# Free Questions for PCCSE by ebraindumps

## Shared by Branch on 15-04-2024

**For More Free Questions and Preparation Resources**

**Check the Links on Last Page**

# Question 1

**Question Type:** MultipleChoice

What should be used to associate Prisma Cloud policies with compliance frameworks?

## Options:

**A-** Compliance

**B-** Custom compliance

**C-** Alert rules

**D-** Policies

## Answer:

B

## Explanation:

In the context of associating Prisma Cloud policies with compliance frameworks, the most appropriate option is 'Custom compliance.' Prisma Cloud provides a comprehensive set of security and compliance policies that can be applied to cloud environments. While predefined policies cover a wide range of compliance standards and best practices, every organization has unique requirements and

may follow specific compliance frameworks that are not directly included in the predefined policies. Custom compliance allows organizations to define their own compliance frameworks and associate specific Prisma Cloud policies with these custom frameworks. This flexibility ensures that organizations can maintain compliance with their specific regulatory and industry standards, tailoring the Prisma Cloud policies to meet their unique compliance needs. Custom compliance frameworks can be created within Prisma Cloud to include a collection of policies that address the specific controls and requirements of the organization's chosen compliance standards, providing a tailored approach to cloud security and compliance.

# Question 2

**Question Type:** **MultipleChoice**

Which two offerings will scan container images in Jenkins pipelines? (Choose two.)

## Options:

**A-** Compute Azure DevOps plugin

**B-** Prisma Cloud Visual Studio Code plugin with Jenkins integration

**C-** Jenkins Docker plugin

**D-** Twistcli

**E-** Compute Jenkins plugin

### Answer:

A, D

### Explanation:

To integrate security scanning within Jenkins pipelines for container images, the most appropriate tools are the Compute Azure DevOps plugin and Twistcli. The Compute Azure DevOps plugin is designed to integrate with CI/CD workflows, allowing automated security scanning of container images as part of the build process in Azure DevOps environments. This plugin can be used in conjunction with Jenkins pipelines through integration points or scripting to trigger scans during the build or deployment stages. Twistcli, on the other hand, is a command-line interface tool provided by Prisma Cloud (formerly Twistlock) that allows for scanning of container images for vulnerabilities and compliance issues. Twistcli can be directly integrated into Jenkins pipelines using shell scripts or pipeline commands to perform security scans on container images before they are deployed. This ensures that only secure and compliant container images are used in production environments, aligning with DevSecOps practices.

## Question 3

**Question Type:** **MultipleChoice**

Which ban for DoS protection will enforce a rate limit for users who are unable to post five (5) ". tar.gz" files within five (5) seconds?

## Options:

**A-** One with an average rate of 5 and file extensions match on ". tar.gz' on Web Application and API Security (WAAS)

**B-** One with an average rate of 5 and file extensions match on ". tar.gz' on Cloud Native Network Firewall (CNNF)

**C-** One with a burst rate of 5 and file extensions match on ". tar.gz' on Web Application and API Security (WAAS) *

**D-** One with a burst rate of 5 and file extensions match on ". tar.gz' on Cloud Native Network Firewall (CNNF)

## Answer:

A

## Explanation:

In the context of DoS protection, enforcing a rate limit is a common strategy to prevent abuse and ensure service availability. The scenario described involves limiting the rate at which users can post '.tar.gz' files to five within five seconds. The correct ban configuration for this requirement would be one that specifies an average rate of 5 with a file extension match on ".tar.gz' within the Web Application and API Security (WAAS) component of a security solution like Prisma Cloud. WAAS is designed to protect web applications and APIs from various threats, including DoS attacks, by applying policies that can limit actions based on specific criteria, such as file types and request rates. This configuration ensures that any attempt to upload more than five '.tar.gz' files within a five-second window would be detected and blocked, mitigating the risk of DoS attacks targeting this particular file upload functionality.

# Question 4

**Question Type:** MultipleChoice

Which two integrated development environment (IDE) plugins are supported by Prisma Cloud as part of its Code Security? (Choose two.)

## Options:

**A-** Visual Studio Code

**B-** IntelliJ

**C-** BitBucket

**D-** CircleCI

## Answer:

A, B

## Explanation:

Prisma Cloud by Palo Alto Networks extends its cloud security capabilities to the development environment through the integration with Integrated Development Environments (IDEs) plugins. Among the available options, Visual Studio Code and IntelliJ are supported by Prisma Cloud as part of its Code Security features. These IDE plugins enable developers to incorporate security insights directly into

their development workflows, facilitating early detection and remediation of vulnerabilities and compliance issues in the codebase. Visual Studio Code, known for its versatility and extensive plugin ecosystem, and IntelliJ, popular for its powerful coding assistance and ergonomic design, are both widely used by developers. The integration with Prisma Cloud allows for seamless scanning of code for vulnerabilities, misconfigurations, and compliance with security policies, fostering a DevSecOps culture by shifting security left into the early stages of the development lifecycle.

