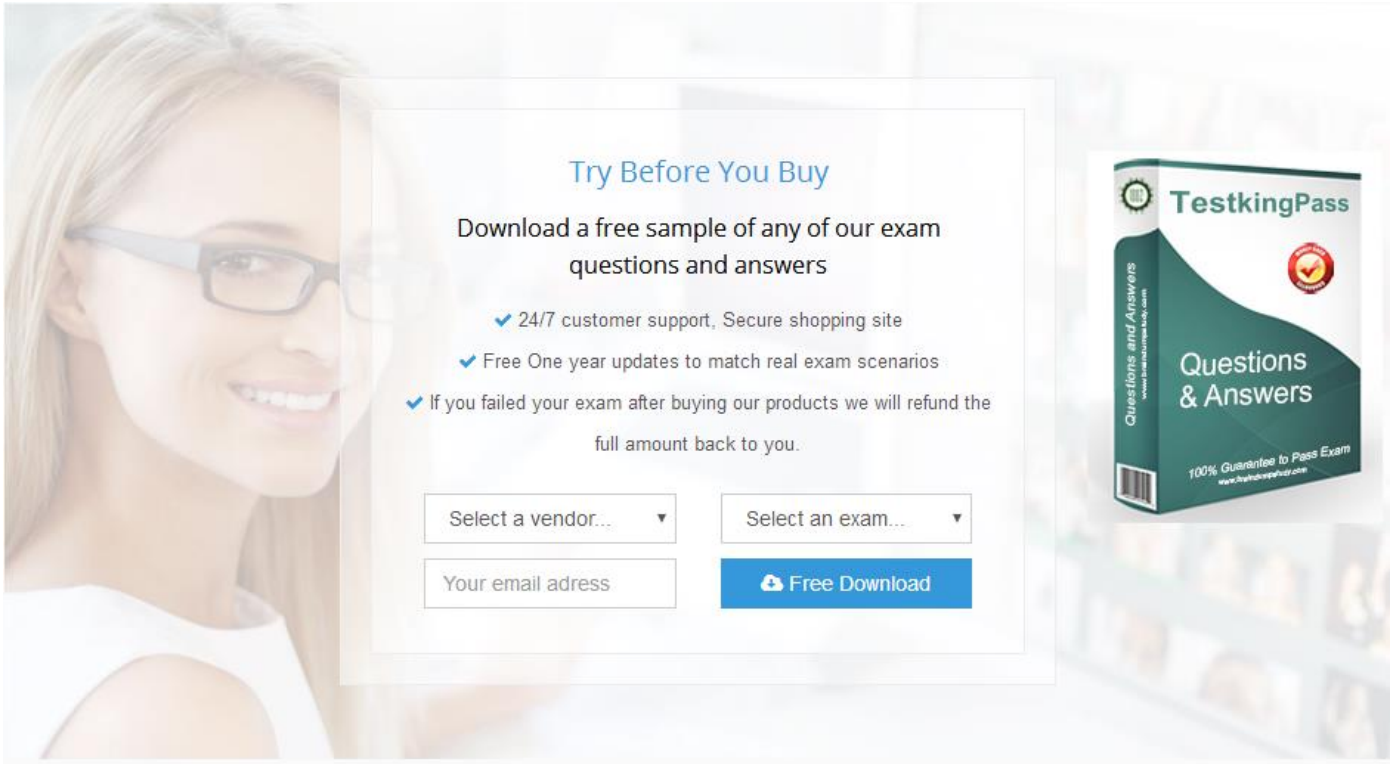
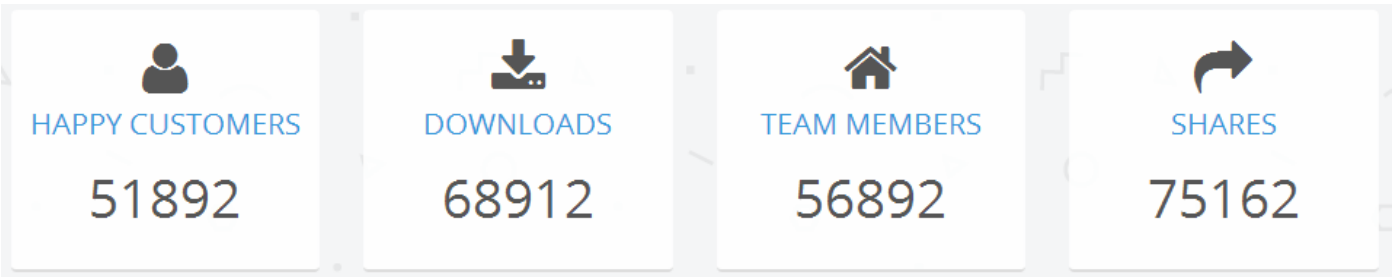
TestkingPass





