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.pass4itsure.com/sc-200.html

100% Passing Guarantee
100% Money Back Assurance

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

Instant Download After Purchase
100% Money Back Guarantee
365 Days Free Update
800,000+ Satisfied Customers

QUESTION 1

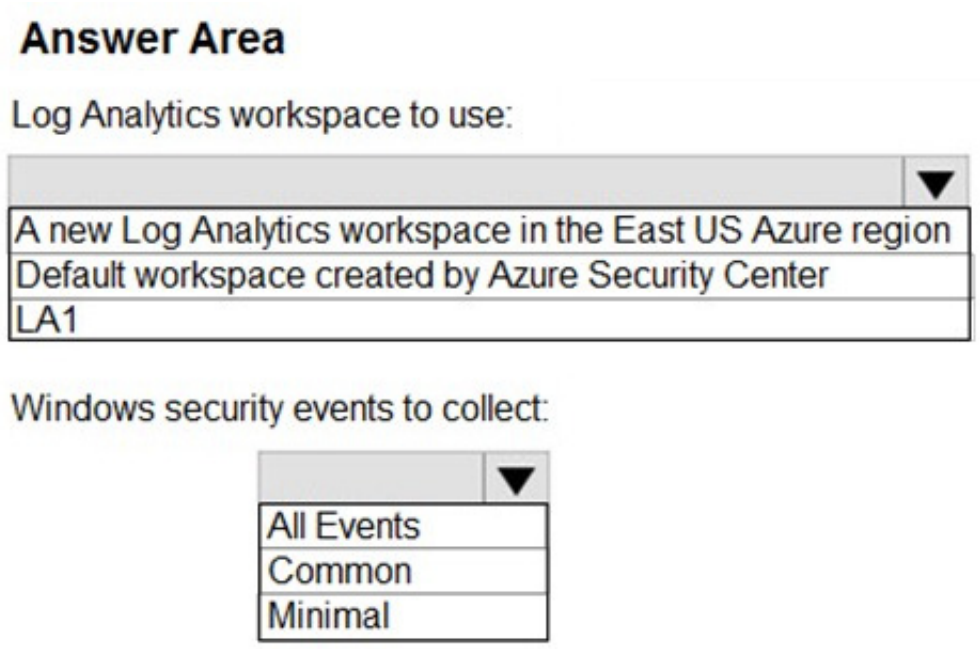
HOTSPOT

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.

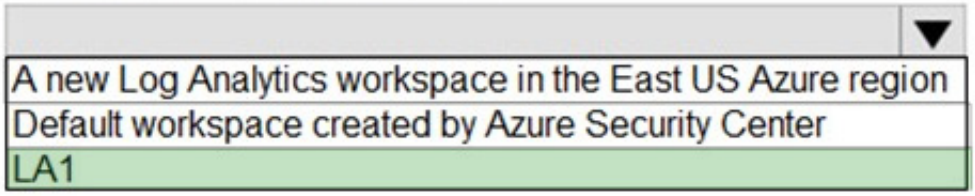
Hot Area:



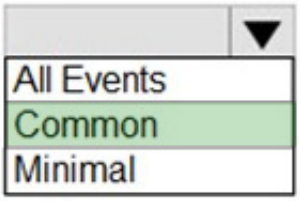
Correct Answer:

Answer Area

Log Analytics workspace to use:



Windows security events to collect:



QUESTION 2

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 have Linux virtual machines on Amazon Web Services (AWS).

You deploy Azure Defender and enable auto-provisioning.

You need to monitor the virtual machines by using Azure Defender.

Solution: You enable Azure Arc and onboard the virtual machines to Azure Arc.

Does this meet the goal?

A. Yes

B. No

Correct Answer: A

Defender for Cloud leverages Azure Arc to simplify the on-boarding and security of virtual machines running in AWS and other clouds. This includes automatic agent provisioning, policy management, vulnerability management, embedded EDR, and much more. Keyword: automatic agent provisioning Source https://techcommunity.microsoft.com/t5/itops-talk-blog/step-by-step-how-to-connect-aws-machines-to-microsoft-defender/ba-p/3251096

QUESTION 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

Correct Answer: A

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

QUESTION 4

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

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

Check any analytics rules, after you map the entities under the "Set rule logic" tab, then you can enable the "Alert grouping" under "Incident settings" by selecting "Enabled", then select "Grouping alerts into a single incident if the selected entity types and details match:" and select the entities from the drop down menu.

QUESTION 5

You plan to review Microsoft Defender for Cloud alerts by using a third-party security information and event management (SIEM) solution.

You need to locate alerts that indicate the use of the Privilege Escalation MITRE ATTandCK tactic.

Which JSON key should you search?

A. Description

B. Intent

C. ExtendedProperies

D. Entities

Correct Answer: B

The "Intent" key is part of the JSON format used by Microsoft Defender for Cloud to transmit security alert data to third-party security information and event management (SIEM) solutions. The "Intent" key provides information on the type of attack or tactic that the alert is related to, and can be used to identify alerts that are specifically related to the Privilege Escalation tactic.

SC-200 PDF Dumps SC-200 Practice Test SC-200 Study Guide