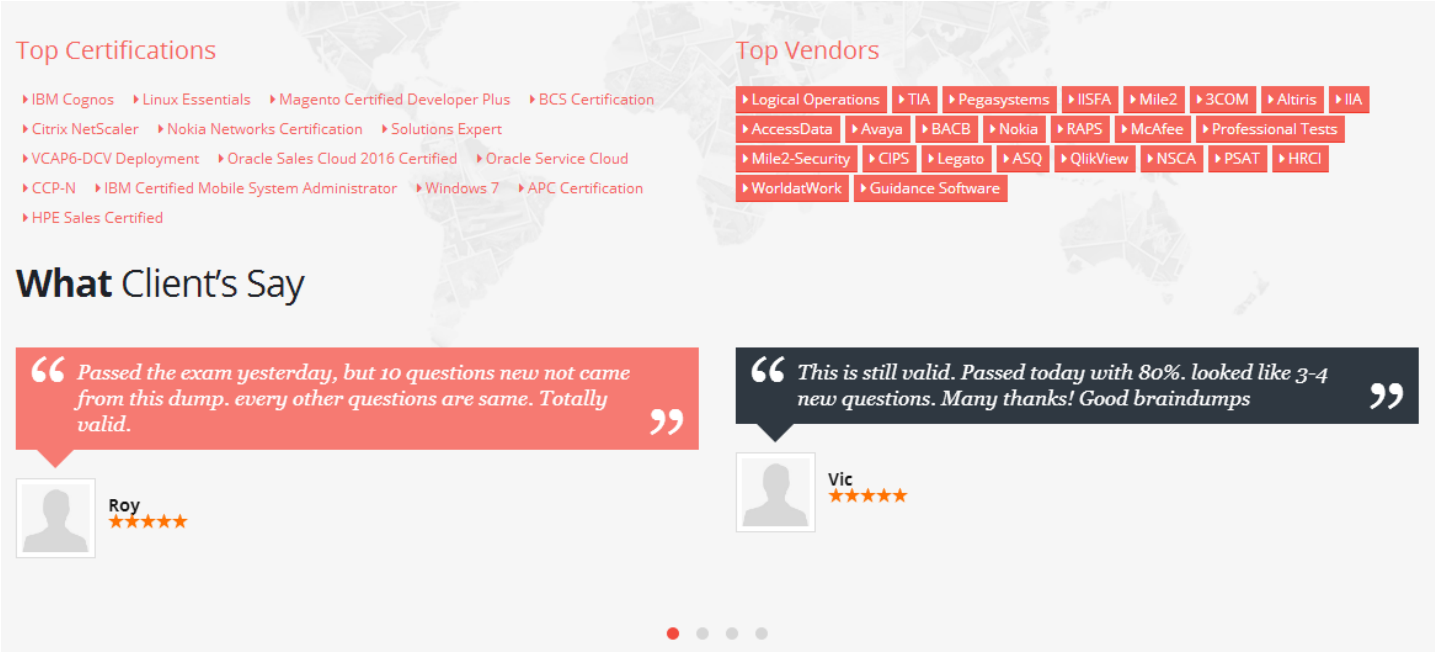
Lead2passExam



http://www.lead2passexam.com/

Available Exam Cram and Valid Dumps - Lead2Pass Exam

Exam : **CloudSec-Pro**

Title : Palo Alto Networks Cloud Security Professional

Vendor : Palo Alto Networks

Version : DEMO

NO.1 Which three options for hardening a customer environment against misconfiguration are included in Prisma Cloud Compute compliance enforcement for hosts? (Choose three.)

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.

NO.2 Which container image scan is constructed correctly?

A. twistcli images scan --docker-address https://us-west1.cloud.twistlock.com/us-3-123456789 myimage/ latest

B. twistcli images scan --address https://us-west1.cloud.twistlock.com/us-3-123456789 myimage/latest

C. twistcli images scan --address https://us-west1.cloud.twistlock.com/us-3-123456789 --container myimage/ latest

D. twistcli images scan --address https://us-west1.cloud.twistlock.com/us-3-123456789 --container myimage/ latest --details

Answer: B

Explanation:

The correct construction for scanning a container image using the TwistCLI tool in Prisma Cloud is option B.

This command specifies the address of the Prisma Cloud Console and the image to be scanned, including its tag. The TwistCLI tool is part of Prisma Cloud's capabilities to integrate security into the CI/CD pipeline, allowing for the scanning of images for vulnerabilities as part of the build process, thus ensuring that only secure images are deployed.