http://www.testkingpass.com

Reliable test dumps & stable pass king & valid test questions

Exam : **PCCSE**

Title : Prisma Certified Cloud Security Engineer

Vendor : Palo Alto Networks

Version : DEMO

NO.1 A customer has a requirement to scan serverless functions for vulnerabilities.
What is the correct option to configure scanning?
A. Configure serverless radar from the Defend > Compliance > Cloud Platforms page.
B. Embed serverless Defender into the function.
C. Configure a function scan policy from the Defend > Vulnerabilities > Functions page.
D. Use Lambda layers to deploy a Defender into the function.
Answer: C
Explanation:
In Prisma Cloud, the capability to scan serverless functions, such as AWS Lambda functions, for vulnerabilities is an integral part of ensuring cloud security posture management (CSPM) and compliance.
Specifically, option C is correct because Prisma Cloud provides a dedicated section for defining policies related to serverless function vulnerabilities under the "Defend > Vulnerabilities > Functions" page. This feature allows administrators to create and manage policies that automatically scan serverless functions for known vulnerabilities, ensuring that the functions comply with the organization's security standards before they are deployed. This approach aligns with Prisma Cloud's comprehensive security model that covers various aspects of cloud security, including serverless functions, as outlined in the "Guide to Cloud Security Posture Management Tools" document https://docs.paloaltonetworks.com/prisma/prisma-cloud/22-12/prisma-cloud-compute-edition-admin/vulnerabilit

NO.2 Which API calls can scan an image named myimage: latest with twistcli and then retrieve the results from Console?
A. $ twistcli images scan \
--address \
--user \
--password \
--verbose \
myimage: latest
B. $ twistcli images scan \
--address \
--user \
--password \
--details \
myimage: latest
C. $ twistcli images scan \
--address \
--user \
--password \
myimage: latest
D. $ twistcli images scan \
--address \
--user \
--password \
--console \

myimage: latest

Answer: B

Explanation:

You can have twistcli generate a detailed report for each scan. The following procedure shows you how to scan an image with twistcli, and then retrieve the results from Console.

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

NO.3 An administrator of Prisma Cloud wants to enable role-based access control for Docker engine. Which configuration step is needed first to accomplish this task?

A. Configure Docker's authentication sequence to first use an identity provider and then Console.

B. Set Defender's listener type to TCP.

C. Set Docker's listener type to TCP.

D. Configure Defender's authentication sequence to first use an identity provider and then Console.

Answer: B

Explanation:

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

NO.4 While writing a custom RQL with array objects in the investigate page, which type of auto-suggestion a user can leverage?

A. Auto-sugestion for array objects that are useful for comparing between arrays

B. Auto-suggestion is not available for array objects

C. Auto-suggestion for array objects that are useful for categorization of resource parameters

D. Auto-suggestion for array objects that are useful for comparing between array elements

Answer: B

Explanation:

The auto suggest works with the operators = and IN . It is not supported for array objects. Use cloud.type attribute to refine the search results.

https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-rql-reference/rql-reference/event-query/ev

