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.geekcert.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

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.

QUESTION 2

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 scheduled query rule for a data connector.

Does this meet the goal?

A. Yes

B. No

Correct Answer: B

Reference: https://docs.microsoft.com/en-us/azure/sentinel/connect-azure-security-center

QUESTION 3

HOTSPOT

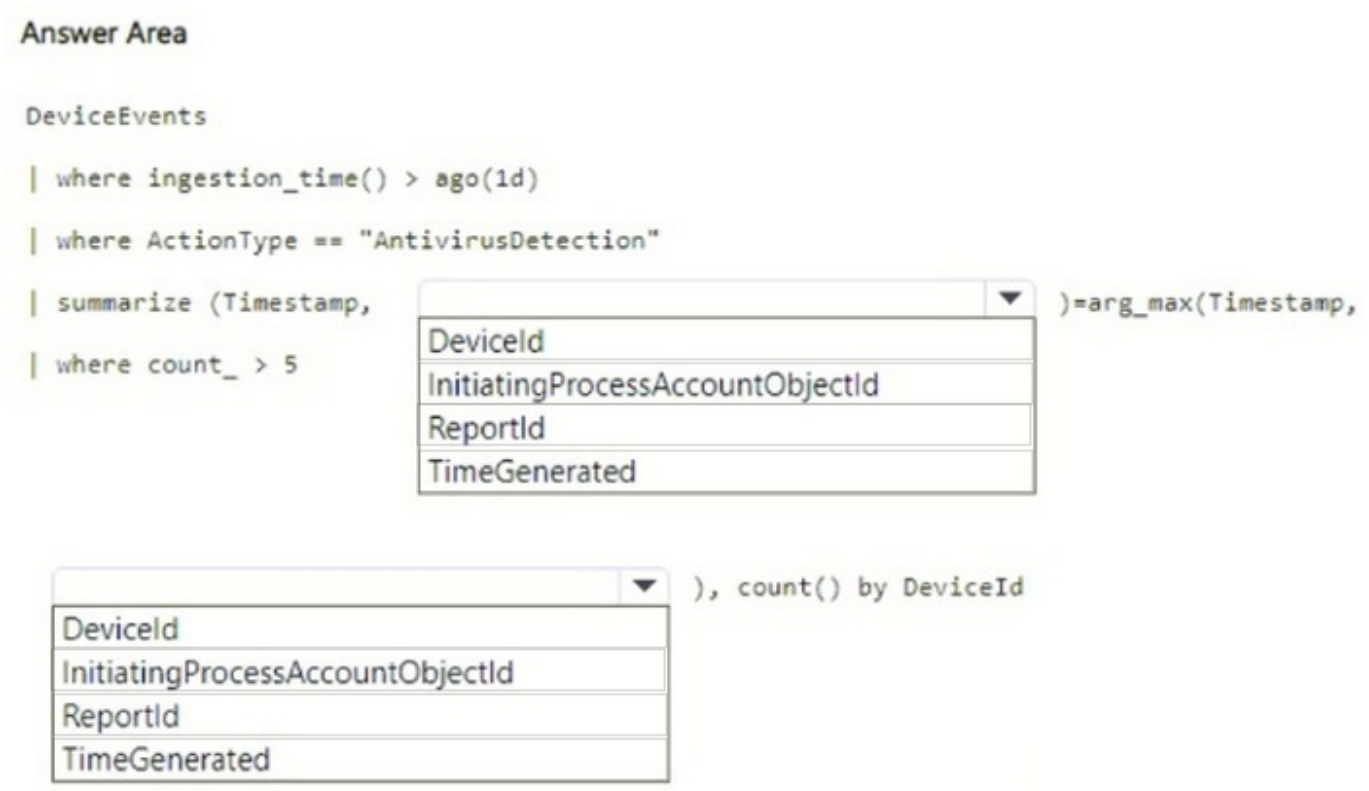
You have a Microsoft 365 subscription that uses Microsoft Defender XDR.

You need to create a custom detection rule that will identify devices that had more than five antivirus detections within the last 24 hours.

