DUMPSHQ

Free Questions for PCCSE by dumpshq

Shared by Garza on 18-01-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: **MultipleChoice**

Given this information:

The password is: password123

The image to scan is: myimage:latest

Which twistcli command should be used to scan a Container for vulnerabilities and display the details about each vulnerability?

Options:

A) twistcli images scan --console-address https://prisma-console.mydomain.local -u cluster -p password123 -- details myimage:latest

B) twistcli images scan --console-address prisma-console.mydomain.local -u cluster -p password123 -- vulnerability-details myimage:latest

C) twistcli images scan --address prisma-console.mydomain.local -u cluster -p password123 --vulnerability- details myimage:latest

D) twistcli images scan --address https://prisma-console.mydomain.local -u cluster -p password123 --details myimage:latest

Answer:

D

Question 2

Question Type: MultipleChoice

Given this information:

* The Console is located at https//prisma-console mydomain local

* The username is ciuser

* The password is password123

* The Image to scan is myimage latest

Which twistcli command should be used to scan a Container for vulnerabilities and display the details about each vulnerability?

Options:

A) twistcli images scan ---console-address https //prisma-console mydomain local -u ciuser -p password123 -details myimage latest

B) twistcli images scan ---address prisma-console mydomain local -u ciuser -p password123 -vulnerability-details myimage latest

C) twistcli images scan -address https //prisma-console mydomain local -u ciuser -p password123 -details myimage latest

D) twistcli images scan ---console-address prisma-console mydomain local -u ciuser -p password!23 -vulnerability-details myimage.latest

Answer:

D

Question 3

Question Type: **MultipleChoice**

You are an existing customer of Prisma Cloud Enterprise. You want to onboard a public cloud account and immediately see all of the alerts associated with this account based off ALL of your tenant's existing enabled policies. There is no requirement to send alerts from this account to a downstream application at this time.

Which options shows the steps required during the alert rule creation process to achieve this objective?

Options:

A) Ensure the public cloud account is assigned to an account group
Assign the confirmed account group to alert rule
Select one or more policies as part of the alert rule
Add alert notifications
Confirm the alert rule

B) Ensure the public cloud account is assigned to an account group
Assign the confirmed account group to alert rule
Select one or more policies checkbox as part of the alert rule

Confirm the alert rule

C) Ensure the public cloud account is assigned to an account group
Assign the confirmed account group to alert rule
Select 'select all policies' checkbox as part of the alert rule
Confirm the alert rule

D) Ensure the public cloud account is assigned to an account group
Assign the confirmed account group to alert rule
Select 'select all policies' checkbox as part of the alert rule
Add alert notifications
Confirm the alert rule

Answer:

A

Question 4

Question Type: **MultipleChoice**

You have onboarded a public cloud account into Prisma Cloud Enterprise Configuration Resource ingestion is visible in the Asset Inventory for the onboarded account, but no alerts are being generated for the configuration assets in the account

Config policies are enabled in the Prisma Cloud Enterprise tenant, with those policies associated to existing alert rules RQL statements on the Investigate matching those policies return config resource results successfully

Why are no alerts being generated''

Options:

A) The public cloud account does not have audit trail ingestion enabled.

B) The public cloud account is not associated with an alert notification.

C) The public cloud account does not have access to configuration resources.

D) The public cloud account is not associated with an alert rule

Answer:

B

Question 5

Question Type: MultipleChoice

A customer wants to be notified about port scanning network activities in their environment Which policy type detects this behavior?

Options:

A) Network

B) Anomaly

C) Config

D) Port Scan

Answer:

B

Question 6

Question Type: MultipleChoice

A customer has Defenders connected to Prisma Cloud Enterprise The Defenders are deployed as a DaemonSet in OpenShift. How should the administrator get a report of vulnerabilities on hosts'?

Options:

A) Navigate to Defend > Vulnerabilities > VM Images

B) Navigate to Monitor > Vulnerabilities > Hosts

C) Navigate to Defend > Vulnerabilities > Hosts

D) Navigate to Monitor > Vulnerabilities > CVE Viewer

Answer:

C

Question 7

Question Type: **MultipleChoice**

How are the following categorized?

* Backdoor account access

* Hijacked processes

* Lateral movement

* Port scanning

Options:

A) audits

B) models

C) admission controllers

D) incidents

Answer:

A

Question 8

Question Type: **MultipleChoice**

Which statement is true about obtaining Console images for Prisma Cloud Compute Edition'?

To retrieve Prisma Cloud Console images using URL auth;

Options:

A) 1 Access registry-urt-auth twistlock com, and authenticate using the user certificate

2. Retrieve the Prisma Cloud Console images using 'docker pull'

To retrieve Prisma Cloud Console images using basic auth:

B) 1. Access registry twistlock com. and authenticate using 'docker login'

2 Retrieve the Prisma Cloud Console images using 'docker pull'

To retrieve Prisma Cloud Console images using URL auth

C) 1 Access registry-auth.twistlock com and authenticate using the user certificate

2. Retrieve the Prisma Cloud Console images using 'docker pull'

To retrieve Prisma Cloud Console images using basic auth

D) 1 Access registry paloaltonetworks com. and authenticate using 'docker login'

2 Retrieve the Prisma Cloud Console images using 'docker pull'

Answer:

C

Question 9

Question Type: **MultipleChoice**

A customer is deploying Defenders to a Fargate environment It wants to understand the vulnerabilities in the images it is deploying. How should the customer automate vulnerability scanning for images deployed to Fargate?

Options:

A) Embed a Fargate Defender to automatically scan for vulnerabilities

B) Use Cloud Compliance to identify misconfigured AWS accounts

C) Set up a vulnerability scanner on the registry

D) Designate a Fargate Defender to serve a dedicated image scanner

Answer:

A