NO.5 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

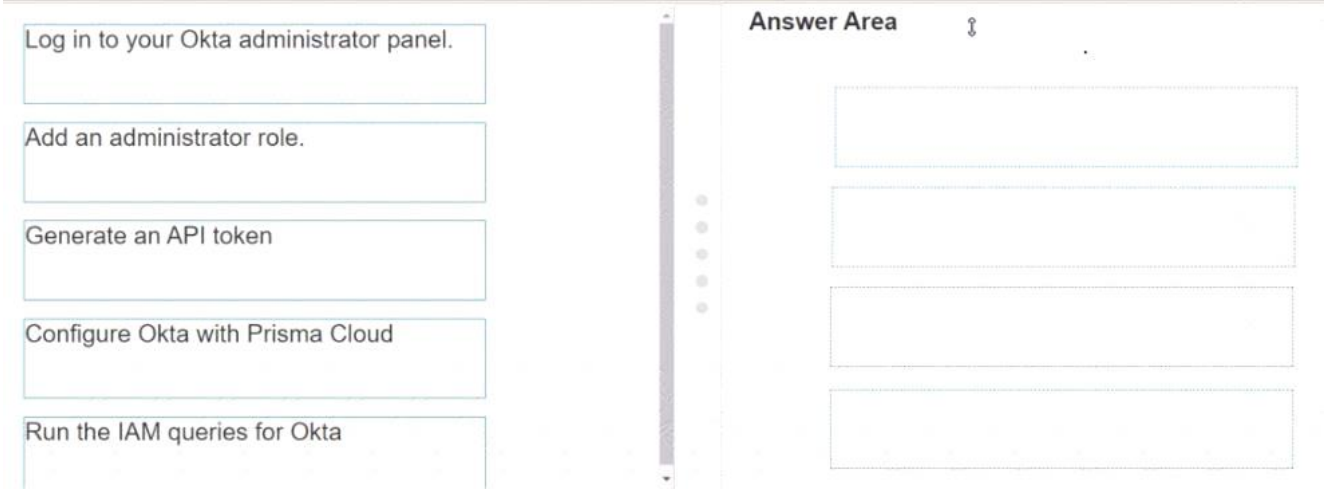
Answer: C D

Explanation:

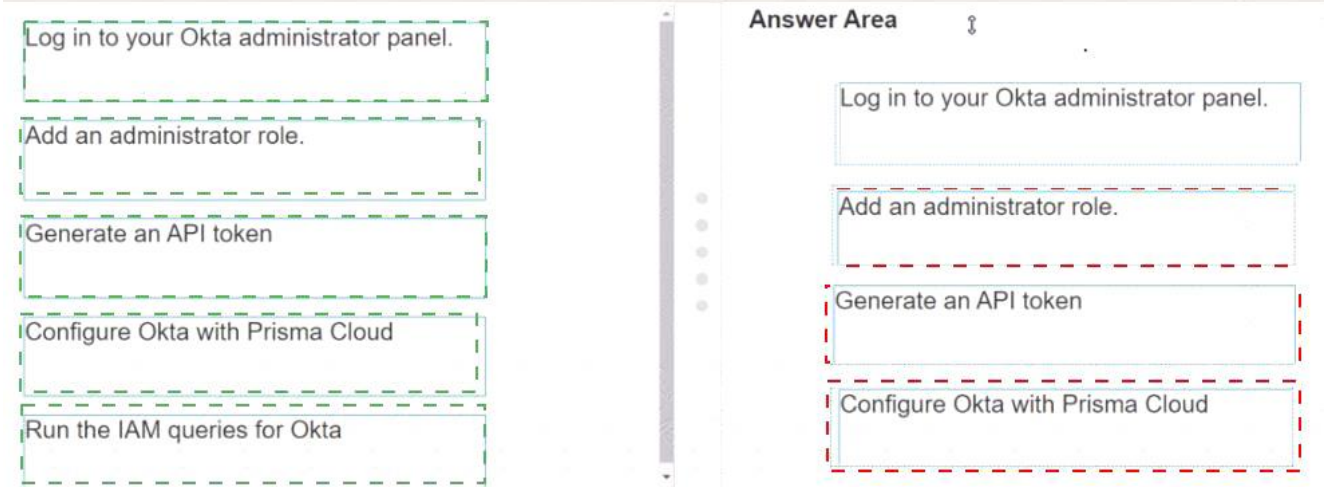
Under Web-Application and API Security (WAAS) bot protection in Prisma Cloud, unknown bots are categorized based on their behavior and characteristics. Web scrapers and HTTP libraries fall into the category of unknown bots. Web scrapers are automated scripts or programs that extract data from websites, often without permission, while HTTP libraries are tools used for making HTTP requests.

Both can be used benignly but may also be employed in malicious activities, hence their classification as unknown bots requiring further analysis.

