

Exam Questions SC-200

Microsoft Security Operations Analyst

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



NEW QUESTION 1

- (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 2

- (Exam 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:

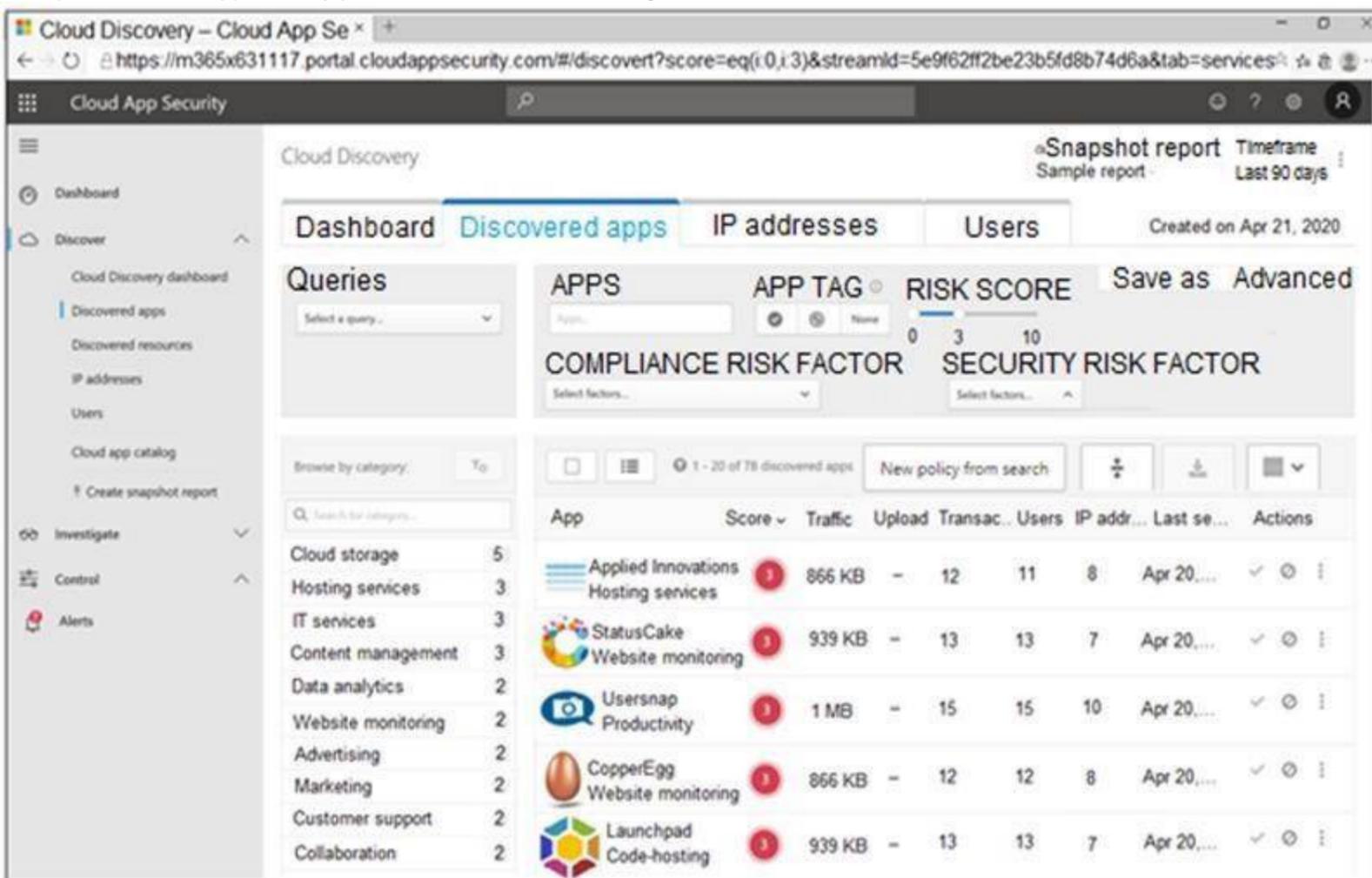
Reference:

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

NEW QUESTION 3

- (Exam Topic 3)

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.

Actions

Answer Area

- 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.



- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Reference:
<https://docs.microsoft.com/en-us/cloud-app-security/governance-discovery>

NEW QUESTION 4

- (Exam Topic 3)

