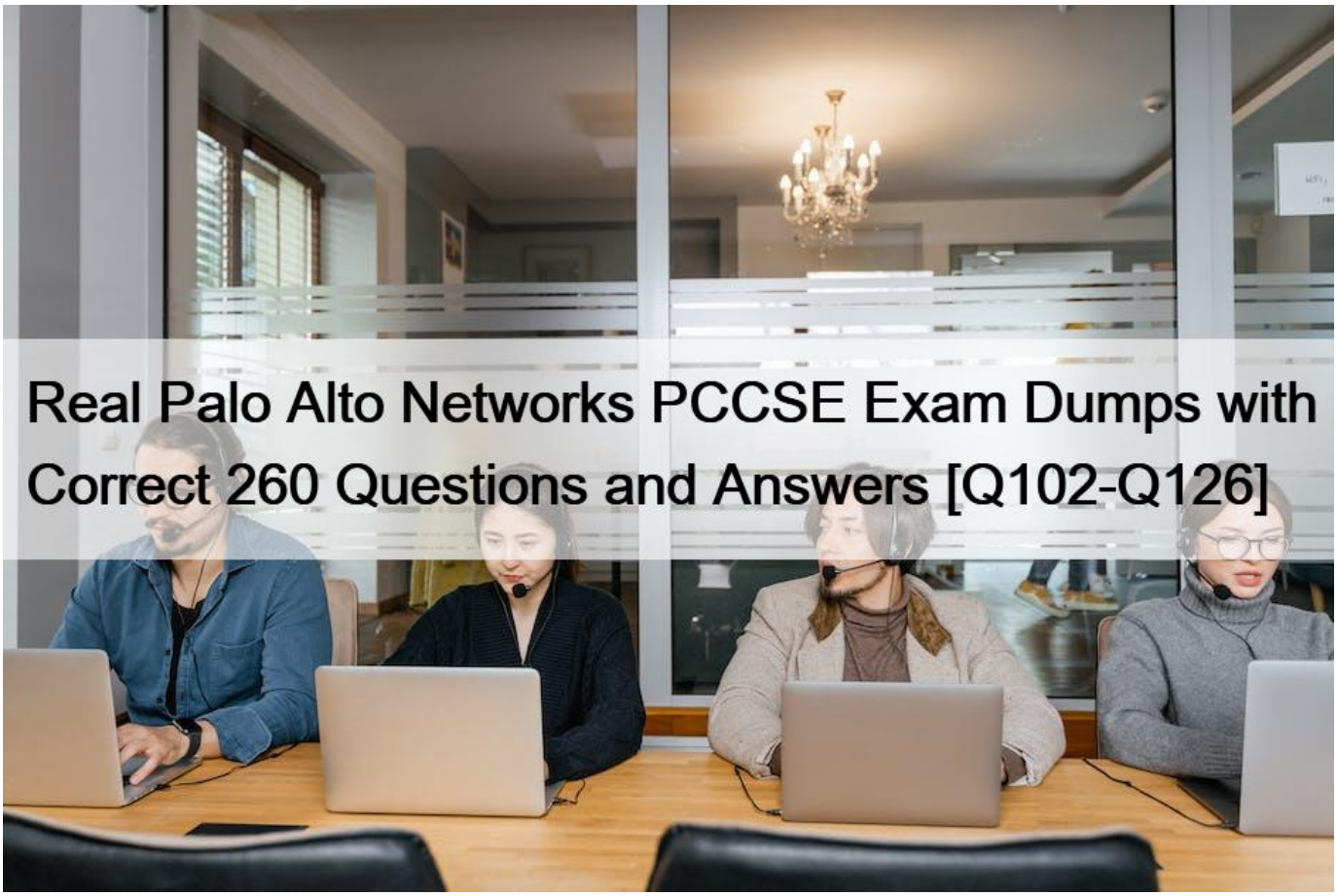
Real Palo Alto Networks PCCSE Exam Dumps with Correct 260 Questions and Answers [Q102-Q126