NO.6 Put the steps of integrating Okta with Prisma Cloud in the right order in relation to CIEM or SSO okra integration.



Answer:



Explanation:

* Log in to your Okta administrator panel.
* Add an administrator role.
* Generate an API token.
* Configure Okta with Prisma Cloud.
* Run the IAM queries for Okta.

When integrating Okta with Prisma Cloud, especially in the context of Cloud Infrastructure Entitlement Management (CIEM) or Single Sign-On (SSO) integration, the process must be conducted in a sequence that establishes the necessary permissions and configurations for successful integration.

The first step is to log in to the Okta administrator panel. This is where you will manage your Okta settings and begin the integration process.

Once logged in, the next step is to add an administrator role. This involves assigning a role within Okta that has the appropriate permissions to create and manage API tokens and to perform integration tasks.

After setting up the correct administrative role, the third step is to generate an API token. This token

will be used to authenticate the communications between Okta and Prisma Cloud. The API token acts as a secure method of verifying that requests made to Prisma Cloud are authorized.
With the API token generated, the fourth step is to configure Okta with Prisma Cloud. This step typically involves entering the API token into Prisma Cloud and setting up the necessary configurations within Prisma Cloud to recognize and accept authentication requests from Okta.
The final step is to run the Identity and Access Management (IAM) queries for Okta within Prisma Cloud.
This step is crucial for CIEM, as it allows Prisma Cloud to query Okta for identity information, user roles, and entitlements, ensuring that the correct permissions are enforced across the cloud environment and that SSO is functioning correctly.
Following these steps in order will ensure that Okta is properly integrated with Prisma Cloud, providing a secure and efficient method for managing cloud access and entitlements.

NO.7 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:
To ensure that sensitive data such as SSNs and credit card numbers are not visible in Dashboard > Data view during investigations, the correct method is to go to Settings > Data > Snippet Masking and select Full Mask (A). This feature in Prisma Cloud allows administrators to mask sensitive data snippets within the dashboard, ensuring that such information is obfuscated and not exposed to unauthorized viewers. Full Masking provides a robust level of protection by completely hiding the sensitive values, thereby enhancing data privacy and compliance with regulations that mandate the protection of personal and financial information.

NO.8 A customer has a development environment with 50 connected Defenders. A maintenance window is set for Monday to upgrade 30 stand-alone Defenders in the development environment, but there is no maintenance window available until Sunday to upgrade the remaining 20 stand-alone Defenders.
Which recommended action manages this situation?

A. Go to Manage > Defender > Manage, then click Defenders, and use the Scheduler to choose which Defenders will be automatically upgraded during the maintenance window.

B. Find a maintenance window that is suitable to upgrade all stand-alone Defenders in the development environment.

C. Upgrade a subset of the Defenders by clicking the individual Actions > Upgrade button in the row that corresponds to the Defender that should be upgraded during the maintenance window.

D. Open a support case with Palo Alto Networks to arrange an automatic upgrade.

Answer: C

Explanation:
Managing Defender upgrades in a Prisma Cloud environment requires careful planning, especially in scenarios where not all Defenders can be upgraded simultaneously due to maintenance window constraints.
* Option C: Upgrade a subset of the Defenders by clicking the individual Actions > Upgrade button in the row that corresponds to the Defender that should be upgraded during the maintenance window is the recommended approach in this situation. This option allows administrators to manually select specific Defenders for upgrade within the available maintenance window, providing control over the upgrade process and ensuring that upgrades are aligned with operational requirements and maintenance schedules.
References:
* Prisma Cloud Defender Management Documentation: Details the procedures for managing and upgrading Prisma Cloud Defenders, including manual upgrade processes for individual Defenders.
* Best Practices for Managing Defender Upgrades: Offers guidelines on effectively planning and executing Defender upgrades, emphasizing the importance of aligning upgrade activities with maintenance windows to minimize disruption to the development environment.

