DUMPSBOSS.

Palo Alto Networks Cloud Security Professional

Palo Alto Networks CloudSec-Pro

Version Demo

Total Demo Questions: 28

Total Premium Questions: 288

Buy Premium PDF

https://dumpsboss.co

support@dumpsboss.co

support@dumpsboss.co
dumpsboss.co

Topic Break Down

Topic	No. of Questions
Topic 1, Prisma Cloud Overview and Architecture	53
Topic 2, Cloud Security	56
Topic 3, Application Security	40
Topic 4, Runtime Security	69
Topic 5, Security Operations	67
Topic 6, Mix Questions	3
Total	288

QUESTION NO: 1 - (SIMULATION)

What is the order of steps to create a custom network policy?

(Drag the steps into the correct order of occurrence, from the first step to the last.)

ANSWER: See the explanation for the answer

Explanation:

Correct order:

1. Go to **Policies** and select **Add Policy**.
2. Select **Network** as the policy type.
3. Enter the policy details, such as the policy name, description, severity, and labels.
4. Select the applicable cloud type/account scope and define the network **RQL** query/rule criteria.
5. Associate any required compliance standards or metadata, then select **Save** to create the custom network policy.

In short: `Policies > Add Policy → Network type → Policy details → Network RQL/rule scope → Save.`

QUESTION NO: 2

What is the correct method for ensuring key-sensitive data related to SSNs and credit card numbers cannot be viewed in Dashboard > Data view during investigations?

A. Go to Settings > Data > Snippet Masking and select Full Mask.

B. Go to Settings > Data > Data Patterns, search for SSN Pattern, edit it, and modify the proximity keywords.

C. Go to Settings > Cloud Accounts > Edit Cloud Account > Assign Account Group and select a group with limited permissions.

D. Go to Policies > Data > Clone > Modify Objects containing Financial Information publicly exposed and change the file exposure to Private.

ANSWER: A

Explanation:

Go to Settings > Data > Snippet Masking and select Full Mask. Snippet masking controls how discovered sensitive values are displayed in Prisma Cloud Data Security investigation results, including the Dashboard > Data view. Selecting Full Mask prevents investigators from seeing the actual matched content in snippets, so values such as Social Security numbers and credit card numbers are obfuscated rather than exposed during routine investigation workflows. This control is especially important when the individuals reviewing alerts need enough context to assess the finding but do not have a business requirement to view regulated personal or payment-card data. Applying full masking supports least-privilege access to sensitive content while preserving the data-security finding, its classification, and the surrounding investigation context. It therefore reduces unnecessary disclosure of sensitive values and helps organizations align operational investigations with privacy and data-protection requirements. Palo Alto Networks documents Data Security configuration and investigation capabilities in its Prisma Cloud Data Security documentation and provides additional platform-administration guidance in the Prisma Cloud Administrator's Guide.

QUESTION NO: 3

What are the three states of the Container Runtime Model? (Choose three.)

A. Initiating

B. Learning

C. Active

D. Running

E. Archived

ANSWER: B C E

Explanation:

The three Container Runtime Model states are **Learning**, **Active**, and **Archived**. Prisma Cloud Compute creates a runtime model from observed container behavior, including processes, network activity, and related runtime characteristics. In the Learning state, Prisma Cloud is collecting and baselining the workload's normal behavior. Once the model has sufficient information and is being used to evaluate runtime activity, it is Active. This provides the behavioral context used by runtime protection capabilities to identify activity that does not match the learned model. When the underlying container is no longer running, its model moves to Archived so the historical model remains available for review rather than being treated as an active workload. These state transitions accommodate the short-lived and dynamic nature of containers while preserving useful historical runtime context. Palo Alto Networks documents container runtime modeling and its lifecycle as part of Prisma Cloud Compute runtime defense. See the Prisma Cloud Compute container models documentation and the runtime defense for containers documentation.

QUESTION NO: 4

A customer has a requirement to restrict any container from resolving the name www.evil-url.com.

How should the administrator configure Prisma Cloud Compute to satisfy this requirement?

A. Choose "copy into rule" for any Container, set www.evil-url.com as a blocklisted DNS name in the Container policy and set the policy effect to alert.

B. Set www.evil-url.com as a blocklisted DNS name in the default Container runtime policy, and set the effect to block.

C. Choose "copy into rule" for any Container, set www.evil-url.com as a blocklisted DNS name, and set the effect to prevent.

