Free Questions for PCCSE by certsdeals

Shared by Mcintosh on 24-05-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: **MultipleChoice**

Which IAM RQL query would correctly generate an output to view users who enabled console access with both access keys and passwords?

Options:

A- config from network where api.name = 'aws-iam-get-credential-report' AND json.rule = cert_1_active is true or cert_2_active is true and password_enabled equals 'true'

B- config from cloud.resource where api.name = 'aws-iam-get-credential-report' AND json.rule = access_key_1_active is true or access_key_2_active is true and password_enabled equals 'true'

C- config from cloud.resource where api.name = 'aws-iam-get-credential-report' AND json.rule = access_key_1_active is false or access_key_2_active is true and password_enabled equals '*'

D- config where api.name = 'aws-iam-get-credential-report' AND json.rule= access_key_1_active is true or access_key_2_active is true and password_enabled equals ''true''

Answer:

B

Explanation:

View users who enabled console access with both access keys and passwords: config from cloud.resource where api.name = 'aws-iam-get-credential-report' AND json.rule = access_key_1_active is true or access_key_2_active is true and password_enabled is true https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-rql-reference/rql-reference/config-query/config-query-examples

Question 2

Question Type: MultipleChoice

Which two CI/CD plugins are supported by Prisma Cloud as part of its Code Security? (Choose two.)

Options:

A- Checkov

B- Visual Studio Code

C- CircleCI

D- IntelliJ

Answer:

A, C

Explanation:

https://live.paloaltonetworks.com/t5/blogs/what-is-changing-for-ci-cd-plugins/ba-p/461676

Prisma Cloud has announced changes to its CI/CD plugins due to the acquisition of Bridgecrew1.The existing IaC functionality in Prisma Cloud will be replaced by a Prisma "cloud code security" (CCS) module that delivers Bridgecrew integration in Prisma Cloud1.As part of this change, several CI/CD plugins that Prisma Cloud currently uses will either be replaced or modified1.

According to the information from the link, bothCheckovandCircleCIare listed as integrations that will switch to the Prisma "cloud code security" (CCS) module1.Checkov is an open-source command-line interface (CLI) utility that includes more than 750 predefined policies and supports custom policies1.CircleCI is a continuous integration and continuous delivery platform1.

Question 3

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 4

Question Type: **MultipleChoice**

Which of the following is a reason for alert dismissal?

Options:

A- SNOOZED_AUTO_CLOSE

B- ALERT_RULE_ADDED

C- POLICY_UPDATED

D- USER_DELETED

Answer:

C

Explanation:

https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin/manage-prisma-cloud-alerts/prisma-cloud-alert-resolution-reasons

In Prisma Cloud,POLICY_UPDATEDis a valid reason for the dismissal of an alert. This reason indicates that an alert can be dismissed if the policy that triggered the alert has been updated. When a policy is updated to no longer apply to certain resources or conditions, any open alerts that were generated based on the previous version of the policy may be dismissed as they are no longer relevant.

The other options, such as SNOOZED_AUTO_CLOSE, ALERT_RULE_ADDED, and USER_DELETED, are not standard reasons for the dismissal of an alert in Prisma Cloud. SNOOZED_AUTO_CLOSE refers to the temporary suspension of an alert, ALERT_RULE_ADDED is related to the creation of a new alert rule, and USER_DELETED would pertain to the removal of a user account, not directly to alert dismissal.

Question 5

Question Type: MultipleChoice

Where can a user submit an external new feature request?

Options:

A- Aha

B- Help Center

C- Support Portal

D- Feature Request

Answer:

A

Explanation:

https://prismacloud.ideas.aha.io/ideas

To submit an external new feature request for Prisma Cloud, users can utilize theAhaplatform. By accessing the Palo Alto Networks Aha portal, users can submit their feature requests, suggest enhancements, and contribute to shaping the future of Prisma Cloud. Aha provides a structured way to collect and prioritize customer feedback, ensuring that valuable insights reach the product development teams.

For those seeking to propose new features or improvements, visiting the Aha portal and submitting their ideas is the recommended approach.It allows users to participate in the ongoing evolution of Prisma Cloud by sharing their requirements and vision for the platform

Question 6

Question Type: **MultipleChoice**

A customer's Security Operations Center (SOC) team wants to receive alerts from Prisma Cloud via email once a day about all policies that have a violation, rather than receiving an alert every time a new violation occurs.

Which alert rule configuration meets this requirement?