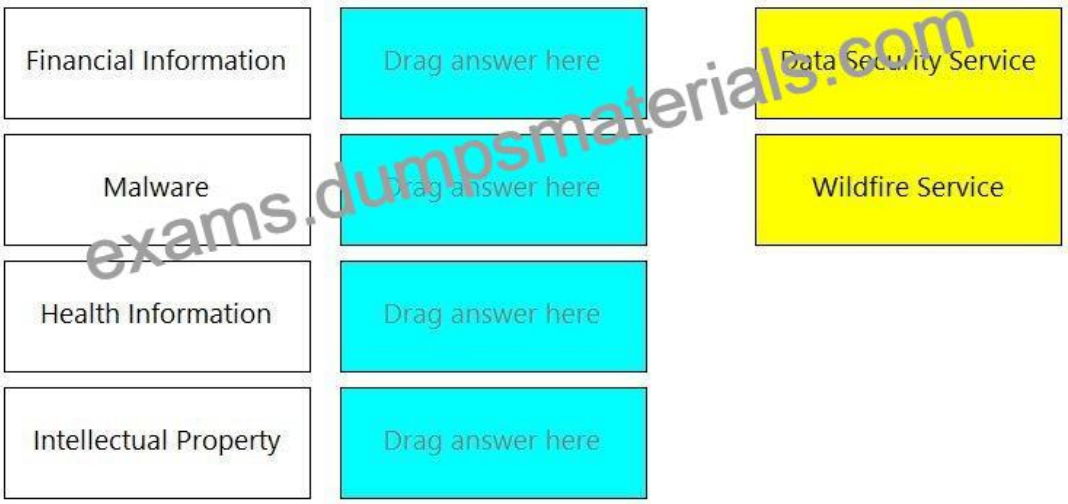


Real Palo Alto Networks PCCSE Exam Dumps with Correct 260 Questions and Answers
Valid PCCSE Test Answers & Palo Alto Networks PCCSE Exam PDF

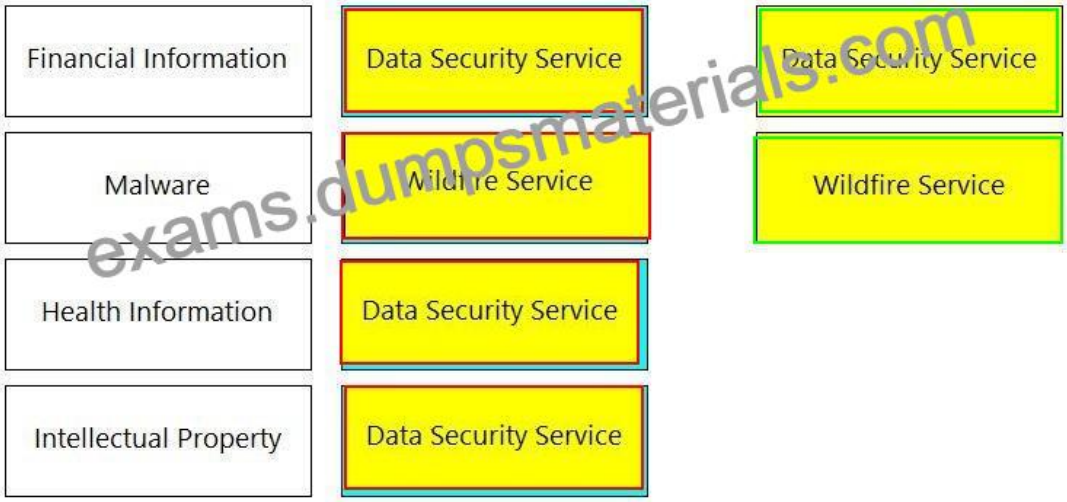
NO.102 Match the service on the right that evaluates each exposure type on the left.

(Select your answer from the pull-down list. Answers may be used more than once or not at all.)

Answer Area



Answer Area



Reference:

https://www.paloaltonetworks.com/prisma/cloud/cloud-data-security

NO.103 Which two variables must be modified to achieve automatic remediation for identity and access management (IAM) alerts in Azure cloud? (Choose two.)
* SQS_QUEUE_NAME
* SB_QUEUE_KEY
* YOUR_ACCOUNT_NUMBER
* API_ENDPOINT

NO.104 Which type of compliance check is available for rules under Defend > Compliance > Containers and Images

> CI?
* Container
* Image

* Host
* Functions

NO.105 Which “kind” of Kubernetes object is configured to ensure that Defender is acting as the admission controller?
* MutatingWebhookConfiguration
* DestinationRules
* ValidatingWebhookConfiguration
* PodSecurityPolicies

In the context of Kubernetes, an admission controller is a piece of code that intercepts requests to the Kubernetes API server before the persistence of the object, but after the request is authenticated and authorized. The admission controller lets you apply complex validation and policy controls to objects before they are created or updated.