D. Set www.evil-url.com as a blocklisted DNS name in the default Container policy and set the effect to prevent.

ANSWER: D

Explanation:

Set www.evil-url.com as a blocklisted DNS name in the default Container policy and set the effect to prevent. The default Container runtime policy provides the baseline runtime-defense behavior for containers that do not match a more-specific rule, making it the appropriate policy location when the requirement applies broadly to any container. Adding the fully qualified DNS name to the blocklist defines the prohibited destination name at DNS-resolution time rather than relying on a network URL filter. Setting the rule effect to prevent enables enforcement: Prisma Cloud Compute blocks the protected runtime activity when a container attempts to resolve the listed name. This combination therefore implements an active DNS control that stops containers from obtaining an address for the prohibited domain and helps prevent subsequent communication with it. Prisma Cloud Compute runtime-defense policies support policy effects that distinguish detection-only behavior from preventive enforcement, and DNS controls are part of the container runtime-defense configuration. See the Prisma Cloud Compute Runtime Defense for Containers documentation and the Prisma Cloud documentation portal for runtime policy configuration details.

QUESTION NO: 5

Which two processes ensure that builds can function after a Console upgrade? (Choose two.)

A. allowing Jenkins to automatically update the plugin

B. updating any build environments that have twistcli included to use the latest version

C. configuring build pipelines to download twistcli at the start of each build

D. creating a new policy that allows older versions of twistcli to connect the Console

ANSWER: B C

Explanation:

Updating any build environments that have twistcli included to use the latest version ensures that the CLI embedded, cached, or otherwise maintained in those environments remains aligned with the upgraded Prisma Cloud Compute Console. Build pipelines use `twistcli` to perform tasks such as image and IaC scanning and to send results to Console. Refreshing the binary as part of the Console-upgrade process preserves the expected compatibility and ensures builds use the capabilities, checks, and API behavior delivered by the current Console release.

Configuring build pipelines to download twistcli at the start of each build is an operationally stronger way to accomplish the same outcome continuously. Rather than relying on a manually maintained CLI binary in every CI worker or build image, the pipeline retrieves the Console-provided/current `twistcli` before running scan commands. This prevents stale tooling from persisting across Console upgrades and makes new or ephemeral runners behave consistently with long-lived runners. Palo Alto Networks documents downloading `twistcli` from Console for CI/CD integration and identifies it as the command-line utility used to scan artifacts in build workflows. See the Prisma Cloud Compute CI/CD documentation and the Prisma Cloud Compute upgrade guidance.

QUESTION NO: 6

Which component(s), if any, will Palo Alto Networks host and run when a customer purchases Prisma Cloud Enterprise Edition?

A. Defenders

B. Console

C. Jenkins

D. twistcli

ANSWER: B

Explanation:

Console is correct. Prisma Cloud Enterprise Edition provides the Prisma Cloud Compute Console as a Palo Alto Networks-hosted SaaS service. The Console is the centralized control plane for Prisma Cloud Compute: it supplies the web interface and API used to configure security policies, manage compliance and runtime settings, review vulnerabilities and alerts, and administer Compute deployments. Because Palo Alto Networks operates this Console in the Enterprise Edition service, the customer accesses it through their Prisma Cloud tenant rather than installing, maintaining, upgrading, and operating the Console infrastructure themselves. This hosted-management model lets customers focus on connecting cloud environments and deploying the relevant workload-protection coverage while Palo Alto Networks manages the availability and lifecycle of the Console service. Palo Alto Networks documentation describes Prisma Cloud Compute as using Console for centralized administration and identifies the SaaS/Enterprise offering as the Palo Alto Networks-managed deployment model. See the Prisma Cloud Compute getting-started documentation and the Prisma Cloud Compute documentation for the Console's role and deployment guidance.

QUESTION NO: 7

A customer is deploying Defenders to a Fargate environment. It wants to understand the vulnerabilities in the image it is deploying.

How should the customer automate vulnerability scanning for images deployed to Fargate?