NO.3 How does assigning an account group to an administrative user on Prisma Cloud help restrict access to resources?

A. It restricts access only to certain types of resources within the cloud account.

B. It restricts access to all resources and data within the cloud account.

C. It restricts access only to the resources and data that pertains to the cloud account(s) within an account group.

D. It does not restrict access to any resources within the cloud account.

Answer: C

Explanation:

In Prisma Cloud, assigning an administrative user to an account group is a way to implement the principle of least privilege by restricting the user's access to a specific subset of resources and data. Account groups are logical collections of cloud accounts, and by associating an administrative user with a particular account group, their access is limited to only those resources and data associated with the cloud accounts within that group. This mechanism ensures that users have access only to the information and resources necessary for their role or tasks, enhancing security by minimizing the potential for unauthorized access or actions within the cloud environment.

NO.4 What is a benefit of the Cloud Discovery feature?

A. It does not require any specific permissions to be granted before use.

B. It helps engineers find all cloud-native services being used only on AWS.

C. It offers coverage for serverless functions on AWS only.

D. It enables engineers to continuously monitor all accounts and report on the services that are unprotected.

Answer: D

Explanation:

The Cloud Discovery feature in Prisma Cloud allows engineers to monitor accounts continuously and report on cloud-native services that are unprotected across different cloud service providers. This feature requires specific permissions to access and assess the cloud environment's configuration and security posture. Thus, the correct answer is D: It enables engineers to continuously monitor all accounts and report on the services that are unprotected.

https://docs.prismacloud.io/en/classic/compute-admin-guide/cloud-service-providers/cloud-accounts- discovery-pcee

NO.5 A customer wants to be notified about port scanning network activities in their environment. Which policy type detects this behavior?

A. Network

B. Port Scan

C. Anomaly

D. Config

Answer: C

Explanation:

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

NO.6 Which intensity setting for anomaly alerts is used for the measurement of 100 events over 30 days?

A. High

B. Medium

C. Low

D. Very High

Answer: B
Explanation:
In the context of setting anomaly alert intensities in Prisma Cloud, an intensity setting of "Medium" could be used for the measurement of 100 events over 30 days. This setting indicates a moderate level of anomaly detection sensitivity, which is suitable for environments where there is a need to balance between detecting potential security issues and minimizing false positives.
Reference: https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin/manage-prisma- cloud- administrators/define-prisma-cloud-enterprise-settings.html
https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin/manage-prisma-cloud- administrators/define-prisma-cloud-enterprise-settings

NO.7 Which role must be assigned to DevOps users who need access to deploy Container and Host Defenders in Compute?
A. Cloud Provisioning Admin
B. Build and Deploy Security
C. System Admin
D. Developer
Answer: A
Explanation:
Cloud Provisioning Admin (Defender Manager) DevOps team members that need to manage Defender deployments without sysadmin privileges.
https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma- cloud-admin -compute/authentication/prisma_cloud_user_roles

NO.8 Which ROL query is used to detect certain high-risk activities executed by a root user in AWS?
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

NO.9 An S3 bucket within AWS has generated an alert by violating the Prisma Cloud Default policy "AWS S3 buckets are accessible to public". The policy definition follows:
config where cloud.type = 'aws' AND api.name='aws-s3api-get-bucket-acl' AND json.rule="((((acl.grants[?(@.grantee=='AllUsers')] size > 0) or policyStatus.isPublic is true) and publicAccessBlockConfiguration does not exist) or ((acl.grants[?(@.grantee=='AllUsers')] size > 0) and publicAccessBlockConfiguration.

ignorePublicAcis is false) or (policyStatus.isPublic is true and publicAccessBlockConfiguration. restrictPublicBuckets is false)) and websiteConfiguration does not exist" Why did this alert get generated?

A. an event within the cloud account

B. network traffic to the S3 bucket

C. configuration of the S3 bucket

D. anomalous behaviors

Answer: C

Explanation:

The alert "AWS S3 buckets are accessible to public" is generated due to the configuration of the S3 bucket, which has been set in a way that allows public access. The policy definition provided checks for various conditions that would make an S3 bucket publicly accessible, such as grants to 'AllUsers', the absence of a 'publicAccessBlockConfiguration', or specific configurations that do not restrict public access. Therefore, the alert is triggered by the configuration settings of the S3 bucket that violate the policy's criteria for public accessibility.