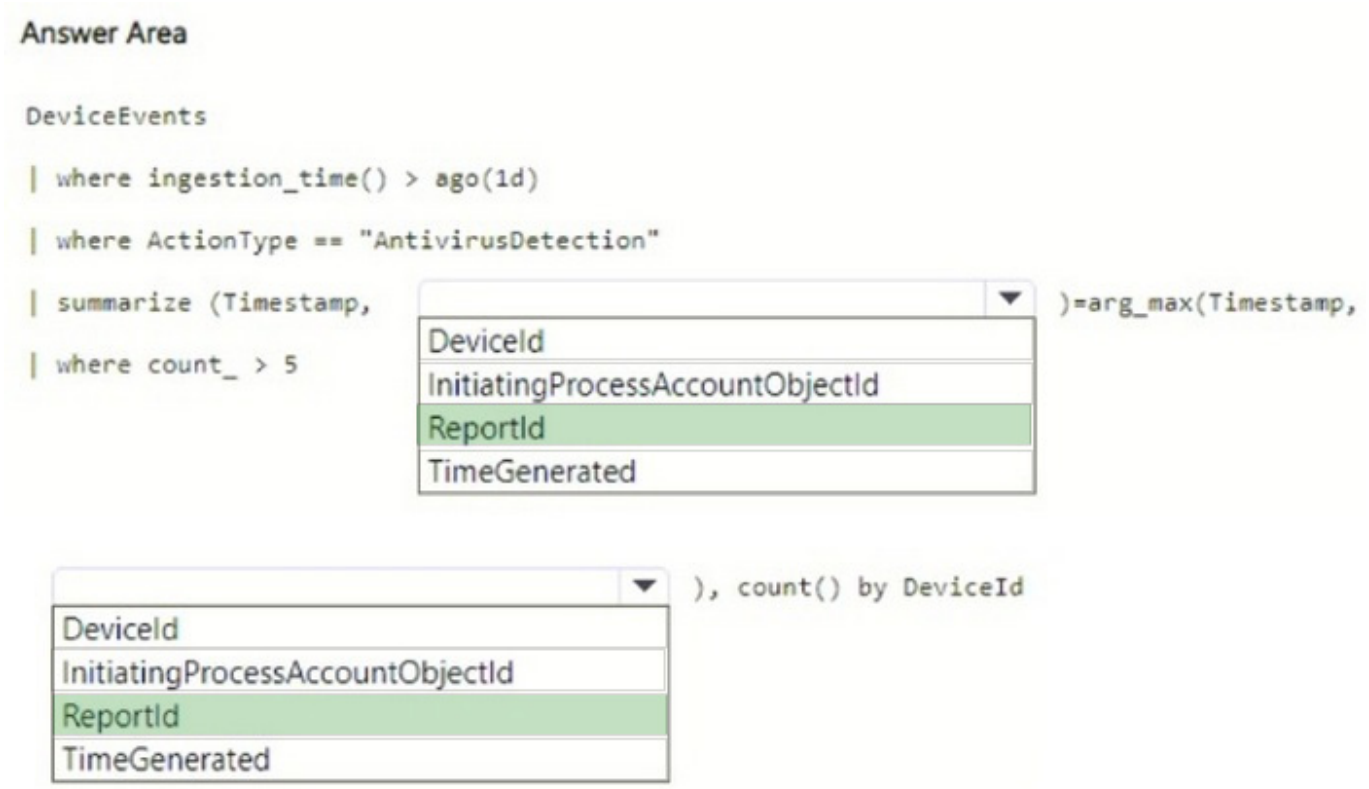
How should you complete the query? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:



Correct Answer:



QUESTION 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

Correct Answer: B

Reference: https://docs.microsoft.com/en-us/azure/sentinel/tutorial-respond-threats-playbook

QUESTION 5

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

Correct Answer: A

When you open Microsoft Sentinel, you are presented with a list of all the workspaces to which you have access rights, across all selected tenants and subscriptions. To the left of each workspace name is a checkbox. Selecting the name of a single workspace will bring you into that workspace. To choose multiple workspaces, select all the corresponding checkboxes, and then select the View incidents button at the top of the page.

https://learn.microsoft.com/en-us/azure/sentinel/multiple-workspace-view