A. Set up a vulnerability scanner on the registry

B. Embed a Fargate Defender to automatically scan for vulnerabilities

C. Designate a Fargate Defender to serve a dedicated image scanner

D. Use Cloud Compliance to identify misconfigured AWS accounts

ANSWER: A

Explanation:

Set up a vulnerability scanner on the registry is correct because vulnerability assessment is most effective before an image is deployed as an Amazon ECS Fargate task. Prisma Cloud Compute can scan container images held in supported registries, identifying operating-system and application dependency vulnerabilities from the image contents and associated package metadata. This gives the customer continuous visibility into newly discovered vulnerabilities affecting images already stored in the registry, as well as images introduced through the delivery pipeline.

For Fargate workloads, Defenders provide runtime protection and visibility for running tasks, but the image-vulnerability posture should be established through registry scanning and enforced before deployment. The customer can connect the registry to Prisma Cloud Compute, define scan coverage and alerting policies, and use the resulting vulnerability findings to remediate, gate, or otherwise control images before they are used by Fargate services. This separation supports a shift-left workflow: image risk is evaluated at the registry stage, while runtime protection remains available once the workload starts. Palo Alto Networks documents registry scanning and its image-vulnerability reporting capabilities in the Registry Scan documentation and describes container image scanning in the Vulnerability Management documentation.

QUESTION NO: 8

Which method should be used to authenticate to Prisma Cloud Enterprise programmatically?

A. single sign-on

B. SAML

C. basic authentication

D. access key

ANSWER: D

Explanation:

access key is the appropriate method for programmatic authentication to Prisma Cloud Enterprise. Prisma Cloud API integrations use a dedicated access key and associated secret key to obtain a short-lived JSON Web Token (JWT) from the authentication endpoint. The integration then includes that token in subsequent API requests, allowing automation to interact securely with Prisma Cloud services without requiring an interactive user sign-in. This model is designed for scripts, CI/CD pipelines, security orchestration platforms, and other non-human workloads. Access keys can be created and managed within Prisma Cloud, enabling organizations to scope, rotate, and revoke programmatic credentials as part of their operational security practices. Using dedicated machine credentials also provides clearer auditability than sharing an individual user's login. Palo Alto Networks documents the access-key workflow and token retrieval process in its Prisma Cloud API documentation: Prisma Cloud API access keys. For authentication endpoint details and the required request format, see Prisma Cloud API URLs.

QUESTION NO: 9

How are the following categorized?

Backdoor account access Hijacked processes Lateral movement

Port scanning

A. audits

B. incidents

C. admission controllers

D. models

ANSWER: D

Explanation:

models is correct. In Prisma Cloud Compute runtime protection, these named detections are behavioral models: predefined analytic detections that identify runtime activity patterns associated with potentially malicious behavior. Backdoor account access identifies activity consistent with establishing or using unauthorized persistence; hijacked processes identifies indications that a running process has been compromised or manipulated; lateral movement identifies behavior associated with movement between workloads or systems; and port scanning identifies reconnaissance-style network activity. The model evaluates observed runtime telemetry, such as process execution and network connections, against its detection logic and can generate a security finding when the modeled behavior is observed. This model-based approach enables Prisma Cloud to identify meaningful attack techniques rather than merely presenting isolated low-level events. Security teams can then investigate the associated runtime evidence and respond according to the workload's context and risk. Palo Alto Networks documents Prisma Cloud Compute as its workload-protection capability, including runtime defense and monitoring functions, in the Prisma Cloud Compute Administration documentation. Additional product documentation and runtime-security guidance are available through the Prisma Cloud documentation portal.

QUESTION NO: 10

A customer has a requirement to scan serverless functions for vulnerabilities.

Which three settings are required to configure serverless scanning? (Choose three.)

A. Defender Name

B. Region

C. Credential

D. Console Address

E. Provider

ANSWER: B C E

Explanation:

Serverless vulnerability scanning must be configured with the cloud context and access details necessary to discover and retrieve function artifacts. **Provider** identifies the cloud environment that hosts the functions and determines the applicable integration workflow. **Region** scopes discovery to the cloud region in which the functions are deployed, allowing Prisma Cloud Compute to locate the relevant serverless resources. **Credential** supplies the authorized cloud-account access required to enumerate functions and obtain the deployment packages, layers, or container images that must be assessed for vulnerabilities. Together, these settings establish the provider-specific target, the deployment location, and authenticated API access needed for a successful serverless scan. This configuration supports Prisma Cloud Compute's serverless protection capabilities, which include visibility into vulnerabilities associated with deployed cloud functions. Palo Alto Networks documents Prisma Cloud Compute administration and its workload-protection configuration in the Prisma Cloud Compute Administration documentation and provides product documentation resources through the Prisma Cloud documentation portal.

