- (Exam Topic 3)

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

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

You are configuring Microsoft Defender for Identity integration with Active Directory.

From the Microsoft Defender for identity portal, you need to configure several accounts for attackers to exploit.

Solution: You add the accounts to an Active Directory group and add the group as a Sensitive group. Does this meet the goal?

- A. Yes
- B. No

**Answer: B**

#### Explanation:

Reference:

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

#### NEW QUESTION 62

- (Exam Topic 3)

You have a suppression rule in Azure Security Center for 10 virtual machines that are used for testing. The virtual machines run Windows Server.

You are troubleshooting an issue on the virtual machines.

In Security Center, you need to view the alerts generated by the virtual machines during the last five days. What should you do?

- A. Change the rule expiration date of the suppression rule.
- B. Change the state of the suppression rule to Disabled.
- C. Modify the filter for the Security alerts page.
- D. View the Windows event logs on the virtual machines.

**Answer: B**

#### Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/security-center/alerts-suppression-rules>

#### NEW QUESTION 64

- (Exam Topic 3)

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

You need to add threat indicators for all the IP addresses in a range of 171.23.3432-171.2334.63. The solution must minimize administrative effort.

What should you do in the Microsoft 365 Defender portal?

- A. Create an import file that contains the IP address of 171.23.34.32/27. Select Import and import the file.
- B. Select Add indicator and set the IP address to 171.2334.32-171.23.34.63.
- C. Select Add indicator and set the IP address to 171.23.34.32/27
- D. Create an import file that contains the individual IP addresses in the rang
- E. Select Import and import the file.

**Answer: C**

#### Explanation:

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

Reference:

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

#### NEW QUESTION 69

- (Exam Topic 3)

You have a Microsoft 365 subscription that uses Microsoft 365 Defender. You need to identify all the entities affected by an incident.

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

- A. Investigations
- B. Devices
- C. Evidence and Response
- D. Alerts

**Answer: C**

#### Explanation:

The Evidence and Response tab shows all the supported events and suspicious entities in the alerts in the incident.

Reference: <https://docs.microsoft.com/en-us/microsoft-365/security/defender/investigate-incidents>

#### NEW QUESTION 70

- (Exam Topic 3)

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

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

What should you do?

- A. Create a playbook.
- B. Create a watchlist.

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

**Answer:** C

**Explanation:**

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

**NEW QUESTION 73**

- (Exam Topic 3)

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:**

Reference: <https://docs.microsoft.com/en-us/azure/sentinel/tutorial-investigate-cases#use-the-investigation-graph-to-deep-d>

**NEW QUESTION 78**

- (Exam Topic 3)

You have the following KQL query.

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

Statements	Yes	No
The <code>username</code> 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 <code>IPList</code> variable is set as the IP address entity.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

Statements	Yes	No
The <code>username</code> field is set as the account entity.	<input checked="" type="radio"/>	<input type="radio"/>
The watchlist cannot be updated after it is created.	<input checked="" type="radio"/>	<input type="radio"/>
The <code>IPList</code> variable is set as the IP address entity.	<input type="radio"/>	<input checked="" type="radio"/>

**NEW QUESTION 83**

- (Exam Topic 3)

You have a Microsoft Sentinel workspace.

You need to create a KQL query that will identify successful sign-ins from multiple countries during the last three hours.

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

NOTE Each correct selection is worth one point

**Answer Area**

```
let timeframe = ago(3h);
let threshold = 5;
[
  imAuthentication
  imNetworkSession
  imProcessCreate
  imWebSession
]
| where TimeGenerated > timeframe
| where EventType=='Logon' and EventResult=='Success'
| where isnotempty(SrcGeoCountry)
| summarize StartTime = min(TimeGenerated), EndTime = max(TimeGenerated), Vendors=make_set(EventVendor), Products=make_set(EventProduct), '
NumOfCountries = dcount( [
  DstGeoCountry
  SrcGeoCountry
  SrcGeoRegion
] ) by TargetUserId, TargetUserPrincipalName, TargetUserType
| where NumOfCountries >= threshold
| extend timestamp = StartTime, AccountCustomEntity = TargetUserPrincipalName
```

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

**Answer Area**

```

let timeframe = ago(3h);
let threshold = 5;

| where TimeGenerated > timeframe
| where EventType=='Logon' and EventResult=='Success'
| where isnotempty(SrcGeoCountry)
| summarize StartTime = min(TimeGenerated), EndTime = max(TimeGenerated), Vendors=make_set(EventVendor), Products=make_set(EventProduct),
NumOfCountries = dcount( SrcGeoRegion ) by TargetUserId, TargetUserPrincipalName, TargetUserType
| where NumOfCountries >= threshold
| extend timestamp = StartTime, AccountCustomEntity = TargetUserPrincipalName

```

**NEW QUESTION 87**

- (Exam Topic 3)

You have the following environment:

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

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

You deploy Microsoft Defender for Identity by using standalone sensors.

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

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

**Answer:** AD

**Explanation:**

Reference:

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

**NEW QUESTION 89**

- (Exam Topic 3)

You use Azure Sentinel.

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

Which role should you assign to the analyst?

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

**Answer:** A

**Explanation:**

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

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

**NEW QUESTION 90**

.....

## Relate Links

**100% Pass Your SC-200 Exam with Exam Bible Prep Materials**

<https://www.exambible.com/SC-200-exam/>

## Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - <https://www.exambible.com/>