Free Questions for SC-200 by ebraindumps

Shared by Mclean on 12-12-2023

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

You have a Microsoft 365 subscription that uses Microsoft Purview.

Your company has a project named Project1.

You need to identify all the email messages that have the word Project1 in the subject line. The solution must search only the mailboxes of users that worked on Project1.

What should you do?

Options:

A- Create a records management disposition.

B- Perform a user data search.

C- Perform an audit search.

D- Perform a content search.

Answer:

D

Question 2

Question Type: MultipleChoice

You have a Microsoft Sentinel workspace that has user and Entity Behavior Analytics (UEBA) enabled for Signin Logs.

You need to ensure that failed interactive sign-ins are detected.

The solution must minimize administrative effort.

What should you use?

Options:

A- a scheduled alert query

B- a UEBA activity template

C- the Activity Log data connector

D- a hunting query

Answer:

B

Question 3

Question Type: MultipleChoice

You have a Microsoft 365 E5 subscription that uses Microsoft Defender for Endpoint

You need to create a query that will link the AlertInfo, AlertEvidence, and DeviceLogonEvents tables. The solution must return all the rows in the tables.

Which operator should you use?

Options:

A- join kind = inner

B- evaluate hint. Remote =

C- search *

D- union kind = inner

Answer:

A

Question 4

Question Type: MultipleChoice

You have a Microsoft 365 E5 subscription that uses Microsoft Defender for Endpoint

You need to identify any devices that triggered a malware alert and collect evidence related to the alert. The solution must ensure that you can use the results to initiate device isolation for the affected devices.

What should you use in the Microsoft 365 Defender portal?

Options:

A- Incidents

B- Investigations

C- Advanced hunting

D- Remediation

Answer:

A

Question 5

Question Type: MultipleChoice

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?

Options:

A- Microsoft Sentinel - Incidents

B- Microsoft Sentinel - Workbooks

C- Microsoft Sentinel

D- Log Analytics workspaces

Answer:

D

Question 6

Question Type: MultipleChoice

You have a Microsoft Sentinel workspace that uses the Microsoft 365 Defender data connector.

From Microsoft Sentinel, you investigate a Microsoft 365 incident.

You need to update the incident to include an alert generated by Microsoft Defender for Cloud Apps.

What should you use?

Options:

A- the entity side panel of the Timeline card in Microsoft Sentinel

B- the investigation graph on the Incidents page of Microsoft Sentinel

C- the Timeline tab on the Incidents page of Microsoft Sentinel

D- the Alerts page in the Microsoft 365 Defender portal

Answer:

A

Question 7

Question Type: MultipleChoice

You have a Microsoft 365 E5 subscription that contains 100 Linux devices. The devices are onboarded to Microsoft Defender 365. You need to initiate the collection of investigation packages from the devices by using the Microsoft 365 Defender portal. Which response action should you use?

Options:

A- Run antivirus scan

B- Initiate Automated Investigation

C- Collect investigation package

D- Initiate Live Response Session

Answer:

D

Question 8

Question Type: MultipleChoice

You have an Azure subscription that uses Microsoft Defender for Cloud.

You have an Amazon Web Services (AWS) subscription. The subscription contains multiple virtual machines that run Windows Server.

You need to enable Microsoft Defender for Servers on the virtual machines.

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

NOTE: Each correct answer is worth one point.

Options:

A- From Defender for Cloud, enable agentless scanning.

B- Install the Azure Virtual Machine Agent (VM Agent) on each virtual machine.

C- Onboard the virtual machines to Microsoft Defender for Endpoint.

D- From Defender for Cloud, configure auto-provisioning.

E- From Defender for Cloud, configure the AWS connector.

Answer:

B, C

Question 9

Question Type: MultipleChoice

You have a Microsoft Sentinel playbook that is triggered by using the Azure Activity connector.

You need to create a new near-real-time (NRT) analytics rule that will use the playbook.

What should you configure for the rule?

Options:

A- the Incident automation settings

B- entity mapping

C- the query rule

D- the Alert automation settings

Answer:

B

Question 10

Question Type: MultipleChoice

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

You plan to create a hunting query from Microsoft Defender.

You need to create a custom tracked query that will be used to assess the threat status of the subscription.

From the Microsoft 365 Defender portal, which page should you use to create the query?

Options:

A- Policies & rules

B- Explorer

C- Threat analytics

D- Advanced Hunting

Answer:

D

Question 11

Question Type: MultipleChoice

You have an Azure subscription that uses Microsoft Sentinel and contains 100 Linux virtual machines.

You need to monitor the virtual machines by using Microsoft Sentinel. The solution must meet the fallowing requirements:

* Minimize administrative effort

* Minimize the parsing required to read log data

What should you configure?

Options:

A- REST API integration

B- a SysJog connector

C- a Log Analytics Data Collector API

D- a Common Event Format (CEF) connector

Answer:

B

Question 12

Question Type: MultipleChoice

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

You have a virtual machine named Server! that runs Windows Server 2022 and is hosted in Amazon Web Services (AWS).

You need to collect logs and resolve vulnerabilities for Server1 by using Defender for Cloud.

What should you install first on Server1?

Options:

A- the Microsoft Monitoring Agent

B- the Azure Arc agent

C- the Azure Monitor agent

D- the Azure Pipelines agent

Answer:

C