QUESTION NO: 11

A customer does not want alerts to be generated from network traffic that originates from trusted internal networks.

Which setting should you use to meet this customer's request?

A. Trusted Login IP Addresses

B. Anomaly Trusted List

C. Trusted Alert IP Addresses

D. Enterprise Alert Disposition

ANSWER: C

Explanation:

Trusted Alert IP Addresses is the appropriate setting because it identifies source IP addresses or network ranges that Prisma Cloud should treat as trusted when evaluating network-traffic alert activity. Adding the organization's trusted internal network addresses to this setting suppresses alert generation for traffic originating from those sources, which directly satisfies the requirement to avoid alerts from known internal networks. This configuration is intended for reducing expected, non-actionable alert volume while retaining alerting for activity from sources that are not explicitly trusted. The entries should be limited to verified internal address ranges and reviewed when network architecture changes, so that the suppression scope remains aligned with the organization's trusted-network boundaries. Palo Alto Networks documents trusted alert IP address configuration as part of managing alert behavior and recommends using the platform's alert-management settings to tune expected activity without changing the underlying visibility of the environment. See the Prisma Cloud alert management documentation and the Prisma Cloud anomaly policy documentation for the related alerting and anomaly configuration model.

QUESTION NO: 12

Which two attributes of policies can be fetched using API? (Choose two.)

A. policy label

B. policy signature

C. policy mode

D. policy violation

ANSWER: A C

Explanation:

policy label and **policy mode** are attributes available when retrieving Prisma Cloud policy definitions through the API. Labels are policy metadata used to organize, classify, and manage policies, including custom labels that help teams identify policies by ownership, framework, environment, or operational purpose. This makes labels useful for API-driven inventory, reporting, and policy-management workflows.

Policy mode is also returned as part of the policy definition. It identifies the policy's operating mode, such as whether it follows the Prisma Cloud default mode or a user-defined mode. Retrieving this value enables automation to accurately understand and preserve how a policy is configured when policies are audited, exported, compared, or updated programmatically. Prisma Cloud's policy API exposes policy-definition metadata—including labels and policy mode—rather than limiting results to a policy name or identifier. See the official Prisma Cloud Policies API reference and the Prisma Cloud Policy API documentation for policy retrieval details and response fields.

QUESTION NO: 13

If you are required to run in an air-gapped environment, which product should you install?

A. Prisma Cloud Jenkins Plugin

B. Prisma Cloud Compute Edition

C. Prisma Cloud with self-hosted plugin

D. Prisma Cloud Enterprise Edition

ANSWER: B

Explanation:

Prisma Cloud Compute Edition is the appropriate product for an air-gapped environment because it is designed to support self-hosted deployment of the Compute Console and Defenders within the customer's own infrastructure. This model enables organizations to manage and protect hosts, containers, Kubernetes workloads, serverless functions, and application images without requiring the deployment environment to maintain direct connectivity to the public internet or the Prisma Cloud SaaS service. For disconnected deployments, administrators obtain the required installation artifacts and container images through an approved connected process, transfer them into the isolated network, and deploy the Console locally. The locally deployed Console then provides centralized policy management, vulnerability and compliance visibility, runtime protection, and Defender management for the protected environment. This architecture is particularly suited to regulated, classified, operational-technology, and otherwise isolated networks where outbound cloud access is prohibited or tightly controlled. Palo Alto Networks documents Compute Edition as the self-hosted Prisma Cloud Compute offering and provides specific procedures for air-gapped installation and operation. See the Prisma Cloud Compute Edition documentation and the air-gapped installation guidance.

QUESTION NO: 14

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

A. Redlock

B. Defender

C. Twistlock

D. Default

ANSWER: C

Explanation:

Twistlock is the default Kubernetes namespace used by the Prisma Cloud Compute Defender DaemonSet deployment script. When the script generates and applies the Kubernetes resources needed to run host or container Defenders, it uses the `twistlock` namespace unless the deployment configuration is customized. This namespace convention originates from Twistlock, the former product name for Prisma Cloud Compute, and it remains present in Compute deployment artifacts and operational documentation. Using a dedicated namespace separates Defender resources, such as the DaemonSet, service account, ConfigMaps, and related permissions, from application workloads and helps administrators manage the security tooling consistently. Although Kubernetes administrators can modify manifests or deployment commands to use an organization-specific namespace, that customization does not change the documented default. Therefore, for a question asking which namespace is created by default during Defender DaemonSet deployment, **Twistlock** is the accurate answer. Palo Alto Networks documents Defender deployment and Kubernetes configuration in its Kubernetes Defender installation guidance and describes DaemonSet deployment configuration, including namespace-related settings, in the DaemonSet configuration documentation.

