



Palo Alto Networks CloudSec-Pro Practice Questions

Shared by Garner on 17-08-2026

For More Free Questions and Preparation Resources

Check the Links on Last Page



Question 1

Question Type: MultipleChoice

Which three platforms support the twistcli tool? (Choose three.)

Options:

- A- Linux
- B- Windows
- C- Android
- D- MacOS
- E- Solaris



Answer:

A, B, D

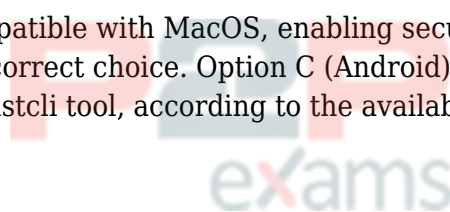
Explanation:

The twistcli tool, part of Prisma Cloud's suite of security tools, supports various platforms for security scanning and configuration. The correct platforms supported by twistcli include:

A . Linux: twistcli is widely used on Linux platforms for scanning container images, host vulnerabilities, and more, making it a correct choice.

B . Windows: twistcli supports Windows, allowing users to perform security scans and checks on Windows-based systems, making it a correct choice.

D . MacOS: twistcli is also compatible with MacOS, enabling security operations on Apple's operating system, making it a correct choice. Option C (Android) and E (Solaris) are not supported platforms for the twistcli tool, according to the available documentation on Prisma Cloud.



Question 2

Question Type: MultipleChoice

A customer has serverless functions that are deployed in multiple clouds.

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

Options:

- A- Alibaba
- B- GCP
- C- AWS
- D- Azure

Answer:

C

Explanation:

The serverless cloud provider covered by the "overly permissive service access" compliance check is AWS (Amazon Web Services). AWS Lambda, which is the serverless computing platform provided by AWS, may have functions that are assigned more permissions than they require to perform their operations, leading to security risks.

In the context of CSPM tools, such as Prisma Cloud, checks for overly permissive service access would typically include examining the policies attached to AWS Lambda functions to ensure that they adhere to the principle of least privilege. Such checks help identify and rectify overly broad permissions that could potentially be exploited by attackers.

The reference for this can be found in AWS best practices for Lambda security, which emphasize the importance of granting minimal privileges necessary for the Lambda function to perform its tasks, thereby reducing the potential attack surface.

Question 3

Question Type: MultipleChoice

The administrator wants to review the Console audit logs from within the Console.

Which page in the Console should the administrator use to review this data, if it can be reviewed at all?

Options:

- A- Navigate to Monitor > Events > Host Log Inspection
- B- The audit logs can be viewed only externally to the Console
- C- Navigate to Manage > Defenders > View Logs

D- Navigate to Manage > View Logs > History

Answer:

D

Explanation:

https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin-compute/audit/audit_admin_activity



Question 4

Question Type: MultipleChoice

What factor is not used in calculating the net effective permissions for a resource in AWS?

Options:

- A- AWS IAM policy
- B- Permission boundaries
- C- IPTables firewall rule
- D- AWS service control policies (SCPs)

Answer:

C



Explanation:

In the context of calculating net effective permissions for a resource in AWS, IPTables firewall rule is not used. Net effective permissions in AWS are determined by evaluating various AWS-specific mechanisms such as IAM policies, permission boundaries, and service control policies (SCPs). IAM policies define what actions are allowed or denied for various AWS resources. Permission boundaries provide a way to delegate administration for IAM entities, setting the maximum permissions that an IAM entity can have. SCPs are part of AWS Organizations and allow for central control over the maximum available permissions for all accounts within an organization. IPTables, on the other hand, is a Linux-based application for setting up firewall rules on individual hosts and is not directly related to AWS resource permissions. Therefore, IPTables firewall rules are not considered when calculating net effective permissions in AWS, making option C the correct answer.