# Question 5

**Question Type:** **MultipleChoice**

Which set of steps is the correct process for obtaining Console images for Prisma Cloud Compute Edition?

## Options:

**A-** To retrieve Prisma Cloud Console images using basic authentication:
1. Access registry.twistlock.com and authenticate using 'docker login.'
2. Retrieve the Prisma Cloud Console images using 'docker pull.'

**B-** To retrieve Prisma Cloud Console images using URL authentication:
1. Access registry-url-auth.twistlock.com and authenticate using the user certificate.
2. Retrieve the Prisma Cloud Console images using 'docker pull.'

**C-** To retrieve Prisma Cloud Console images using URL authentication:

1. Access registry-auth.twistlock.com and authenticate using the user certificate.
2. Retrieve the Prisma Cloud Console images using 'docker pull.'

**D-** To retrieve Prisma Cloud Console images using basic authentication:

1. Access registry.paloaltonetworks.com and authenticate using 'docker login.'
2. Retrieve the Prisma Cloud Console images using 'docker pull.'

## Answer:

D

## Explanation:

Prisma Cloud, part of Palo Alto Networks' cloud security suite, offers Console images that can be retrieved for deployment in various environments. The correct process for obtaining these images involves using basic authentication with Docker, a widely-used containerization platform. Users must first access the official Palo Alto Networks registry at registry.paloaltonetworks.com. Here, they are required to authenticate using the 'docker login' command, which prompts for credentials. Upon successful authentication, users can then use the 'docker pull' command to retrieve the Prisma Cloud Console images. This method ensures secure access to the latest Console images for deployment within an organization's infrastructure, aligning with best practices for container image management and deployment.

# Question 6

**Question Type:** MultipleChoice

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

## Options:

**A-** AWS 1AM 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 7

**Question Type:** **MultipleChoice**

Prisma Cloud supports sending audit event records to which three targets? (Choose three.)

## Options:

**A-** SNMP Traps

**B-** Stdout

**C-** Netflow

**D-** Prometheus

**E-** Syslog

## Answer:

A, D, E

## Explanation:

Prisma Cloud, a comprehensive cloud security solution by Palo Alto Networks, is designed to provide extensive monitoring and auditing capabilities across cloud environments. To facilitate real-time alerting and integration with external monitoring and management systems, Prisma Cloud supports sending audit event records to various targets. SNMP Traps, Prometheus, and Syslog are among the supported targets. SNMP Traps allow for the integration with network management systems, enabling real-time alerts for network administrators. Prometheus, a popular open-source monitoring and alerting toolkit, is widely used for its powerful querying language and visualization capabilities, making it an ideal target for Prisma Cloud's detailed security metrics. Syslog support ensures compatibility with a broad range of logging and security information and event management (SIEM) systems, allowing organizations to centralize and analyze security alerts within their existing infrastructure. These integrations are crucial for ensuring that security teams can respond promptly to potential threats and maintain compliance across their cloud environments.

# Question 8

**Question Type:** MultipleChoice

Console is running in a Kubernetes cluster, and Defenders need to be deployed on nodes within this cluster.

How should the Defenders in Kubernetes be deployed using the default Console service name?

## Options:

**A-** From the deployment page in Console, choose 'twistlock-console' for Console identifier, generate DaemonSet file, and apply DaemonSet to the twistlock namespace.

**B-** From the deployment page, configure the cloud credential in Console and allow cloud discovery to auto-protect the Kubernetes nodes.

**C-** From the deployment page in Console, choose 'twistlock-console' for Console identifier and run the 'curl | bash' script on the master Kubernetes node.

**D-** From the deployment page in Console, choose 'pod name' for Console identifier, generate DaemonSet file, and apply the DaemonSet to twistlock namespace.

## Answer:

A

## Explanation:

In Kubernetes environments, deploying Defenders to protect nodes involves leveraging DaemonSets, which ensure that every node in the cluster runs a copy of a specific pod. When the Console is running within a Kubernetes cluster, it's essential to correctly reference the Console service to ensure seamless communication between Defenders and the Console. Option A is the most straightforward and Kubernetes-native method for deploying Defenders. By choosing 'twistlock-console' as the Console identifier on the deployment page within the Console, users can generate a DaemonSet configuration file tailored for the Twistlock namespace. This approach ensures that

the Defenders are correctly configured to communicate with the Console, providing comprehensive security coverage across the Kubernetes nodes. This method aligns with best practices for deploying security agents in Kubernetes and is supported by Prisma Cloud (formerly Twistlock) documentation, which provides step-by-step instructions for deploying Defenders using DaemonSets.