QUESTION NO: 15

Which two bot categories belong to unknown bots under Web-Application and API Security (WAAS) bot protection? (Choose two.)

A. News bots

B. Search engine crawlers

C. Web scrapers

D. HTTP libraries

ANSWER: C D

Explanation:

Web scrapers and HTTP libraries are the bot categories classified as unknown bots in Prisma Cloud Compute Web-Application and API Security bot protection. WAAS evaluates incoming requests using bot-identification signals, including request attributes and user-agent characteristics, then groups recognized traffic into known and unknown bot categories. Web scrapers commonly automate retrieval and extraction of content from web pages or application endpoints. Although they can support legitimate collection use cases, their automated behavior can also be used for large-scale harvesting of application data. HTTP libraries are software clients and frameworks used to create HTTP requests programmatically. They are frequently legitimate development tools, but they can also be used to automate requests in ways that resemble scripted abuse. Because these categories do not inherently establish the trusted identity or purpose associated with recognized good bots, WAAS treats them as unknown bot types so that a policy can alert on, deny, or otherwise control their access according to the application's security requirements. Palo Alto Networks documents WAAS bot protection and its bot categorization capabilities in the WAAS Bot Protection documentation and the WAAS administration documentation.

QUESTION NO: 16

Which two filters are available in the SecOps dashboard? (Choose two.)

A. Time range

B. Account Groups

C. Service Name

D. Cloud Region

ANSWER: A B

Explanation:

The SecOps dashboard supports the **Time range** and **Account Groups** filters to help security teams scope the dashboard's findings and operational metrics to the context they need to investigate. **Time range** lets users select the period represented by the dashboard data. This is useful for reviewing recent activity, assessing changes over a defined period, and focusing triage on the relevant operational window. **Account Groups** lets users limit the dashboard view to a defined set of cloud accounts. Because cloud environments commonly span multiple accounts, subscriptions, or projects, this filter supports delegated ownership and enables teams to review the security posture and workload risk for the part of the organization they manage. Together, these filters allow SecOps personnel to efficiently focus on a particular time window and cloud-account scope without losing the broader dashboard workflow. Palo Alto Networks documents dashboard filtering and account-group-based scoping as part of Prisma Cloud's administrative and operational experience. See the Prisma Cloud Administrator's Guide and the Prisma Cloud Account Groups documentation.

QUESTION NO: 17

What is the primary purpose of Prisma Cloud Code Security?

A. To provide a platform for developers to create custom security policies for applications

B. To triage alerts and incidents in realtime during deployment

C. To address cloud infrastructure misconfigurations in code before they become alerts or incidents

D. To offer instant feedback on application performance issues and bottlenecks

ANSWER: C

Explanation:

Prisma Cloud Code Security is primarily intended to shift cloud security checks earlier into the software development lifecycle, enabling teams to identify and remediate cloud infrastructure risks while they are still represented as code. The capability scans infrastructure-as-code templates, such as Terraform, CloudFormation, ARM, and Kubernetes manifests, for configuration issues that could create insecure cloud resources after deployment. It also provides developers with actionable findings in their source-control and CI/CD workflows, so remediation can occur before a change reaches production.

Accordingly, “To address cloud infrastructure misconfigurations in code before they become alerts or incidents” accurately captures the preventive purpose of Code Security. Fixing an issue at the code stage helps organizations avoid deploying noncompliant or exposed infrastructure and reduces the operational effort of investigating and correcting resulting runtime alerts. This supports a DevSecOps model in which developers and security teams share responsibility for secure cloud delivery. Palo Alto Networks describes Code Security as providing visibility and security scanning for code and infrastructure as code before deployment. See the Prisma Cloud Code Security documentation and the Prisma Cloud Code Security overview.

QUESTION NO: 18

What are the two ways to scope a CI policy for image scanning? (Choose two.)