NO.10 Which RQL will trigger the following audit event activity?

A. event from cloud.audit_logs where operation ConsoleLogin AND user = 'root'

B. event from cloud.audit_logs where operation IN('cloudsql.instances.update','cloudsql.sslCerts.create', cloudsql.instances.create','cloudsq

C. event from cloud.audit_logs where cloud.service = s3.amazonaws.com' AND json.rule = $.userAgent contains 'parrot1

D. event from cloud.audit_logs where operation IN ('GetBucketWebsite', 'PutBucketWebsite', 'DeleteBucketWebsite')

Answer: A

Explanation:

The correct RQL to trigger the audit event activity shown is Option A. This RQL is designed to capture events from cloud audit logs where a ConsoleLogin operation occurs by the 'root' user. The given audit event details match this RQL's criteria, which specifies the operation type and the user involved in the event.

NO.11 An administrator has a requirement to ingest all Console and Defender logs to Splunk. Which option will satisfy this requirement in Prisma Cloud Compute?

A. Enable the API settings for logging.

B. Enable the CSV export in the Console.

C. Enable the syslog option in the Console

D. Enable the Splunk option in the Console.

Answer: C

Explanation:

Log into Console. / Go to Manage > Alerts > Logging. / Configure Prisma Cloud to send audit event records to syslog, stdout and Prometheus.

https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin-compute/audit/logging To ingest all Console and Defender logs into Splunk within Prisma Cloud Compute, the most effective method is to enable the syslog option in the Console. This configuration

allows the direct export of logs in a format compatible with Splunk, facilitating real-time log analysis and monitoring. This setup supports continuous security monitoring and advanced threat detection capabilities by utilizing Splunk's extensive data processing and visualization tools.

NO.12 Which of the following is a reason for alert dismissal?

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_UPDATED is 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.

NO.13 A customer has a requirement to terminate any Container from image topSecret:latest when a process named ransomWare is executed.

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

A. set the Container model to manual relearn and set the default runtime rule to block for process protection.

B. set the Container model to relearn and set the default runtime rule to prevent for process protection.

C. add a new runtime policy targeted at a specific Container name, add ransomWare process into the denied process list, and set the action to "prevent".

D. choose "copy into rule" for the Container, add a ransomWare process into the denied process list, and set the action to "block".

Answer: D

Explanation:

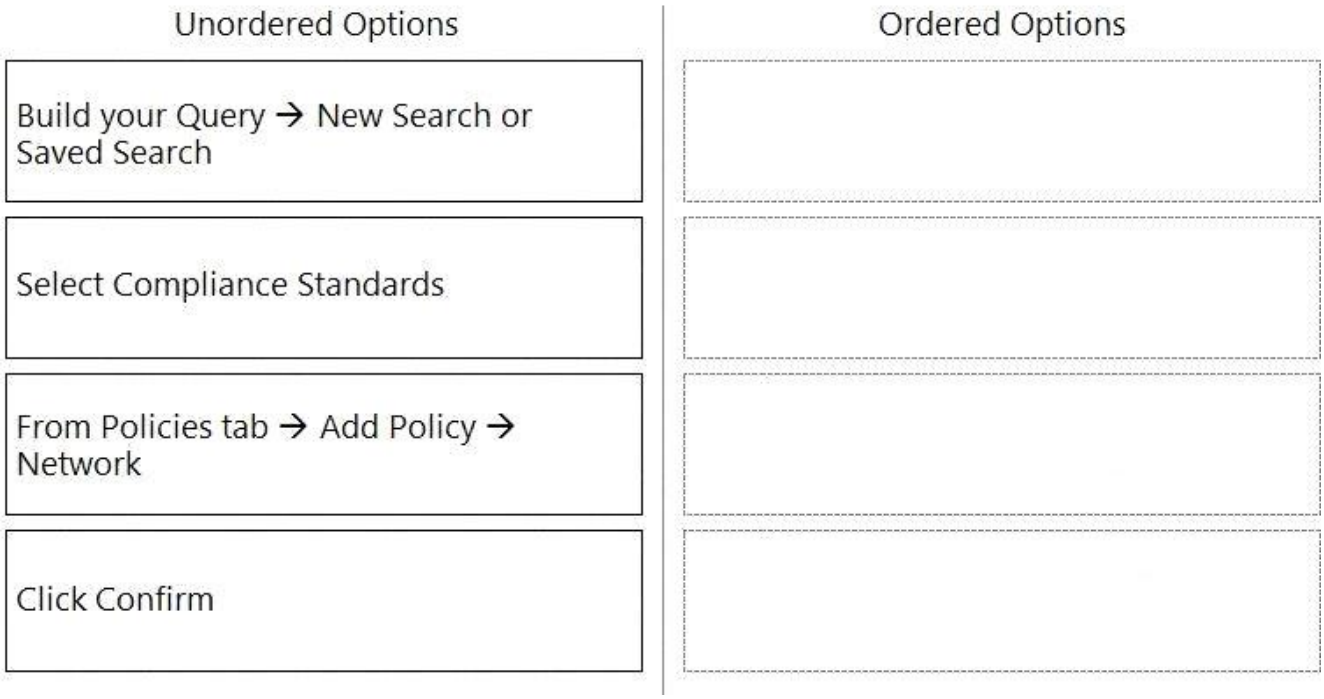
https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin-compute/runtime_defense