NO.9 Which two variables must be modified to achieve automatic remediation for identity and access management (IAM) alerts in Azure cloud? (Choose two.)
A. API_ENDPOINT
B. SQS_QUEUE_NAME
C. SB_QUEUE_KEY
D. YOUR_ACCOUNT_NUMBER
Answer: A C
Explanation:
AZURE:
% export SB_QUEUE_KEY=your_sb_queue_key
% export SB_QUEUE_KEY_NAME=your_sb_queue_key_name
% export SB_QUEUE_NAME_SPACE=your_sb_queue_name_space
% export API_ENDPOINT=api_tenant
% export
AUTH_KEY=your_jwt_tokenhttps://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin/prism

NO.10 An administrator sees that a runtime audit has been generated for a Container. The audit message is "DNS resolution of suspicious name wikipedia.com. type A".
Why would this message appear as an audit?
A. The DNS was not learned as part of the Container model or added to the DNS allow list.
B. This is a DNS known to be a source of malware.
C. The process calling out to this domain was not part of the Container model.
D. The Layer7 firewall detected this as anomalous behavior.
Answer: A
Explanation:
The runtime audit message indicating "DNS resolution of suspicious name wikipedia.com. type A" would appear as an audit because the DNS was not learned as part of the Container model or added

to the DNS allow list (option A). In cloud security platforms like Prisma Cloud, runtime protection policies monitor the behavior of running containers and compare it against a learned model of expected behavior. If a container attempts to resolve a DNS name that was not observed during the learning phase or specifically allowed, it triggers an audit event to alert security teams of potentially malicious activity.

NO.11 A customer wants to scan a serverless function as part of a build process. Which twistcli command can be used to scan serverless functions?

A. twistcli function scan <SERVERLESS_FUNCTION.ZIP>

B. twistcli scan serverless <SERVERLESS_FUNCTION.ZIP>

C. twistcli serverless AWS <SERVERLESS_FUNCTION.ZIP>

D. twiscli serverless scan <SERVERLESS_FUNCTION.ZIP>

Answer: D

Explanation:

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

NO.12 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:

https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin-compute/vulnerability_managemen Configuring vulnerability policies within Prisma Cloud involves several options that cater to different aspects of vulnerability management and policy enforcement. Options A, C, and D are valid configurations for vulnerability policies:

A: Individual actions based on package type allow for tailored responses to vulnerabilities found in specific types of software packages, enabling more granular control over the remediation process.

C: Applying policies only when a vendor fix is available helps prioritize the remediation of vulnerabilities for which a patch or update has been released by the software vendor, ensuring efficient use of resources in addressing the most actionable security issues.

D: Setting individual grace periods for each severity level allows organizations to define different time frames for addressing vulnerabilities based on their severity, enabling a prioritized and risk-based approach to vulnerability management.

These configurations support a comprehensive vulnerability management strategy by allowing customization and prioritization based on the nature of the vulnerability, the availability of fixes, and the risk level associated with each vulnerability.

NO.13 Web-Application and API Security (WAAS) provides protection for which two protocols?

(Choose two.)

A. HTTP

B. SSH

C. Tomcat Web Connector via AJP

D. TLS

Answer: A D

Explanation:

Web-Application and API Security (WAAS) is a feature within Prisma Cloud that focuses on protecting web applications and APIs from various threats and vulnerabilities. The primary protocols it provides protection for are HTTP (Hypertext Transfer Protocol) and TLS (Transport Layer Security). HTTP is the foundation of data communication for the World Wide Web, and TLS is a cryptographic protocol designed to provide communications security over a computer network. While SSH (Secure Shell) is a protocol for secure remote login and other secure network services, and Tomcat Web Connector via AJP (Apache JServ Protocol) is used for Tomcat server communication, they are not the primary focus of WAAS protection.

NO.14 The security team wants to protect a web application container from an SQLi attack. Which type of policy should the administrator create to protect the container?

A. CNAF

B. Runtime

C. Compliance

D. CNNF

Answer: A

Explanation:

To protect a web application container from an SQL Injection (SQLi) attack, the administrator should create a Cloud Native Application Firewall (CNAF) policy. CNAF policies are designed to protect applications running in containers from various types of attacks, including SQLi, by inspecting the traffic going to and from the containerized applications and blocking malicious requests.

NO.15 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.16 An administrator has been tasked with a requirement by your DevSecOps team to write a script to continuously query programmatically the existing users, and the user's associated permission levels, in a Prisma Cloud Enterprise tenant.
Which public documentation location should be reviewed to help determine the required attributes to carry out this step?

