# SC-200<sup>Q&As</sup>

SC-200$^{Q\&As}$

## Microsoft Security Operations Analyst

## Pass Microsoft SC-200 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

**https://www.lead4pass.com/sc-200.html**

### 100% Passing Guarantee
### 100% Money Back Assurance

Following Questions and Answers are all new published by Microsoft
Official Exam Center

**QUESTION 1**

You provision Azure Sentinel for a new Azure subscription.

You are configuring the Security Events connector.

While creating a new rule from a template in the connector, you decide to generate a new alert for every event.

You create the following rule query.

```
let timeframe = 1d;
SecurityEvent
| where TimeGenerated >= ago(timeframe)
| where EventID == 1102 and EventSourceName == "Microsoft-Windows-Eventlog"
| summarize StartTimeUtc = min(TimeGenerated), EndTimeUtc = max(TimeGenerated),
EventCount = count() by
Computer, Account, EventID, Activity
| extend timestamp = StartTimeUtc, AccountCustomEntity = Account,
HostCustomEntity = Computer
```

By which two components can you group alerts into incidents? Each correct answer presents a complete solution.
NOTE: Each correct selection is worth one point.

A. user

B. resource group

C. IP address

D. computer

Correct Answer: CD

**QUESTION 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.

Correct Answer: C

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

**QUESTION 3**

You plan to create a custom Azure Sentinel query that will provide a visual representation of the security alerts generated by Azure Security Center.

You need to create a query that will be used to display a bar graph.

What should you include in the query?

A. extend

B. bin

C. count

D. workspace

Correct Answer: C

Reference: https://docs.microsoft.com/en-us/azure/azure-monitor/visualize/workbooks-chart-visualizations

**QUESTION 4**

You plan to create a custom Azure Sentinel query that will track anomalous Azure Active Directory (Azure AD) sign-in activity and present the activity as a time chart aggregated by day.

You need to create a query that will be used to display the time chart.

What should you include in the query?

A. extend

B. bin

C. makeset

D. workspace

Correct Answer: B

Reference: https://docs.microsoft.com/en-us/azure/azure-monitor/logs/get-started-queries

**QUESTION 5**

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

A. executive

B. sales

C. marketing

Correct Answer: B

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

**QUESTION 6**

DRAG DROP

You have resources in Azure and Google cloud.

You need to ingest Google Cloud Platform (GCP) data into Azure Defender.

In which order should you perform the actions? To answer, move all actions from the list of actions to the answer area and arrange them in the correct order.

Select and Place:



Correct Answer:

## Actions

## Answer Area

| Configure the GCP Security Command Center. |
| Enable Security Health Analytics. |
| Enable the GCP Security Command Center API. |
| Create a dedicated service account and a private key. |
| From Azure Security Center, add cloud connectors. |

**QUESTION 7**

DRAG DROP

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.

Select and Place:

**Actions**

| Change the alert severity threshold for emails to **Medium**. |
| Copy an executable file on a virtual machine and rename the file as ASC_AlertTest_662jfi039N.exe. |
| Enable Azure Defender for the subscription. |
| Change the alert severity threshold for emails to **Low**. |
| Run the executable file and specify the appropriate arguments. |
| Rename the executable file as AlertTest.exe. |

**Answer Area**

Correct Answer:

**Actions**

| Change the alert severity threshold for emails to **Medium**. |
| |
| |
| Change the alert severity threshold for emails to **Low**. |
| |
| Rename the executable file as AlertTest.exe. |

**Answer Area**

| Enable Azure Defender for the subscription. |
| Copy an executable file on a virtual machine and rename the file as ASC_AlertTest_662jfi039N.exe. |
| Run the executable file and specify the appropriate arguments. |