/runtime_defense_containers

NO.14 What is the order of steps to create a custom network policy?

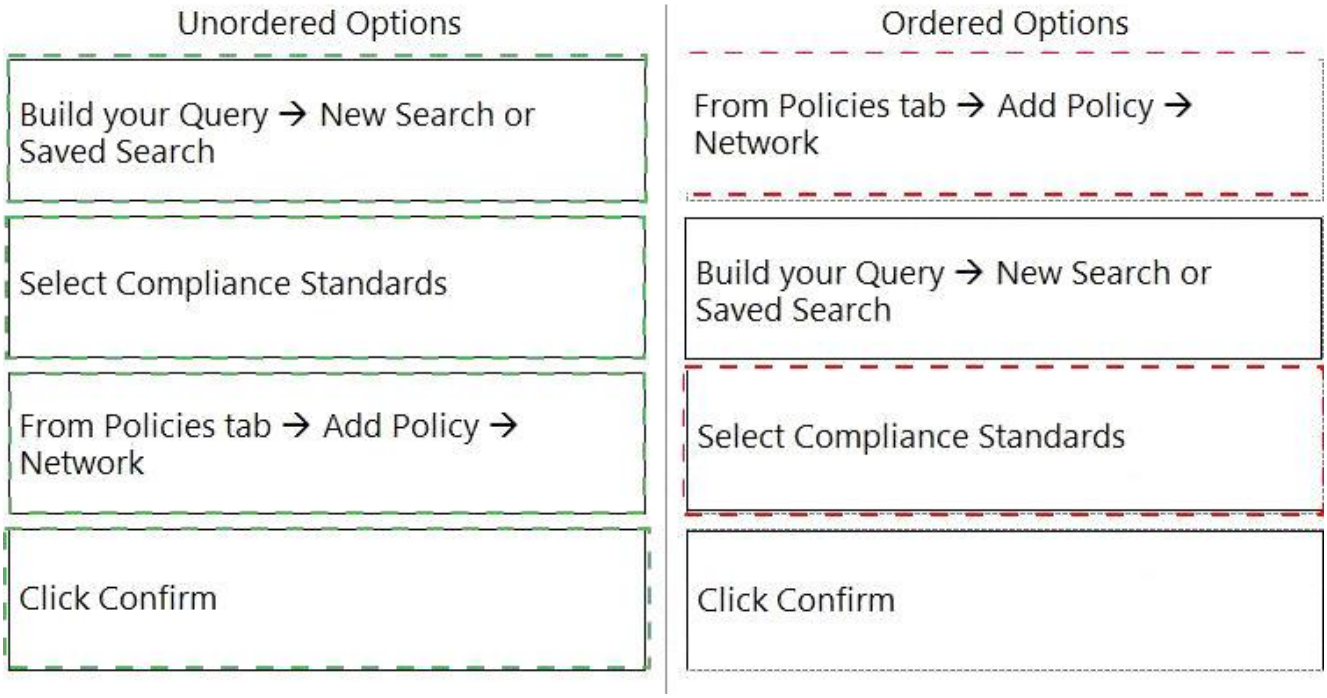
(Drag the steps into the correct order of occurrence, from the first step to the last.)

Answer Area



Answer:

Answer Area



Explanation:

A picture containing table Description automatically generated

Answer Area

Unordered Options	Ordered Options
Build your Query → New Search or Saved Search	From Policies tab → Add Policy → Network
Select Compliance Standards	Build your Query → New Search or Saved Search
From Policies tab → Add Policy → Network	Select Compliance Standards
Click Confirm	Click Confirm

Reference:
https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin/prisma-cloud-policies/create-a- policy.html Select Policies and click Add Policy Build the query Add the compliance standards Click Submit.
https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin/prisma-cloud-policies/create-a- policy

NO.15 The compliance team needs to associate Prisma Cloud policies with compliance frameworks. Which option should the team select to perform this task?