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	<div style="width: 100%; height: 10px; background-color: red;"></div>
> Secure management ports	+9% (4 points)	1 of 2 resources	<div style="width: 50%; height: 10px; background-color: red;"></div> <div style="width: 50%; height: 10px; background-color: yellow;"></div>
> Enable encryption at rest	+9% (4 points)	2 of 2 resources	<div style="width: 100%; height: 10px; background-color: red;"></div>
> Remediate security configurations	+4% (2 points)	1 of 2 resources	<div style="width: 50%; height: 10px; background-color: red;"></div> <div style="width: 50%; height: 10px; background-color: yellow;"></div>
> Apply adaptive application control	+3% (2 points)	1 of 2 resources	<div style="width: 50%; height: 10px; background-color: red;"></div> <div style="width: 50%; height: 10px; background-color: yellow;"></div>
> Apply system updates ✔ Completed	+0% (0 points)	None	<div style="width: 100%; height: 10px; background-color: yellow;"></div>
> Enable endpoint protection ✔ Completed	+0% (0 points)	None	<div style="width: 100%; height: 10px; background-color: yellow;"></div>
> Remediate vulnerabilities ✔ Completed	+0% (0 points)	None	<div style="width: 100%; height: 10px; background-color: yellow;"></div>
> Implement security best practices ✔ Completed	+0% (0 points)	None	<div style="width: 100%; height: 10px; background-color: yellow;"></div>
> Enable MFA ✔ Completed	+0% (0 points)	None	<div style="width: 50%; height: 10px; background-color: yellow;"></div> <div style="width: 50%; height: 10px; background-color: gray;"></div>
> Manage access and permissions ✔ Completed	+0% (0 points)	None	<div style="width: 100%; height: 10px; background-color: yellow;"></div>

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:

Reference:

<https://techcommunity.microsoft.com/t5/azure-security-center/security-control-restrict-unauthorized-network-ac> <https://techcommunity.microsoft.com/t5/azure-security-center/security-control-secure-management-ports/ba-p/1>

NEW QUESTION 5

- (Exam Topic 3)

You are configuring Azure Sentinel.

You need to send a Microsoft Teams message to a channel whenever a sign-in from a suspicious IP address is detected.

Which two actions should you perform in Azure Sentinel? Each correct answer presents part of the solution. NOTE: Each correct selection is worth one point.

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

Answer: AB

NEW QUESTION 6

- (Exam Topic 3)

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

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

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

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

Solution: From 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 7

- (Exam Topic 3)

You have an Azure Sentinel workspace.

You need to test a playbook manually in the Azure portal. From where can you run the test in Azure Sentinel?

- A. Playbooks
- B. Analytics
- C. Threat intelligence
- D. Incidents

Answer: D

Explanation:

Reference:
<https://docs.microsoft.com/en-us/azure/sentinel/tutorial-respond-threats-playbook#run-a-playbook-on-demand>

NEW QUESTION 8

- (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 9

- (Exam Topic 3)

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: B

NEW QUESTION 10

- (Exam Topic 3)

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

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

You use Azure Security Center.

You receive a security alert in Security Center.

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

Solution: From Security alerts, you select the alert, select Take Action, and then expand the Mitigate the threat section.

Does this meet the goal?

- A. Yes
- B. No

Answer: A

Explanation:

Reference:

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

NEW QUESTION 10

- (Exam Topic 3)

Your company uses Microsoft Defender for Endpoint.

The company has Microsoft Word documents that contain macros. The documents are used frequently on the devices of the company's accounting team.

You need to hide false positive in the Alerts queue, while maintaining the existing security posture. Which three actions should you perform? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

- A. Resolve the alert automatically.
- B. Hide the alert.
- C. Create a suppression rule scoped to any device.
- D. Create a suppression rule scoped to a device group.
- E. Generate the alert.

Answer: BCE

Explanation:

Reference:

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

NEW QUESTION 11

- (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 15

- (Exam Topic 3)

You have a playbook in Azure Sentinel.

When you trigger the playbook, it sends an email to a distribution group.

You need to modify the playbook to send the email to the owner of the resource instead of the distribution group.

What should you do?

- A. Add a parameter and modify the trigger.
- B. Add a custom data connector and modify the trigger.
- C. Add a condition and modify the action.
- D. Add a parameter and modify the action.

Answer: D

Explanation:

Reference:

<https://azsec.azurewebsites.net/2020/01/19/notify-azure-sentinel-alert-to-your-email-automatically/>

NEW QUESTION 16

- (Exam Topic 3)

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 17

- (Exam Topic 3)

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 22

- (Exam Topic 3)

Your company uses Azure Security Center and Azure Defender.

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

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

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

Answer: C

Explanation:

Reference:

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

NEW QUESTION 26

- (Exam Topic 3)

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

You plan to use LA1 to automatically remediate security risks detected in 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.

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:

Reference:

<https://docs.microsoft.com/en-us/azure/security-center/workflow-automation#create-a-logic-app-and-define-when-to-trigger>

NEW QUESTION 31

- (Exam Topic 3)

You create an Azure subscription named sub1.

In sub1, you create a Log Analytics workspace named workspace1.

You enable Azure Security Center and configure Security Center to use workspace1.

You need to ensure that Security Center processes events from the Azure virtual machines that report to workspace1.

What should you do?

- A. In workspace1, install a solution.
- B. In sub1, register a provider.
- C. From Security Center, create a Workflow automation.
- D. In workspace1, create a workbook.

Answer: A

Explanation:

Reference:

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

NEW QUESTION 35

.....

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