**QUESTION 8**

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

A. notebooks in Azure Sentinel

B. Microsoft Cloud App Security
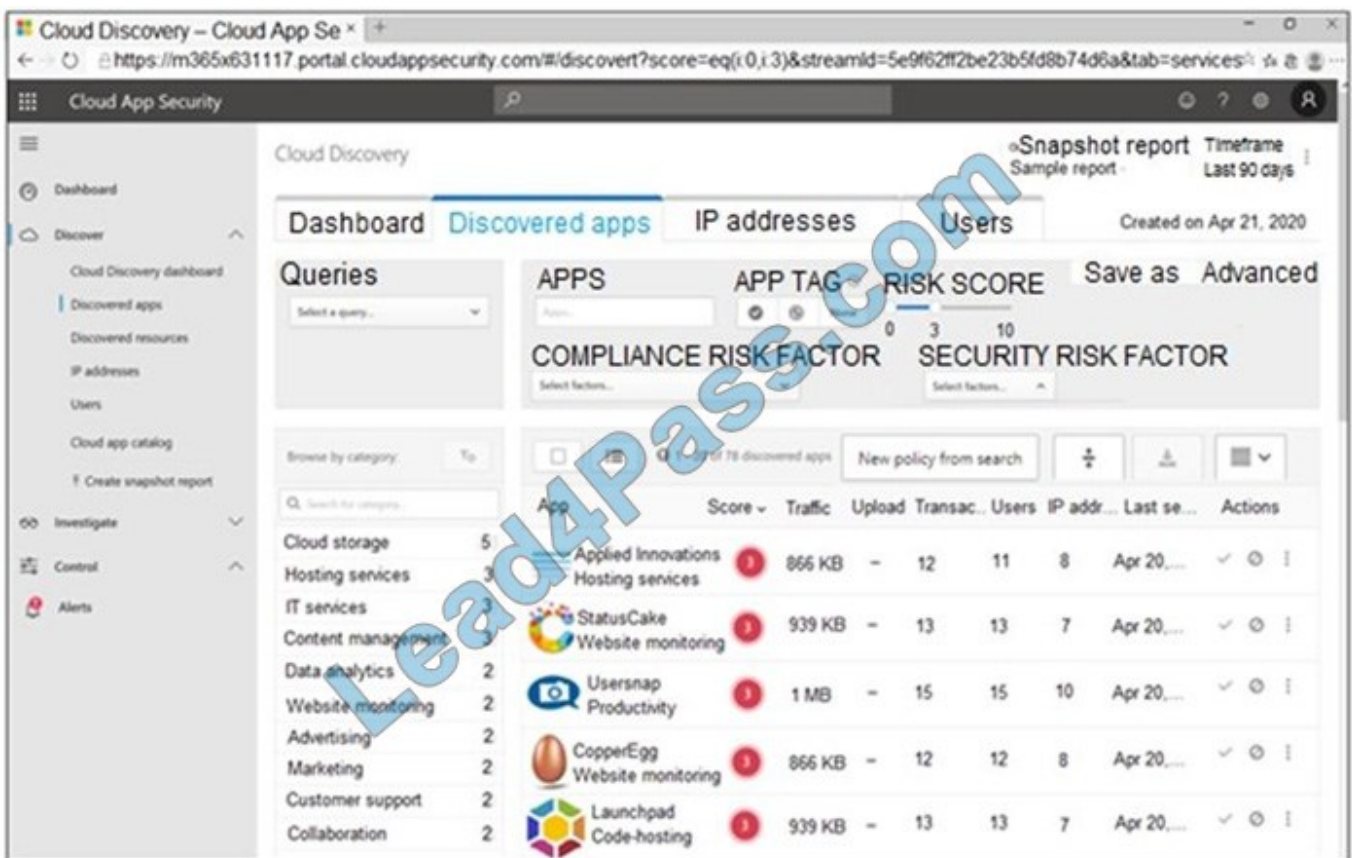
C. Azure Monitor

D. hunting queries in Azure Sentinel

Correct Answer: A

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

---

**QUESTION 9**

DRAG DROP

You open the Cloud App Security portal as shown in the following exhibit.

You need to remediate the risk for the Launchpad app.

