Free Questions for PCCSE by certsdeals

Shared by Marquez on 22-07-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

Which three Orchestrator types are supported when deploying Defender? (Choose three.)

Options:

A- Red Hat OpenShift

B- Amazon ECS

C- Docker Swarm

D- Azure ACS

E- Kubernetes

Answer:

A, B, E

Explanation:

Kubernetes, Openshift, ECS https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin-compute/install/deploy-defender/orchestrator

Prisma Cloud supports integration with multiple orchestrators to facilitate the deployment of its Defender component in various environments. The supported orchestrators include Red Hat OpenShift, Amazon ECS, and Kubernetes. These platforms are supported because they provide robust environments for container orchestration, allowing Prisma Cloud to efficiently manage security operations across different cloud-native technologies.

Question 2

Question Type: **MultipleChoice**

Which serverless cloud provider is covered by the "overly permissive service access" compliance check?

Options:

A- Alibaba

B- Azure

C- Amazon Web Services (AWS)

D- Google Cloud Platform (GCP)

Answer:

C

Explanation:

The 'overly permissive service access' compliance check is specifically designed to evaluate and ensure that cloud services are not granted more permissions than necessary, which could lead to potential security risks. Among the listed options, Amazon Web Services (AWS) is known for its extensive service offerings and the complexity of its Identity and Access Management (IAM) configurations. Prisma Cloud, a comprehensive cloud security platform by Palo Alto Networks, provides extensive support for AWS, including checks for overly permissive service access. This ensures that AWS environments adhere to the principle of least privilege, reducing the attack surface by limiting access to the minimum necessary to perform required tasks. Prisma Cloud's capabilities in AWS environments are detailed in various resources, including documentation and guides provided by Palo Alto Networks, which highlight its effectiveness in identifying and mitigating risks associated with excessive permissions in AWS services.

Question 3

Question Type: **MultipleChoice**

Which step should a SecOps engineer implement in order to create a network exposure policy that identifies instances accessible from any untrusted internet sources?

Options:

A- In Policy Section-> Add Policy-> Config type -> Define Policy details Like Name,Severity-> Configure RQL query 'config from network where source.network = UNTRUSTJNTERNET and dest.resource.type = 'Instance' and dest.cloud.type = 'AWS*' -> define compliance standard -> Define recommendation for remediation & save.

B- In Policy Section-> Add Policy-> Network type -> Define Policy details Like Name.Severity-> Configure RQL query 'network from vpc.flow_record where source.publicnetwork IN ('Suspicious IPs', 'Internet IPs') and dest.resource IN (resource where role IN ('Instance))' -> define compliance standard -> Define recommendation for remediation & save.

C- In Policy Section-> Add Policy-> Network type -> Define Policy details Like Name.Severity-> Configure RQL query 'network from vpc.flow_record where source.publicnetwork IN ('Suspicious IPs', 'Internet IPs') and dest.resource IN (resource where role IN (Instance))' -> define compliance standard -> Define recommendation for remediation & save.

D- In Policy Section-> Add Policy-> Network type -> Define Policy details Like Name.Severity-> Configure RQL query 'config from network where source.network = UNTRUSTJNTERNET and dest.resource.type = 'Instance' and dest.cloud.type = 'AWS'' -> Define recommendation for remediation & save.

Answer:

A

Explanation:

To create a network exposure policy that identifies instances accessible from any untrusted internet sources, a SecOps engineer would need to navigate to the Policy section within Prisma Cloud and add a new policy of the Config type. They would define the details of the policy such as the name and severity level and then configure the RQL query to specify conditions that match instances accessible from untrusted internet sources. The RQL query provided in the answer specifies that the source of the network traffic should be from an untrusted internet and that the destination resource should be an instance in the AWS cloud. After defining the compliance standards and providing recommendations for remediation, the policy can be saved to be enforced within the environment.

Question 4

Question Type: MultipleChoice

Which two elements are included in the audit trail section of the asset detail view? (Choose two).

Options:

A- Configuration changes

B- Findings

C- Overview

D- Alert and vulnerability events

Answer:

A, D

Explanation:

The audit trail section of an asset's detail view in Prisma Cloud typically includes a log of configuration changes and alert and vulnerability events associated with the asset. These elements are crucial for tracking the history of modifications to an asset's configuration and the security incidents that have affected it. This information is instrumental in understanding the security posture of the asset over time and in conducting thorough investigations after a security event has been detected.

Question 5

Question Type: MultipleChoice

Taking which action will automatically enable all severity levels?

Options:

A- Navigate to Settings > Enterprise Settings and enable all severity levels in the alarm center.

B- Navigate to Policies > Settings and enable all severity levels in the alarm center.

C- Navigate to Settings > Enterprise Settings and ensure all severity levels are checked under 'auto-enable default policies.

D- Navigate to Policies > Settings and ensure all severity levels are checked under 'auto-enable default policies.

Answer:

D

Explanation:

In Prisma Cloud, to automatically enable all severity levels for alerts, a user would need to navigate to the Policies section, then to Settings. Within this area, there is an option for 'auto-enable default policies,' which, when checked for all severity levels, ensures that any default policies related to those severities are automatically activated. This is a configuration setting that streamlines the alerting process by ensuring that all relevant severity levels are covered by the default policies without the need for manual intervention.

https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin/prisma-cloud-policies/manage-prisma-cloud-policies

Step 1- To enable global settings for Prisma Cloud default policies click 'Settings' and select 'Enterprise Settings' Step 2- To enable policies based on severity, select Auto enable new default policies of the type---Critical, High, Medium, Low or Informational.

Question 6

Question Type: MultipleChoice

Which two information types cannot be seen in the data security dashboard? (Choose two).

Options:

A- Bucket owner

B- Object Data Profile by Region

C- Top Publicly Exposed Objects By Data Profile

D- Object content

E- Total objects

Answer:

A, D

Explanation:

The data security dashboard in Prisma Cloud provides a comprehensive overview of the security posture related to cloud data storage. However, certain information types, such as the identity of the bucket owner and the actual content within an object, are not typically displayed on such dashboards. This is because the dashboard focuses more on aggregated data profiles, exposure levels, and compliance-related information rather than individual ownership details or the specific content of objects, which may require separate

detailed analysis or are managed through different security mechanisms.

Question 7

Question Type: MultipleChoice

Which ROL query is used to detect certain high-risk activities executed by a root user in AWS?

Options:

A- event from cloud.audit_logs where operation IN ('ChangePassword', 'ConsoleLogin', 'DeactivateMFADevice', 'DeleteAccessKey' , 'DeleteAlarms') AND user = 'root'

B- event from cloud.security_logs where operation IN ('ChangePassword', 'ConsoleLogin', 'DeactivateMFADevice', 'DeleteAccessKey' , 'DeleteAlarms') AND user = 'root'

C- config from cloud.audit_logs where operation IN ('ChangePassword', 'ConsoleLogin', 'DeactivateMFADevice', 'DeleteAccessKey', 'DeleteAlarms') AND user = 'root'

D- event from cloud.audit_logs where Risk.Level = 'high' AND user = 'root'

Answer:

A

Explanation:

https://docs.prismacloud.io/en/classic/rql-reference/rql-reference/event-query/event-query-examples

https://docs.prismacloud.io/en/classic/rql-reference/rql-reference/event-query/event-query-examples#idda895fd2-4496-4b31-9766-7d50215dcc18