Options:

A- Configure an alert rule with all the defaults except selecting email within the 'Alert Notifications' tab and specifying recipient.

B- Configure an alert rule. Under the 'Policies' tab, select 'High Risk Severity Policies.' In the 'Set Alert Notifications' tab, select 'Email > Recurring,' set to repeat every 1 day, and enable 'Email.'

C- Set up email integrations under the 'Integrations' tab in 'Settings' and create a notification template.

D- Configure an alert rule. Under the 'Policies' tab, select 'All Policies.' In the 'Set Alert Notifications' tab, select 'Email > Recurring,' set to repeat every 1 day, and then enable 'Email.'

Answer:

D

Explanation:

To receive daily email alerts for all policy violations, the SOC team should configure an alert rule that encompasses all policies and sets the notification frequency to once per day. This can be achieved by:

Navigating to the "Policies" tab within the alert rule configuration and selecting "All Policies" to ensure that the rule applies to every policy.

Moving to the "Set Alert Notifications" tab and choosing the "Email" notification method.

Setting the notification to "Recurring" with a frequency of every 1 day.

Enabling the email notification by specifying the recipient's email address.

This configuration ensures that the SOC team will receive a consolidated email once a day that includes information on all policies that have been violated, rather than receiving multiple alerts throughout the day as new violations occur. It allows the team to review the compliance status efficiently and prioritize their response accordingly.

Question 7

Question Type: **MultipleChoice**

Which report includes an executive summary and a list of policy violations, including a page with details for each policy?

Options:

A- Compliance Standard

B- Business Unit

C- Cloud Security Assessment

D- Detailed

Answer:

C

Explanation:

The Cloud Security Assessment report is a PDF report that summarizes the risks from open alerts in the monitored cloud accounts for a specific cloud type. The report includes an executive summary and a list of policy violations, including a page with details for each policy that includes the description and the compliance standards that are associated with it, the number of resources that passed and failed the check within the specified time period. https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin/manage-prisma-cloud-alerts/generate-reports-on-prisma-cloud-alerts

The report that includes an executive summary along with a list of policy violations and detailed pages for each policy is the 'Cloud Security Assessment' report. This type of report is designed to provide organizations with a comprehensive overview of their cloud security posture, highlighting both compliance with security policies and areas needing attention.

Question 8

Question Type: MultipleChoice

Creation of a new custom compliance standard that is based on other individual custom compliance standards needs to be automated.

Assuming the necessary data from other standards has been collected, which API order should be used for this new compliance standard?

Options:

A- 1) https://api.prismacloud.io/compliance/add
2) https://api.prismacloud.io/compliance/requirementId/section
3) https://api.prismacloud.io/compliance/complianceId/requirement

B- 1) https://api.prismacloud.io/compliance
2) https://api.prismacloud.io/compliance/complianceId/requirement
3) https://api.prismacloud.io/compliance/requirementId/section

C- 1) https://api.prismacloud.io/compliance/add
2) https://api.prismacloud.io/compliance/complianceId/requirement
3) https://api.prismacloud.io/compliance/requirementId/section

D- 1) https://api.prismacloud.io/compliance
2) https://api.prismacloud.io/compliance/requirementId/section

3) https://api.prismacloud.io/compliance/complianceId/requirement

Answer:

B

Explanation:

https://api.prismacloud.io/compliance Add Compliance Standard https://api.prismacloud.io/compliance/complianceId/requirement Add Compliance Requirement https://api.prismacloud.io/compliance/requirementId/section Add Compliance Requirement Section https://pan.dev/prisma-cloud/api/cspm/get-all-standards/

Question 9

Question Type: MultipleChoice

Which three options for hardening a customer environment against misconfiguration are included in Prisma Cloud Compute compliance enforcement for hosts? (Choose three.)

Options:

A- Serverless functions

B- Docker daemon configuration

C- Cloud provider tags

D- Host configuration

E- Hosts without Defender agents

Answer:

B, D, E

Explanation:

Prisma Cloud scans all hosts for compliance issues, provided that a defender is installed or the host is covered by an agentless scan. Among these, the following compliance issues are covered.

-Host configuration

-Docker daemon configuration

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

Prisma Cloud Compute's compliance enforcement capabilities for hosts include ensuring proper configurations of Docker daemons and host operating systems, as well as managing hosts that do not have Defender agents installed. These measures are critical for hardening environments against misconfigurations which could lead to security vulnerabilities.