A. container name

B. image name

C. hostname

D. image labels

ANSWER: B D

Explanation:

image name and **image labels** are the available scoping methods for a Prisma Cloud Compute CI policy used for image scanning. Image-name scoping targets the policy at container images whose repository or image identifier matches the defined scope. This lets teams apply controls to the images associated with a particular application, service, repository namespace, or build stream without applying the policy indiscriminately to every image evaluated in CI.

Image-label scoping uses metadata embedded in the image configuration. Labels are useful when an organization uses a consistent metadata convention—such as application ownership, environment, business unit, or compliance classification—and wants policy evaluation to follow that metadata. As a result, image labels provide a portable way to classify images even when naming conventions vary across registries or pipelines. These scopes help make CI policy enforcement specific, repeatable, and aligned with the image attributes available during a build or pipeline scan. Palo Alto Networks documents CI policy configuration and its image-focused policy controls in the Prisma Cloud Compute CI policies documentation and the Compute compliance documentation.

QUESTION NO: 19

Which two statements apply to the Defender type Container Defender - Linux?

A. It is implemented as runtime protection in the userspace.

B. It is deployed as a service.

C. It is deployed as a container.

D. It is incapable of filesystem runtime defense.

ANSWER: A C

Explanation:

Container Defender - Linux is designed to protect an individual Linux container’s workload from within the containerized environment. It is deployed as a container, typically alongside the workload it protects, so it can be incorporated into container deployment workflows and receive the configuration needed for runtime security. This model is useful where protection is required at the individual-container level rather than through a host-level Defender deployment.

The Defender provides runtime protection in userspace. Prisma Cloud’s runtime protection architecture uses the Defender to observe and enforce protections for workload activity without requiring a kernel module inside the protected workload container. For Linux containers, this includes runtime-defense capabilities that monitor relevant process, network, and

filesystem activity according to the configured runtime rules. The container-based deployment and userspace runtime-protection model therefore describe the key characteristics of Container Defender - Linux.

See the Prisma Cloud Compute documentation on installing Container Defender and Runtime Defense.

QUESTION NO: 20 - (SIMULATION)

Which order of steps map a policy to a custom compliance standard?

(Drag the steps into the correct order of occurrence, from the first step to the last.)

ANSWER: See the explanation for the answer

Explanation:

Correct order:

1. Click **Compliance Standards**.
2. Add the **custom compliance standard**.
3. Edit the applicable **policy**.
4. Select/add the custom **compliance standard** from the policy's compliance-standard drop-down menu.

The custom standard must be created before it can be selected and mapped to a policy.

QUESTION NO: 21

What is required for Prisma Cloud to successfully execute auto-remediation commands?

A. Read access to the cloud platform

B. Write access to the cloud platform

C. Access to the cloud platform only for Azure

D. Prisma Cloud requires no access to the cloud platform

ANSWER: B

Explanation:

Prisma Cloud requires **Write access to the cloud platform** to execute auto-remediation commands. Auto-remediation does more than identify a configuration issue: it invokes an approved remediation action that changes resources or their settings in the connected cloud account. Depending on the policy and cloud provider, that action might modify a resource configuration, update a security setting, apply a tag, alter a network control, or otherwise bring the resource back into the organization's desired secure state. The Prisma Cloud role, service principal, or equivalent cloud identity must therefore be granted the relevant create, update, delete, or other write-level API permissions for the target resource and action. Permissions should follow least-privilege principles, granting only the specific remediation capabilities required rather than unrestricted administrative access. Cloud-account onboarding and access configuration are foundational because Prisma Cloud uses the permissions assigned to its cloud identity when interacting with provider APIs. Palo Alto Networks documents cloud account connection and required permissions at Connect Cloud Accounts. Prisma Cloud's remediation capabilities and workflows are also documented in the Code Remediations documentation.

QUESTION NO: 22

A security team has a requirement to ensure the environment is scanned for vulnerabilities. What are three options for configuring vulnerability policies? (Choose three.)