The ValidatingWebhookConfiguration is a Kubernetes object that tells the API server to send an admission validation request to a service (the admission webhook) when a request to create, update, or delete a Kubernetes object matches the rules defined in the configuration. The webhook can then approve or deny the request based on custom logic.

The MutatingWebhookConfiguration is similar but is used to modify objects before they are created or updated, which is not the primary function of an admission controller acting in a protective or validating capacity.

DestinationRules are related to Istio service mesh and are not relevant to Kubernetes admission control.

PodSecurityPolicies (PSPs) are a type of admission controller in Kubernetes but they are predefined by Kubernetes and do not require a specific configuration object like ValidatingWebhookConfiguration. PSPs are also deprecated in recent versions of Kubernetes.

Therefore, the correct answer is C. ValidatingWebhookConfiguration, as it is the Kubernetes object used to configure admission webhooks for validating requests, which aligns with the role of Defender acting as an admission controller in Prisma Cloud.

Reference from the provided documents:

The documents uploaded do not contain specific details about Kubernetes objects or Prisma Cloud’s integration with Kubernetes. However, this explanation aligns with general Kubernetes practices and Prisma Cloud’s capabilities in securing Kubernetes environments.

NO.106 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?
* Prisma Cloud Administrator’s Guide (Compute)
* Prisma Cloud API Reference
* Prisma Cloud Compute API Reference
* Prisma Cloud Enterprise Administrator’s Guide

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.107 Which role does Prisma Cloud play when configuring SSO?
* JIT
* Service provider
* SAML
* Identity provider issuer

When configuring Single Sign-On (SSO) in Prisma Cloud, the platform acts as the Service Provider (SP). In the SSO process, the Service Provider relies on an Identity Provider (IdP) to authenticate users. Prisma Cloud, as the SP, integrates with an IdP to allow users to log in using their existing credentials managed by the IdP.

This setup simplifies the authentication process, enhances security by centralizing user credentials, and provides a seamless user experience.

NO.108 Which command should be used in the Prisma Cloud twistcli tool to scan the nginx:latest image for vulnerabilities and compliance issues?

A)

B)

```
$ twistcli images scan
--address <COMPUTE_CONSOLE>
--username <COMPUTE_CONSOLE_USER>
--password <COMPUTE_CONSOLE_PASSWD>
--details
nginx:latest
```

C)

```
$ twistcli images scan
--address <COMPUTE_CONSOLE>
--user <COMPUTE_CONSOLE_USER>
--password <COMPUTE_CONSOLE_PASSWD>
--details
nginx:latest
```

D)

* Option A
* Option B
* Option C
* Option D

The correct command to scan the nginx:latest image for vulnerabilities and compliance issues using the Prisma Cloud twistcli tool is shown in Option D. This command uses twistcli images scan with specified parameters for the console address, username, and password, and it outputs the results to a file named scan- results.json. This allows for the scanning results to be saved and reviewed in a structured format, which aids in further analysis and tracking of vulnerabilities and compliance issues.

NO.109 Per security requirements, an administrator needs to provide a list of people who are receiving e-mails for Prisma Cloud alerts.

Where can the administrator locate this list of e-mail recipients?
* Target section within an Alert Rule.
* Notification Template section within Alerts.
* Users section within Settings.
* Set Alert Notification section within an Alert Rule.

NO.110 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?
* an event within the cloud account
* network traffic to the S3 bucket
* configuration of the S3 bucket
* anomalous behaviors

NO.111 Which three steps are involved in onboarding an account for Data Security? (Choose three.)
* Create a read-only role with in-line policies
* Create a Cloudtrail with SNS Topic
* Enable Flow Logs
* Enter the RoleARN and SNSARN
* Create a S3 bucket

Onboarding an account for Data Security involves several critical steps to ensure comprehensive coverage and effective monitoring. The steps involved include B. Create a Cloudtrail with SNS Topic to track and manage API calls and relevant notifications, D. Enter the RoleARN and SNSARN to provide necessary access and integration points for data security functions, and E. Create a S3 bucket which serves as a storage solution for logging and data capture essential for security analysis.