A. Prisma Cloud Administrator's Guide (Compute)

B. Prisma Cloud API Reference

C. Prisma Cloud Compute API Reference

D. Prisma Cloud Enterprise Administrator's Guide

Answer: B

Explanation:
Prisma Cloud has a REST API that enables you to access Prisma Cloud features programmatically. Most actions supported on the Prisma Cloud web interface are available with the REST API, refer to the Prisma Cloud REST API Reference for details about the REST API. https://pan.dev/prisma-cloud/api/cspm/ For scripting and programmatically querying user data and associated permission levels in a Prisma Cloud Enterprise tenant, the Prisma Cloud API Reference is the most relevant documentation. This reference guide provides detailed information on the available APIs, including those for user and permissions management. It outlines the necessary attributes, endpoints, and methods required to programmatically interact with the Prisma Cloud platform.
The API Reference is designed to help developers and administrators understand how to leverage the Prisma Cloud APIs to automate tasks, such as querying existing users and their permission levels. It includes examples and explanations that are crucial for writing effective scripts that integrate with the Prisma Cloud infrastructure.
While the Administrator's Guides provide valuable information on managing the platform, the API Reference is specifically tailored for developers looking to automate and script interactions with Prisma Cloud services.
Therefore, reviewing the Prisma Cloud API Reference will provide the necessary details to fulfill the DevSecOps team's requirement1.

NO.17 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.

NO.18 What are two built-in RBAC permission groups for Prisma Cloud? (Choose two.)

A. Group Membership Admin

B. Group Admin

C. Account Group Admin

D. Account Group Read Only

Answer: A C

Explanation:

Prisma Cloud includes built-in Role-Based Access Control (RBAC) permission groups to manage user access and permissions efficiently. Among the options, Group Membership Admin and Account Group Admin are two built-in RBAC permission groups. Group Membership Admins are responsible for managing user memberships within groups, while Account Group Admins have administrative privileges over specific account groups, allowing them to manage resources and policies within those groups. These roles help in delegating administrative tasks and enforcing the principle of least privilege.

NO.19 What is the function of the external ID when onboarding a new Amazon Web Services (AWS) account in Prisma Cloud?

A. It is a unique identifier needed only when Monitor & Protect mode is selected.

B. It is the resource name for the Prisma Cloud Role.

C. It is a UUID that establishes a trust relationship between the Prisma Cloud account and the AWS account in order to extract data.

D. It is the default name of the PrismaCloudApp stack.

Answer: C

Explanation:

The external ID plays a crucial role when onboarding a new Amazon Web Services (AWS) account in Prisma Cloud. It serves as a UUID (Universally Unique Identifier) that establishes a trust relationship between the Prisma Cloud account and the AWS account. This trust relationship is essential for allowing Prisma Cloud to securely extract data and perform security monitoring and compliance checks within the AWS environment.

The use of an external ID ensures that Prisma Cloud can access the necessary information from the AWS account without compromising the security of the AWS account's credentials, adhering to the principle of least privilege and enhancing the overall security posture.

NO.20 What are the three states of the Container Runtime Model? (Choose three.)