A. Custom Compliance

B. Policies

C. Compliance

D. Alert Rules

Answer: A

Explanation:
1) Select Policies 2) Select the policy rule to edit, on 3 Compliance Standards click + and associate the policy with the compliance standard (https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin
/prisma-cloud-compliance/create-a-custom-compliance-standard)

NO.16 When configuring SSO how many IdP providers can be enabled for all the cloud accounts monitored by Prisma Cloud?

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.

NO.17 Given the following RQL:
event from cloud.audit_logs where operation IN ('CreateCryptoKey', 'DestroyCryptoKeyVersion', 'v1.compute.disks.createSnapshot')
Which audit event snippet is identified?

A.

```
"request": { "resource": "604173093072", "@type":
"type.googleapis.com/google.iam.v1.SetIamPolicyRequest", "policy": { "bindings": [
```

B.

```
{ "Statement": [ { "Action": "*", "Effect": "Allow", "Resource": "*"
 } ], "Version": "2012-10-17"
```

C.

```
"payload": { "requestMetadata": { "callerSuppliedUserAgent": "Terraform/0.14.0
(+https://www.terraform.io) Terrafom-Plugin-SDK/2.1.0 terraform-provider-google/3.50.0,gzip(gfe)",
 "callerIp": "34.265.226.252" }, "request": { "@type":
"type.googleapis.com/compute.disks.createSnapshot" },
```

Answer: C
Explanation:
https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-rql-reference/rql-reference/event-query
/event-query-examples

NO.18 Which two required request headers interface with Prisma Cloud API? (Choose two.)
A. Content-type:application/json
B. x-redlock-auth
C. >x-redlock-request-id
D. Content-type:application/xml
Answer: A B
Reference: https://prisma.pan.dev/api/cloud/api-headers/
Interfacing with the Prisma Cloud API, especially for tasks such as automation, integration, and advanced querying, requires specific request headers for authentication and data format specification. "Content-type:
application/json" is essential for indicating that the request body is formatted as JSON, which is a widely accepted data interchange format. The "x-redlock-auth" header is critical for passing the API access key or token, which authenticates the request to Prisma Cloud's API. This authentication mechanism ensures secure access to Prisma Cloud's capabilities while maintaining the integrity and confidentiality of the interactions.

NO.19 Which two options may be used to upgrade the Defenders with a Console v20.04 and Kubernetes deployment? (Choose two.)

A. Run the provided curl | bash script from Console to remove Defenders, and then use Cloud Discovery to automatically redeploy Defenders.

B. Remove Defenders DaemonSet, and then use Cloud Discovery to automatically redeploy the Defenders.

C. Remove Defenders, and then deploy the new DaemonSet so Defenders do not have to automatically update on each deployment.

D. Let Defenders automatically upgrade.

Answer: C D

Explanation:

For upgrading Defenders with a Console v20.04 and Kubernetes deployment, the following two options are viable:

* C. Remove Defenders, and then deploy the new DaemonSet: This option involves manually removing the existing Defenders and then deploying a new DaemonSet. This method ensures that the Defenders are updated to the latest version without relying on automatic updates12.
* D. Let Defenders automatically upgrade: Prisma Cloud provides the capability for Defenders to automatically upgrade themselves. This feature simplifies the upgrade process by eliminating the need for manual intervention3.

Both methods are supported and can be used depending on the organization's policies and preferences regarding Defender upgrades. The automatic upgrade feature is particularly useful for maintaining up-to-date security without manual oversight, while the manual removal and redeployment of a new DaemonSet can be preferred in environments where more control over the upgrade process is desired123.

NO.20 A business unit has acquired a company that has a very large AWS account footprint. The plan is to immediately start onboarding the new company's AWS accounts into Prisma Cloud Enterprise tenant immediately. The current company is currently not using AWS Organizations and will require each account to be onboarded individually.

The business unit has decided to cover the scope of this action and determined that a script should be written to onboard each of these accounts with general settings to gain immediate posture visibility across the accounts.

Which API endpoint will specifically add these accounts into the Prisma Cloud Enterprise tenant?

