Free Questions for PCCSE

Shared by Levine on 29-01-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

Which two attributes are required for a custom config RQL? (Choose two.)

Options:

A- json.rule

B- cloud.account

C- api.name

D- tag

Answer:

A, C

Explanation:

For a custom config Resource Query Language (RQL) in Prisma Cloud, two essential attributes are 'json.rule' and 'api.name.' The 'json.rule' attribute allows users to specify the JSON structure that defines the criteria or conditions of the query, essentially dictating what the query is looking for within the cloud environment. The 'api.name' attribute identifies the specific API endpoint that the query will target, providing context and scope for the query. Together, these attributes enable users to craft precise and targeted queries that can assess the configuration and security posture of cloud resources, aiding in compliance checks, security assessments, and other governance tasks.

Question 2

Question Type: MultipleChoice

The security team wants to enable the ''block'' option under compliance checks on the host.

What effect will this option have if it violates the compliance check?

Options:

A- The host will be taken offline.

B- Additional hosts will be prevented form starting.
C- Containers on a host will be stopped.
D- No containers will be allowed to start on that host.

Answer:

D

Explanation:

Enabling the 'block' option under compliance checks on a host in Prisma Cloud signifies a strict enforcement policy, where any container that violates specified compliance checks will be prevented from starting on that host. This preventive measure is crucial for maintaining a secure and compliant cloud environment, ensuring that only containers that meet the organization's compliance and security standards are allowed to run. This approach aligns with Prisma Cloud's proactive security posture management, where potential risks are mitigated before they can impact the cloud environment.

https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin-compute/compliance/manage_compliance

Question 3

Question Type: MultipleChoice

What is the default namespace created by Defender DaemonSet during deployment?

Options:

A- Redlock
B- Defender
C- Twistlock
D- Default

Answer:

C

Explanation:

the default when using the script is twistlock, but you can use whatever you want.
https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin-compute/configure/set_diff_paths_daemon_sets

Question 4

Question Type: MultipleChoice

Which policy type should be used to detect and alert on cryptominer network activity?

Options:

A- Audit event

B- Anomaly

C- Config-build

D- Config-run

Answer:

B

Explanation:

To detect and alert on cryptominer network activity, the policy type that should be used is an Anomaly policy. Anomaly policies in Prisma Cloud are designed to identify unusual and potentially malicious activities, including the network patterns typical of cryptomining operations. These policies leverage behavioral analytics to spot deviations from normal operations, making Option B the correct answer.

Suspicious network actors---Exposes suspicious connections by inspecting the network traffic to and from your cloud environment and correlating it with AutoFocus, Palo Alto Networks threat intelligence feed. AutoFocus identifies IP addresses involved in suspicious or malicious activity and classifies them into one of eighteen categories. Some examples of the categories are Backdoor, Botnet, Cryptominer, DDoS, Ransomware, Rootkit, and Worm. There are thirty-six policies, two for each of the eighteen categories---internal and external.
https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin/prisma-cloud-policies/anomaly-policies

Question 5

Question Type: MultipleChoice

Which two services require external notifications to be enabled for policy violations in the Prisma Cloud environment? (Choose two.)

Options:

A- Splunk

B- QROC

C- SQS

D- Email

Answer:

A, C

Explanation:

https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin/configure-external-integrations-on-prisma-cloud#id24911ff9-c9ec-4503-bb3a-6cfce792a70d

Question 6

Question Type: MultipleChoice

Which two statements explain differences between build and run config policies? (Choose two.)

Options:

A- Run and Network policies belong to the configuration policy set.

B- Build policies allow checking for security misconfigurations in the IaC templates and ensure these issues do not get into production.

C- Run policies monitor network activities in the environment and check for potential issues during runtime.

D- Run policies monitor resources and check for potential issues after these cloud resources are deployed.

Answer:

B, D

Explanation:

The Run policies monitor resources and check for potential issues once these cloud resources are deployed Build policies enable you to check for security misconfigurations in the IaC templates and ensure that these issues do not make their way into production. https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin/prisma-cloud-policies /create-a-policy

B . Build policies: These are designed to identify insecure configurations in your Infrastructure as Code (IaC) templates, such as AWS CloudFormation, HashiCorp Terraform, and Kubernetes App manifests. The goal of build policies is to detect security issues early in the development process, before the actual resources are deployed in runtime environments.This helps ensure that security issues are identified and remediated before they can affect production1.

D . Run policies: These policies are focused on monitoring the deployed cloud resources and checking for potential issues during their operation.Run policies are essential for ongoing security and compliance in the production environment, as they provide visibility into the actual state of resources and their activities1.

Run and Network policies (A) are indeed part of the configuration policy set, but they do not highlight the difference between build and run policies. Similarly, while Run policies do monitor network activities , this statement does not contrast them with Build policies.

Question 7

Question Type: MultipleChoice

What improves product operationalization by adding visibility into feature utilization and missed opportunities?

Options:

A- Adoption Advisor
B- Alarm Advisor
C- Alert Center
D- Alarm Center

Answer:

A

Explanation:

The Adoption Advisor is a feature within Prisma Cloud that aims to improve product operationalization. It provides visibility into how features are utilized, identifies unused capabilities, and suggests ways to leverage the full potential of the platform. Therefore, Option A: Adoption Advisor is the correct answer.