https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/rbac?view=o365-worldwide

QUESTION 39
You have a Microsoft 365 subscription that contains 1,000 Windows 10 devices. The devices have Microsoft Office 365 installed.

You need to mitigate the following device threats:

- Microsoft Excel macros that download scripts from untrusted websites
- Users that open executable attachments in Microsoft Outlook
- Outlook rules and forms exploits

What should you use?

A. Microsoft Defender Antivirus
B. attack surface reduction rules in Microsoft Defender for Endpoint
C. Windows Defender Firewall
D. adaptive application control in Azure Defender

Correct Answer: B
Explanation:
https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/overview-attack-surface-reduction?view=o365-worldwide

QUESTION 40
You have an Azure subscription that uses Microsoft Sentinel.

You need to minimize the administrative effort required to respond to the incidents and remediate the security threats detected by Microsoft Sentinel.

Which two features should you use? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

A. Microsoft Sentinel bookmarks
B. Azure Automation runbooks
C. Microsoft Sentinel automation rules
D. Microsoft Sentinel playbooks
E. Azure Functions apps

Correct Answer: CD
Explanation:
https://docs.microsoft.com/en-us/azure/sentinel/tutorial-respond-threats-playbook?tabs=LAC

QUESTION 41
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.

Correct Answer: AD
Explanation:
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

QUESTION 42
You have a custom Microsoft Sentinel workbook named Workbooks.

You need to add a grid to Workbook1. The solution must ensure that the grid contains a maximum of 100 rows.

What should you do?

A. In the query editor interface, configure Settings.
B. In the query editor interface, select Advanced Editor
C. In the grid query, include the project operator.
D. In the grid query, include the take operator.

Correct Answer: B

QUESTION 43
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 Entity tags, you add the accounts as Honeytoken accounts.

Does this meet the goal?

A. Yes

B. No

Correct Answer: A
Explanation:
https://docs.microsoft.com/en-us/defender-for-identity/manage-sensitive-honeytoken-accounts

QUESTION 44
HOTSPOT
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.

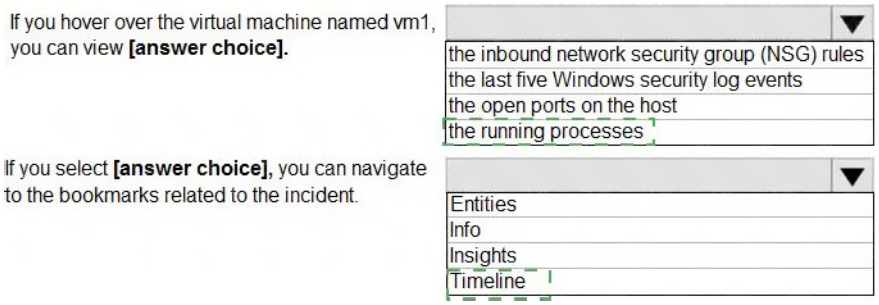
If you hover over the virtual machine named vm1, you can view **[answer choice].**

- 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

Correct Answer:

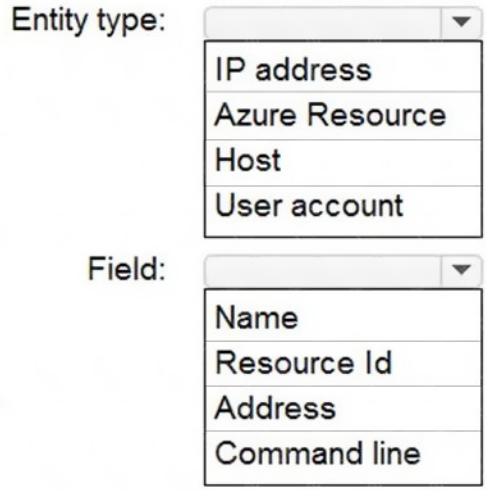


QUESTION 45
HOTSPOT
You have an Azure Storage account that will be accessed by multiple Azure Function apps during the development of an application.

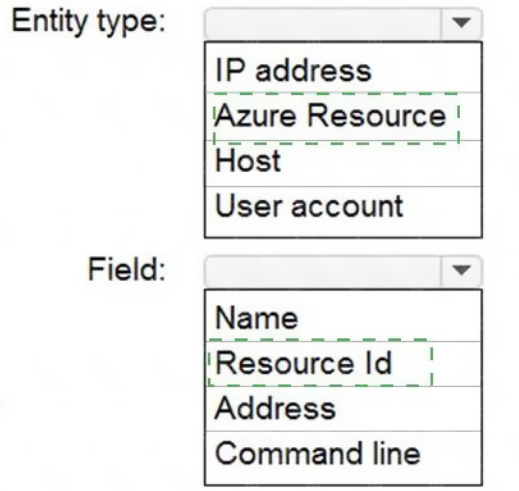
You need to hide Azure Defender alerts for the storage account.

Which entity type and field should you use in a suppression rule? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.



Correct Answer:



QUESTION 46
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

Correct Answer: C
Explanation:
https://docs.microsoft.com/en-us/azure/sentinel/notebooks

QUESTION 47
You have an Azure subscription that has Azure Defender enabled for all supported resource types.

You need to configure the continuous export of high-severity alerts to enable their retrieval from a third-party security information and event management (SIEM) solution.

To which service should you export the alerts?

A. Azure Cosmos DB
B. Azure Event Grid
C. Azure Event Hubs
D. Azure Data Lake
Correct Answer: C