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

Select and Place:

## Actions

Tag the app as **Unsanctioned.**

Run the script on the source appliance.

Run the script in Azure Cloud Shell.

Select the app.

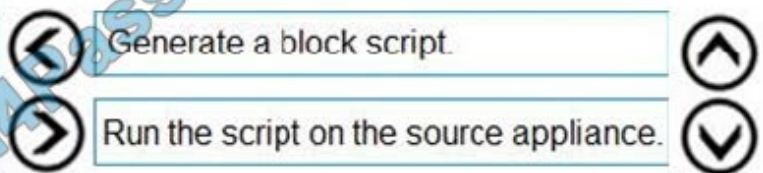Tag the app as **Sanctioned.**

Generate a block script.

## Answer Area

Correct Answer:

## Actions

Run the script in Azure Cloud Shell.

Tag the app as **Sanctioned.**

## Answer Area

Select the app.

Tag the app as **Unsanctioned.**

Generate a block script.

Run the script on the source appliance.

**QUESTION 10**

DRAG DROP

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.

Select and Place:

**Actions**

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.

**Answer Area**

Correct Answer:

**Actions**

Deploy an OMS Gateway on the network.

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

**Answer Area**

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.

**QUESTION 11**

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. And 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.

Correct Answer: B

---

**QUESTION 12**

HOTSPOT

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.

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.

Hot Area:

## 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

Correct Answer:

## 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 |

**QUESTION 13**

You have the following advanced hunting query in Microsoft 365 Defender.

```
DeviceProcessEvents
| where Timestamp > ago (24h)
and InitiatingProcessFileName =~ 'runsll32.exe'
and InitiatingProcessCommandLine !contains '" and InitiatingProcessCommandLine != ""
and FileName in~ ('schtasks.exe')
and ProcessCommandLine has 'Change' and ProcessCommandLine has 'SystemRestore'
and ProcessCommandLine has 'disable'
| project Timestamp, AccountName, ProcessCommandLine
```

You need to receive an alert when any process disables System Restore on a device managed by Microsoft Defender during the last 24 hours.

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

NOTE: Each correct selection is worth one point.

A. Create a detection rule.

B. Create a suppression rule.

C. Add | order by Timestamp to the query.

D. Replace DeviceProcessEvents with DeviceNetworkEvents.

E. Add DeviceId and ReportId to the output of the query.

Correct Answer: AE

Reference: https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/custom-detection-rules

SC-200 VCE Dumps          SC-200 Study Guide          SC-200 Exam Questions

To Read the Whole Q&As, please purchase the Complete Version from Our website.

# Try our product !

100% Guaranteed Success
100% Money Back Guarantee
365 Days Free Update
Instant Download After Purchase
24x7 Customer Support
Average 99.9% Success Rate
More than 800,000 Satisfied Customers Worldwide
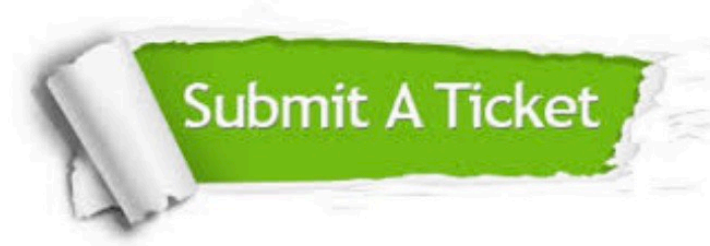Multi-Platform capabilities - Windows, Mac, Android, iPhone, iPod, iPad, Kindle


We provide exam PDF and VCE of Cisco, Microsoft, IBM, CompTIA, Oracle and other IT Certifications.
You can view Vendor list of All Certification Exams offered:

https://www.lead4pass.com/allproducts

## Need Help

Please provide as much detail as possible so we can best assist you.
To update a previously submitted ticket:





Any charges made through this site will appear as Global Simulators Limited.
All trademarks are the property of their respective owners.
Copyright © lead4pass, All Rights Reserved.