Free Questions for SC-200 by vceexamstest

Shared by Ferrell on 20-10-2022

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

You have an Azure subscription that has Microsoft Defender for Cloud enabled.

You have a virtual machine that runs Windows 10 and has the Log Analytics agent installed.

You need to simulate an attack on the virtual machine that will generate an alert.

What should you do first?

Options:

A- Run the Log Analytics Troubleshooting Tool.

B- Copy a executable and rename the file as ASC_AlerTest_662jf10N,exe

C- Modify the settings of the Microsoft Monitoring Agent.

D- Run the MMASetup executable and specify the -foo argument

Answer:

A

Question 2

Question Type: MultipleChoice

You have an Azure subscription that uses Microsoft Defender for Cloud and contains a storage account named storage1. You receive an alert that there was an unusually high volume of delete operations on the blobs in storage1.

You need to identify which blobs were deleted.

What should you review?

Options:

A- the Azure Storage Analytics logs

B- the activity logs of storage1

C- the alert details

D- the related entities of the alert

Answer:

B

Question 3

Question Type: **MultipleChoice**

You have two Azure subscriptions that use Microsoft Defender for Cloud.

You need to ensure that specific Defender for Cloud security alerts are suppressed at the root management group level. The solution must minimize administrative effort.

What should you do in the Azure portal?

Options:

A- Create an Azure Policy assignment.

B- Modify the Workload protections settings in Defender for Cloud.

C- Create an alert rule in Azure Monitor.

D- Modify the alert settings in Defender for Cloud.

Answer:

D

Explanation:

You can use alerts suppression rules to suppress false positives or other unwanted security alerts from Defender for Cloud.

Note: To create a rule directly in the Azure portal:

1. From Defender for Cloud's security alerts page:

Select the specific alert you don't want to see anymore, and from the details pane, select Take action.

Or, select the suppression rules link at the top of the page, and from the suppression rules page select Create new suppression rule:

2. In the new suppression rule pane, enter the details of your new rule.

Your rule can dismiss the alert on all resources so you don't get any alerts like this one in the future.

Your rule can dismiss the alert on specific criteria - when it relates to a specific IP address, process name, user account, Azure resource, or location.

3. Enter details of the rule.

4. Save the rule.

Question 4

Question Type: MultipleChoice

You have a Microsoft Sentinel workspace that contains the following incident.

Brute force attack against Azure Portal analytics rule has been triggered.

You need to identify the geolocation information that corresponds to the incident.

What should you do?

Options:

A- From Overview, review the Potential malicious events map.

B- From Incidents, review the details of the iPCustomEntity entity associated with the incident.

C- From Incidents, review the details of the AccouncCuscomEntity entity associated with the incident.

D- From Investigation, review insights on the incident entity.

Answer:

A

Explanation:

Potential malicious events: When traffic is detected from sources that are known to be malicious, Microsoft Sentinel alerts you on the map. If you see orange, it is inbound traffic: someone is trying to access your organization from a known malicious IP address. If you see

Outbound (red) activity, it means that data from your network is being streamed out of your organization to a known malicious IP address.

Question 5

Question Type: MultipleChoice

You have a Microsoft Sentinel workspace named workspace1 that contains custom Kusto queries.

You need to create a Python-based Jupyter notebook that will create visuals. The visuals will display the results of the queries and be pinned to a dashboard. The solution must minimize development effort.

What should you use to create the visuals?

Options:

A- plotly

B- TensorFlow

C- msticpy

D- matplotlib

Answer:

C

Explanation:

msticpy is a library for InfoSec investigation and hunting in Jupyter Notebooks. It includes functionality to: query log data from multiple sources. enrich the data with Threat Intelligence, geolocations and Azure resource data. extract Indicators of Activity (IoA) from logs and unpack encoded data.

MSTICPy reduces the amount of code that customers need to write for Microsoft Sentinel, and provides:

Data query capabilities, against Microsoft Sentinel tables, Microsoft Defender for Endpoint, Splunk, and other data sources.

Threat intelligence lookups with TI providers, such as VirusTotal and AlienVault OTX.

Enrichment functions like geolocation of IP addresses, Indicator of Compromise (IoC) extraction, and WhoIs lookups.

Visualization tools using event timelines, process trees, and geo mapping.

Advanced analyses, such as time series decomposition, anomaly detection, and clustering.

https://docs.microsoft.com/en-us/azure/sentinel/notebook-get-started

https://msticpy.readthedocs.io/en/latest/

Question 6

Question Type: **MultipleChoice**

You have a Microsoft 365 tenant that uses Microsoft Exchange Online and Microsoft Defender for Office 365.

What should you use to identify whether zero-hour auto purge (ZAP) moved an email message from the mailbox of a user?

Options:

A- the Threat Protection Status report in Microsoft Defender for Office 365

B- the mailbox audit log in Exchange

C- the Safe Attachments file types report in Microsoft Defender for Office 365

D- the mail flow report in Exchange

Answer:

A

Explanation:

To determine if ZAP moved your message, you can use either the Threat Protection Status report or Threat Explorer (and real-time detections).

https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/zero-hour-auto-purge?view=o365-worldwide

Question 7

Question Type: MultipleChoice

You have an Azure subscription named Sub1 and a Microsoft 365 subscription. Sub1 is linked to an Azure Active Directory (Azure AD) tenant named contoso.com.

You create an Azure Sentinel workspace named workspace1. In workspace1, you activate an Azure AD connector for contoso.com and an Office 365 connector for the Microsoft 365 subscription.

You need to use the Fusion rule to detect multi-staged attacks that include suspicious sign-ins to contoso.com followed by anomalous Microsoft Office 365 activity.

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

NOTE: Each correct selection is worth one point.

Options:

A- Create custom rule based on the Office 365 connector templates.

B- Create a Microsoft incident creation rule based on Azure Security Center.

C- Create a Microsoft Cloud App Security connector.

D- Create an Azure AD Identity Protection connector.

Answer:

A, B

Question 8

Question Type: MultipleChoice

You create a hunting query in Azure Sentinel.

You need to receive a notification in the Azure portal as soon as the hunting query detects a match on the query. The solution must minimize effort.

What should you use?

Options:

A- a playbook

B- a notebook

C- a livestream

D- a bookmark

Answer:

C

Explanation:

Use livestream to run a specific query constantly, presenting results as they come in.

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