A. individual actions based on package type

B. output verbosity for blocked requests

C. apply policy only when vendor fix is available

D. individual grace periods for each severity level

E. customize message on blocked requests

ANSWER: A C D

Explanation:

Prisma Cloud Compute vulnerability management rules provide risk-based controls that determine which discovered package vulnerabilities require enforcement and how enforcement is applied. **individual actions based on package type** is supported because vulnerability rules can distinguish package ecosystems, allowing teams to apply enforcement appropriate to the package type being evaluated. This enables a policy to reflect the differing remediation processes and risk profiles that can exist across operating-system and language packages.

apply policy only when vendor fix is available is also a supported configuration criterion. Using fix availability focuses enforcement on vulnerabilities for which an actionable remediation path exists, helping security teams prioritize work that can be resolved through an available vendor update.

individual grace periods for each severity level supports a practical, severity-driven remediation program. Grace periods allow vulnerabilities to remain compliant for a defined interval before policy enforcement applies, and severity-specific periods let critical findings receive the shortest remediation window while allowing proportionate timelines for lower-risk findings. Together, these settings enable tailored vulnerability policy enforcement rather than a single uniform response for every package and finding. See Palo Alto Networks guidance on vulnerability management rules and vulnerability management in Prisma Cloud Compute.

QUESTION NO: 23

Which three steps are involved in onboarding an account for Data Security? (Choose three.)

A. Create a read-only role with in-line policies

B. Create a Cloudtrail with SNS Topic

C. Enable Flow Logs

D. Enter the RoleARN and SNSARN

E. Create a S3 bucket

ANSWER: B D E

Explanation:

Creating a CloudTrail with an SNS topic, entering the RoleARN and SNSARN, and creating an S3 bucket are the required components for AWS Data Security onboarding. The S3 bucket provides the durable AWS location used for CloudTrail log delivery. Those audit records give Prisma Cloud Data Security visibility into relevant account activity and events associated with protected data resources. CloudTrail must be configured to publish notifications through an SNS topic so the integration can receive event notifications; the topic ARN is therefore a required value during onboarding. The RoleARN identifies the AWS IAM role that Prisma Cloud assumes to access the account with the permissions required for Data Security operations, while the SNSARN connects the onboarding configuration to the notifications generated by the CloudTrail integration. Together, these values establish the storage, auditing, notification, and delegated-access components needed for the account connection. AWS documents that a trail delivers log files to an S3 bucket and can publish notifications to an SNS topic, and Palo Alto Networks documents the AWS account onboarding workflow and required role-based access for Prisma Cloud. See AWS CloudTrail documentation and Palo Alto Networks Prisma Cloud AWS onboarding documentation.

QUESTION NO: 24

Which two statements are true about the differences between build and run config policies? (Choose two.)

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

B. Build and Audit Events policies belong to the configuration policy set.

C. Run policies monitor resources, and check for potential issues after these cloud resources are deployed.

D. Build policies enable you to check for security misconfigurations in the IaC templates and ensure that these issues do not get into production.

E. Run policies monitor network activities in your environment, and check for potential issues during runtime.

ANSWER: C D

Explanation:

Run policies monitor deployed cloud resources and evaluate their current configuration against Prisma Cloud's policy logic. They are used after resources exist in the cloud environment, providing ongoing visibility into configuration risks, policy violations, and posture drift that can arise during normal operations. This runtime evaluation is central to cloud security posture management because it enables teams to identify issues in accounts and workloads that are already active and then prioritize remediation based on the affected resource and its risk context.

Build policies apply the same shift-left principle to infrastructure before it is deployed. They scan infrastructure-as-code templates, such as Terraform or CloudFormation, to identify configuration issues during development and CI/CD workflows. Detecting these issues in templates lets developers correct them before the template provisions cloud resources, reducing the likelihood that insecure configurations reach production. Together, build and run policy coverage protects two distinct lifecycle stages: pre-deployment template validation and post-deployment resource monitoring. Palo Alto Networks describes policy management and the available policy types in the Prisma Cloud policy documentation, and explains shift-left IaC security in its Shift Left Security overview.

QUESTION NO: 25

A customer has a requirement to automatically protect all Lambda functions with runtime protection. What is the process to automatically protect all the Lambda functions?