A. https://api.prismacloud.io/cloud/

B. https://api.prismacloud.io/account/aws

C. https://api.prismacloud.io/cloud/aws

D. https://api.prismacloud.io/accountgroup/aws

Answer: C

Explanation:

To add AWS accounts to the Prisma Cloud Enterprise tenant, the correct API endpoint is option C: https://api.

prismacloud.io/cloud/aws. This endpoint is specifically designed for integrating cloud accounts with Prisma Cloud, enabling centralized visibility and security posture management across multiple cloud environments.

By using this API endpoint, each AWS account can be individually onboarded to the Prisma Cloud

platform, allowing for immediate posture visibility and consistent security policy enforcement across the newly acquired company's extensive AWS footprint. This process aligns with Prisma Cloud's capabilities for multi- cloud security and compliance management, ensuring that the onboarding of cloud accounts is both efficient and aligned with the platform's best practices for cloud security.

NO.21 Which two attributes are required for a custom config RQL? (Choose two.)
A. json.rule
B. cloud.account
C. api.name
D. tag
Answer: A C
Explanation:
For a custom config Resource Query Language (RQL) in Prisma Cloud, two essential attributes are "json.
rule" and "api.name." The "json.rule" attribute allows users to specify the JSON structure that defines the criteria or conditions of the query, essentially dictating what the query is looking for within the cloud environment. The "api.name" attribute identifies the specific API endpoint that the query will target, providing context and scope for the query. Together, these attributes enable users to craft precise and targeted queries that can assess the configuration and security posture of cloud resources, aiding in compliance checks, security assessments, and other governance tasks.

NO.22 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
Reference: https://www.optiv.com/insights/source-zero/blog/defending-against-container-threats-palo-alto- prisma-cloud In Prisma Cloud, CI policies for image scanning can be scoped based on the image name and image labels.
These scoping options allow for targeted scanning of images, ensuring that policies are applied to relevant images based on their identifiers or metadata.

NO.23 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 Container Runtime Model in Prisma Cloud typically includes states such as Learning, Active, and Archived. The Learning state is where Prisma Cloud observes container behaviors to understand normal operations and establish a baseline. During this phase, the system is not actively enforcing security policies but is learning the typical behaviors and patterns of container activity. The Active

state is where the system actively enforces security policies based on the learned behaviors and detected anomalies. Containers that exhibit suspicious or malicious activity that deviates from the baseline may trigger alerts or actions based on configured policies. The Archived state refers to containers that are no longer active but whose data and activity logs are retained for historical analysis or compliance purposes.

NO.24 Which file extension type is supported for Malware scanning in Prisma Cloud Data Security (PCDS)?

A. .bat

B. .apk

C. .vb

D. .py

Answer: B

Explanation:

bat --> Data Classification

apk --> Malware Scanning

vb --> Data Classification

py --> Data Classification

https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin/prisma-cloud-data-security

/monitor-data-security-scan-prisma-cloud/supported-file-extensions

Prisma Cloud Data Security (PCDS) supports various file types for malware scanning, including .apk files, which are Android Package files used for installing applications on Android operating systems. This support is crucial for ensuring that applications deployed on or distributed through Android devices are free from malware and safe for user installation.

NO.25 Which type of RQL query should be run to determine if AWS Elastic Compute Cloud (EC2) instances without encryption was enabled?

A. NETWORK

B. EVENT

C. CONFIG

D. SECURITY

Answer: C

Explanation:

To determine if AWS EC2 instances are running without encryption enabled, the appropriate RQL (Resource Query Language) type to use is CONFIG. CONFIG queries in Prisma Cloud are designed to inspect the configuration states of cloud resources and identify compliance with best practices or specific security requirements. By running a CONFIG query, administrators can assess the configuration settings of EC2 instances, including whether encryption features are enabled or not. This type of query allows for deep inspection of resource configurations within cloud environments, making it the ideal choice for identifying unencrypted EC2 instances and thereby helping to ensure data protection and compliance with security policies.

NO.26 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:

The Defender type "Container Defender - Linux" in Prisma Cloud is typically deployed as a container. This deployment method allows the Defender to integrate seamlessly into containerized environments, providing runtime protection and monitoring for container activities. By running as a container, the Container Defender can leverage the native capabilities of the container orchestration platform, such as Kubernetes, to provide security features like threat detection, vulnerability management, and compliance enforcement within the containerized environment. This approach ensures that the security protections are closely aligned with the dynamic and scalable nature of containerized applications.