Question 5

Question Type: MultipleChoice

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

Options:

- A- twistcli
- B- Jenkins Docker plugin
- C- Compute Jenkins plugin
- D- Compute Azure DevOps plugin
- E- Prisma Cloud Visual Studio Code plugin with Jenkins integration

Answer:

A, C

Explanation:

To scan container images in Jenkins pipelines, two effective methods are using twistcli and the Compute Jenkins plugin. twistcli is a command-line tool provided by Prisma Cloud that allows for the scanning of container images for vulnerabilities and compliance issues directly from the CI/CD pipeline. It can be integrated into Jenkins jobs as a build or post-build step to automatically scan images as part of the build process.

The Compute Jenkins plugin is specifically designed for integration with Jenkins, providing a more seamless and automated way to include Prisma Cloud's security scanning capabilities within Jenkins pipelines. This plugin enables Jenkins to trigger image scans with Prisma Cloud directly and can fail builds based on scan results, ensuring that only secure and compliant images are pushed through the CI/CD pipeline.

Both twistcli and the Compute Jenkins plugin are designed to integrate Prisma Cloud's security capabilities into the CI/CD process, enabling DevOps teams to identify and fix security issues early in the development lifecycle.

Question 6

Question Type: MultipleChoice

A customer wants to scan a serverless function as part of a build process. Which twistcli command can be used to scan serverless functions?

Options:

- A- twistcli function scan <SERVERLESS_FUNCTION.ZIP>
- B- twistcli scan serverless <SERVERLESS_FUNCTION.ZIP>
- C- twistcli serverless AWS <SERVERLESS_FUNCTION.ZIP>
- D- twistcli serverless scan <SERVERLESS_FUNCTION.ZIP>

Answer:

D

Explanation:

https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin-compute/vulnerability_management/serverless_functions You can also use the twistcli command line utility to scan your serverless functions. First download your serverless function as a ZIP file, then run: \$ twistcli serverless scan <SERVERLESS_FUNCTION.ZIP>

Question 7

Question Type: MultipleChoice

Which option best are correct statements regarding the use of access keys? (Select two.)

Options:

- A- Access keys must have an expiration date
- B- Up to two access keys can be active at any time
- C- System Admin can create access key for all users
- D- Access keys are used for API calls

Answer:

B, D

Explanation:

Regarding the use of access keys, it is correct that up to two access keys can be active at any time for a single IAM user in AWS, and access keys are used for programmatic API calls to AWS services. This allows for rotation of keys without immediate invalidation of the old key and ensures secure access to AWS services via APIs.

Question 8

Question Type: MultipleChoice

When configuring SSO how many IdP providers can be enabled for all the cloud accounts monitored by Prisma Cloud?

Options:

- A- 2
- B- 4
- C- 1
- D- 3

Answer:

C

Explanation:

Prisma Cloud supports configuring Single Sign-On (SSO) with Identity Providers (IdPs) to streamline user authentication processes. However, for all the cloud accounts monitored by Prisma Cloud, only one IdP provider can be enabled at any given time. This limitation ensures a unified authentication mechanism across the platform, reducing complexity and potential security risks associated with managing multiple IdP configurations.

Question 9

Question Type: MultipleChoice

Which two fields are required to configure SSO in Prisma Cloud? (Choose two.)

Options:

- A- Prisma Cloud Access SAML URL
- B- Identity Provider Issuer
- C- Certificate
- D- Identity Provider Logout URL

Answer:

B, C

Explanation:

Configuring Single Sign-On (SSO) in Prisma Cloud requires the Identity Provider Issuer (Option B) and Certificate (Option C). The Identity Provider Issuer is a unique identifier for the SSO identity provider and is used by Prisma Cloud to establish trust and validate SSO responses. The Certificate, typically an X.509 certificate, is used to sign SSO assertions and ensure the security of the SSO communication. The Prisma Cloud Access SAML URL (Option A) is provided by Prisma Cloud to configure the SSO on the identity provider's side, not the other way around. The Identity Provider Logout URL (Option D) is used for single logout configurations but is not a required field for basic SSO configuration in Prisma Cloud.



To Get Premium Files for CloudSec-Pro Visit

<https://www.p2pexams.com/products/cloudsec-pro>

For More Free Questions Visit

<https://www.p2pexams.com/palo-alto-networks/pdf/cloudsec-pro>

20%
DISCOUNT

P2P
exams