A. Configure a function scan policy from the Defend/Vulnerabilities/Functions page.

B. Configure serverless radar from the Defend/Compliance/Cloud Platforms page.

C. Configure a manually embedded Lambda Defender.

D. Configure a serverless auto-protect rule for the functions.

ANSWER: D

Explanation:

Configure a serverless auto-protect rule for the functions. In Prisma Cloud Compute, serverless auto-protect rules automate deployment of the Prisma Cloud Defender layer to AWS Lambda functions that match the rule's scope. The rule can target functions using AWS account, region, tags, function names, and other supported criteria, so an organization can establish coverage broadly for its Lambda estate rather than modifying each function individually. Once configured, the auto-protect capability continuously evaluates eligible functions and applies runtime protection as functions are created or updated, helping maintain consistent coverage in dynamic serverless environments. This approach is specifically intended for automated runtime defense of Lambda workloads and supports operationally scalable protection without requiring developers to manually package protection into every deployment. Configure the rule with an appropriate scope that includes all required accounts, regions, and functions, then enable it so Prisma Cloud can protect both existing matching functions and newly deployed matching functions. Palo Alto Networks documents the serverless protection workflow and the available automatic deployment model in its Prisma Cloud Compute documentation and serverless security guidance. See Prisma Cloud Compute serverless protection documentation and Palo Alto Networks serverless security overview.

QUESTION NO: 26

When an alert notification from the alarm center is deleted, how many hours will a similar alarm be suppressed by default?

A. 12

B. 8

C. 24

D. 4

ANSWER: C

Explanation:

24 is correct. Deleting an alert notification in the Alarm Center applies the platform's default suppression period to comparable alarms for the next 24 hours. This behavior reduces repeated notifications for the same or substantially similar condition after an administrator has acknowledged it by deleting the notification. The suppression interval is intended to prevent alert fatigue while preserving the underlying alerting and policy-evaluation mechanisms; it does not mean that the security condition has been remediated or that monitoring has stopped. During the default 24-hour period, matching alarms are withheld from notification so responders can focus on new or materially different events. After that interval expires, a similar alarm can again generate a notification if the condition is still present or reoccurs. This aligns with Palo Alto Networks' approach of centralizing cloud-security findings and notifications while supporting operational workflows that reduce duplicate alerts. For related alert-management concepts and how Prisma Cloud generates and manages alerts, see the Prisma Cloud Alerts documentation and the alert notifications documentation.

QUESTION NO: 27

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

A. Checkov

B. Visual Studio Code

C. CircleCI

D. IntelliJ

ANSWER: A C

Explanation:

Checkov and **CircleCI** are supported within Prisma Cloud Code Security workflows. Checkov is Palo Alto Networks' policy-as-code scanning tool for infrastructure as code, and it can be run in automated delivery pipelines to evaluate templates, configurations, and policies before cloud resources are provisioned. This enables teams to identify misconfigurations and policy violations early in the development lifecycle and to enforce build outcomes based on scan findings. CircleCI is a supported continuous integration and delivery environment in which Code Security scanning can be incorporated, allowing checks to run as part of automated build and deployment jobs. Together, Checkov's scanning capabilities and CircleCI pipeline integration support the shift-left approach used by Prisma Cloud Code Security: developers receive actionable findings during code changes rather than after deployment. Palo Alto Networks documents Code Security integrations and scanning workflows in its Prisma Cloud documentation, while Checkov's integration guidance describes its use in CI environments, including CircleCI. See Prisma Cloud Code Security documentation and Checkov continuous-integration documentation.

QUESTION NO: 28

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

A. BitBucket

B. Visual Studio Code

C. CircleCI

D. IntelliJ

ANSWER: A C

Explanation:

BitBucket and **CircleCI** are supported CI/CD integrations for Prisma Cloud DevOps Security. These integrations enable teams to embed Prisma Cloud security checks into automated build and delivery workflows, so infrastructure-as-code, open-source dependencies, containers, and other application-security findings can be evaluated before software is deployed. In a CI/CD workflow, Prisma Cloud can apply policy checks and return results to the pipeline, allowing organizations to establish security gates and prevent builds that violate defined security requirements from progressing.

BitBucket support is useful for teams whose source control and pipeline processes are based on Atlassian Bitbucket and Bitbucket Pipelines. CircleCI support similarly allows security scanning and policy enforcement to run as part of CircleCI jobs and workflows. Both integrations align with the shift-left approach used by Prisma Cloud Code Security: developers receive actionable findings in the tools and automated workflows used during development, rather than discovering issues only after deployment. Palo Alto Networks documents CI/CD integration as part of Prisma Cloud Code Security and provides pipeline-specific guidance for integrating scans into supported build systems. See the Prisma Cloud Code Security documentation and the Shift Left documentation.