A. Initiating

B. Learning

C. Active

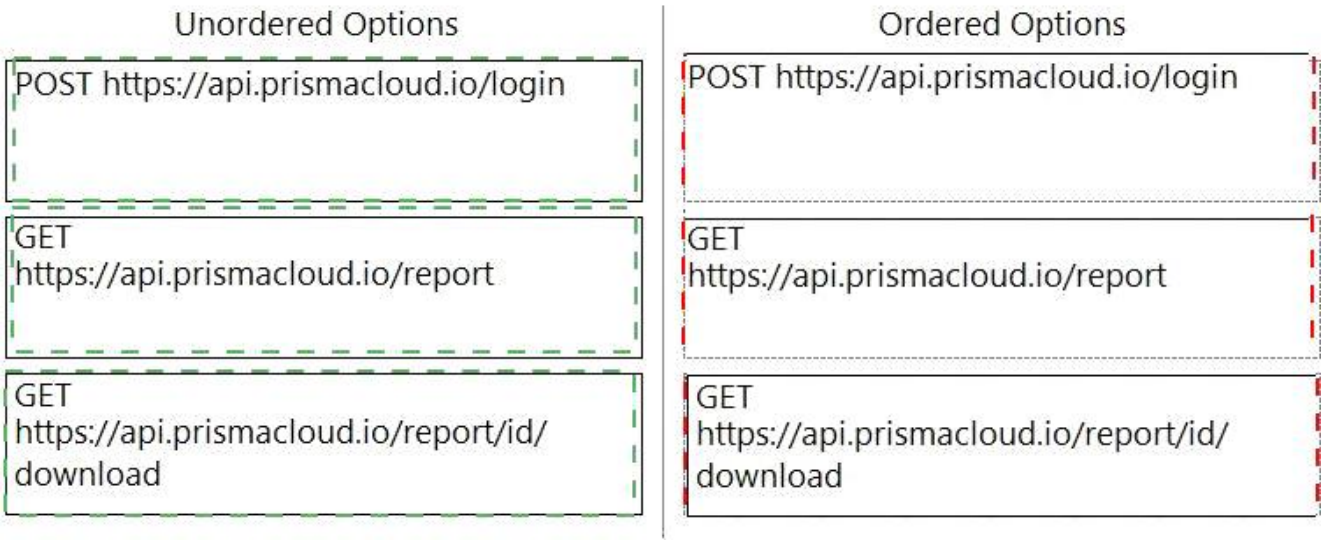
D. Running
E. Archived
Answer: B C E
Explanation:
The Container Runtime Model in Prisma Cloud typically includes states such as Learning, Active, and Archived. The Learning state is where Prisma Cloud observes container behaviors to understand normal operations and establish a baseline. During this phase, 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.21 An administrator has been tasked with creating a custom service that will download any existing compliance report from a Prisma Cloud Enterprise tenant.
In which order will the APIs be executed for this service?
(Drag the steps into the correct order of occurrence, from the first step to the last.)
Answer Area

Unordered Options	Ordered Options
POST https://api.prismacloud.io/login	
GET https://api.prismacloud.io/report	
GET https://api.prismacloud.io/report/id/download	

Answer:

Answer Area



Explanation:
1. Post /Login 2. Get /report 3. Get report/id/download

NO.22 Based on the following information, which RQL query will satisfy the requirement to identify VM hosts deployed to organization public cloud environments exposed to network traffic from the internet and affected by Text4Shell RCE (CVE-2022-42889) vulnerability?
* Network flow logs from all virtual private cloud (VPC) subnets are ingested to the Prisma Cloud Enterprise Edition tenant.
* All virtual machines (VMs) have Prisma Cloud Defender deployed.
A)
B)
C)
D)
A. Option A
B. Option B
C. Option C
D. Option D
Answer: A
Explanation:
The RQL query in Option A is designed to identify VM hosts that are exposed to internet traffic and are affected by the Text4Shell RCE vulnerability (CVE-2022-42889). This query looks for network flow records with byte transfers indicating activity and filters for resources with host vulnerability findings sourced from
'Prisma Cloud'. It also checks for exposure to suspicious or internet IPs, satisfying the criteria for the given scenario.

NO.23 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.24 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:

For Prisma Cloud to execute auto-remediation commands, it requires write access to the cloud platform. This is because auto-remediation involves making changes to configurations or settings within the cloud environment to rectify security issues. Thus, the correct answer is B: Write access to the cloud platform.

NO.25 In Prisma Cloud for Azure Net Effective Permissions Calculation, the following Azure permission levels are supported by which three permissions? (Choose three).

A. Resources

B. Tenant

C. Subscription

D. Resource groups

E. Management Group

Answer: A C E

Explanation:

https://docs.prismacloud.io/en/classic/cspm-admin-guide/prisma-cloud-iam-security/context-used-to-calculate-ef

NO.26 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 designed to integrate security into the DevOps process by scanning infrastructure as code (IaC) templates and configurations for potential security issues. This proactive

approach allows developers and security teams to address misconfigurations and vulnerabilities in the code itself, before they are deployed into the cloud environment and become more challenging to resolve. By identifying and rectifying these issues early in the development lifecycle, organizations can reduce the risk of alerts and incidents arising from misconfigurations in their cloud infrastructure, leading to a more secure and compliant cloud environment.