Free Questions for PCCSE by certsdeals

Shared by Jacobs on 05-09-2022

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

Which "kind" of Kubernetes object that is configured to ensure that Defender is acting as the admission controller?

Options:

A) PodSecurityPolicies

B) DestinationRules

C) ValidatingWebhookConfiguration

D) MutatingWebhookConfiguration

Answer:

D

Question 2

Question Type: MultipleChoice

Which three types of bucket exposure are available in the Data Security module? (Choose three.)

Options:

A) Differential

B) Public

C) Conditional

D) Private

E) International

Answer:

A, C, E

Question 3

Question Type: **MultipleChoice**

A S3 bucket within AWS has generated an alert by violating the Prisma Cloud Default policy "AWS S3 buckets are accessible to public"
The policy definition follows:

config where cloud type = 'aws' AND api name='aws-s3api-get-bucket-acr AND json.rule="((((acl grants{?(@ grantee='AllUsers')] size > 0) or policyStatusisPubiic is true) and publicAccessBlockConfiguration does not exist) or ((ad.grantsp(@ grantee=='AII Users')] size > 0) and publicAccessBlockConfiguration ignorePubhcAds is false) or (policyStatus isPublic is true and publicAccessBlockConfiguration.restrictPublicBuckets is false)) and websiteConfiguration does not exist" Why did this alert get generated?

Options:

A) anomalous behaviors

B) network traffic to the S3 bucket

C) configuration of the S3 bucket

D) an event within the cloud account

Answer:

A

Question 4

Question Type: **MultipleChoice**

An administrator sees that a runtime audit has been generated for a Container The audit message is DNS resolution of suspicious name wikipedia.com. type A".

Why would this message appear as an audit?

Options:

A) The Layer7 firewall detected this as anomalous behavior

B) This is a DNS known to be a source of malware

C) The process calling out to this domain was not part of the Container model.

D) The DNS was not learned as part of the Container model or added to the DNS allow list

Answer:

B

Question 5

Question Type: **MultipleChoice**

The security team wants to protect a web application container from an SQLi attack? Which type of policy should the administrator create to protect the container?

Options:

A) Compliance

B) Runtime

C) CNAF

D) CNNF

Answer:

D

Question 6

Question Type: MultipleChoice

What are two ways to scan container images in Jenkins pipelines? (Choose two)

Options:

A) Compute Jenkins plugin

B) Jenkins Docker plugin

C) Compute Azure DevOps plugin

D) Prisma Cloud Visual Studio Code plugin with Jenkins integration

E) twistcli

Answer:

D, E

Question 7

Question Type: **MultipleChoice**

Review this admission control policy:

```
match[{"msg": msg}] {
input.request.operation == "CREATE"
input.request.kind.kind == "Pod"
input.request.resource.resource == "pods"
input.request.object.spec.containers[_].securityContext.privileged
msg := "Privileged"
}
```

Which response to this policy will be achieved when the effect is set to "block"?

Options:

A) The policy will replace Defender with a privileged Defender

B) The policy will block the creation of a privileged pod

C) The policy will block all pods on a Privileged host

D) The policy will alert only the administrator when a privileged pod is created

Answer:

A

Question 8

Question Type: MultipleChoice

The security team wants to target a CMAF policy for specific running Containers How should the administrator scope the policy to target the Containers?

Options:

A) scope the policy to Image names

B) scope the policy to namespaces

C) scope the policy to Defender names.

D) scope the policy to Host names

Answer:

B

Question 9

Question Type: MultipleChoice

The development team wants to block Cross Site Scripting attacks from pods its environment

How should the team construct the CNAF policy to protect against this attack?

Options:

A) create a Container CNAF policy, targeted at a specific resource, check the box for XSS attack protection and set the action to alert

B) create a Host CNAF policy targeted at a specific resource, check the box for XSS attack protection and set the action to 'prevent'

C) create a Container CNAF policy, targeted at a specific resource, check the box for XSS attack protection and set the action to prevent

D) create a Container CNAF policy, targeted at a specific resource, and they should set 'Explicitly allowed inbound IP sources' to the IP address of the pod.

Answer:

B