NO.112 Which three types of runtime rules can be created? (Choose three.)
* Processes
* Network-outgoing
* Filesystem
* Kubernetes-audit
* Waas-request

In Prisma Cloud, runtime rules are created to monitor and control the behavior of applications and services during their execution to ensure compliance with security policies. The three types of runtime rules that can be created in Prisma Cloud are:

Processes: These rules monitor and control the execution of processes within the environment. They can be used to detect unauthorized or malicious processes and take actions such as alerting, blocking, or terminating the processes.

Network-outgoing: These rules govern the outbound network connections from the applications or containers. They help in controlling access to external resources, preventing data exfiltration, and ensuring that the communication complies with the security policies.

Filesystem: Filesystem rules are related to the access and modification of the file system by applications or containers. These rules can help in detecting unauthorized access, changes to sensitive files, and ensuring that the applications adhere to the least privilege principle in terms of file access.

These runtime rules are essential for maintaining the security and integrity of applications running in cloud environments, especially in dynamic and distributed architectures where traditional perimeter-based security controls may not be sufficient.

NO.113 Given this information:

The Console is located at https://prisma-console.mydomain.local The username is: cluster The password is: password123 The image to scan is: myimage:latest Which twistcli command should be used to scan a Container for vulnerabilities and display the details about each vulnerability?
* twistcli images scan –address https://prisma-console.mydomain.local -u cluster -p password123 –details myimage:latest
* twistcli images scan –console-address prisma-console.mydomain.local -u cluster -p password123 — vulnerability-details myimage:latest
* twistcli images scan –console-address https://prisma-console.mydomain.local -u cluster -p password123 — details myimage:latest
* twistcli images scan –address prisma-console.mydomain.local -u cluster -p password123 –vulnerability- details myimage:latest

NO.114 The Unusual protocol activity (Internal) network anomaly is generating too many alerts. An administrator has been asked to tune it to the option that will generate the least number of events without disabling it entirely.

Which strategy should the administrator use to achieve this goal?
* Disable the policy
* Set the Alert Disposition to Conservative
* Change the Training Threshold to Low
* Set Alert Disposition to Aggressive

Section: (none)

Explanation

NO.115 In Prisma Cloud Software Release 22.06 (Kepler), which Registry type is added?
* Sonatype Nexus
* Google Artifact Registry
* Azure Container Registry
* IBM Cloud Container Registry

NO.116 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?
* set the Container model to manual relearn and set the default runtime rule to block for process protection.
* set the Container model to relearn and set the default runtime rule to prevent for process protection.
* 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”.
* choose “copy into rule” for the Container, add a ransomWare process into the denied process list, and set the action to “block”.
https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin-compute/runtime_defense/runtime_

NO.117 Which ROL query is used to detect certain high-risk activities executed by a root user in AWS?
* event from cloud.audit_logs where operation IN (‘ChangePassword’, ‘ConsoleLogin’,

‘DeactivateMFADevice’, ‘DeleteAccessKey’ , ‘DeleteAlarms’) AND user = ‘root’
* event from cloud.security_logs where operation IN (‘ChangePassword’, ‘ConsoleLogin’,

‘DeactivateMFADevice’, ‘DeleteAccessKey’ , ‘DeleteAlarms’) AND user = ‘root’
* config from cloud.audit_logs where operation IN (‘ChangePassword’, ‘ConsoleLogin’,

‘DeactivateMFADevice’, ‘DeleteAccessKey’, ‘DeleteAlarms’) AND user = ‘root’
* event from cloud.audit_logs where Risk.Level = ‘high’ AND user = ‘root’
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

NO.118 Console is running in a Kubernetes cluster, and you need to deploy Defenders on nodes within this cluster.

Which option shows the steps to deploy the Defenders in Kubernetes using the default Console service name?
* From the deployment page in Console, choose pod name for Console identifier, generate DaemonSet file, and apply the DaemonSet to twistlock namespace.
* From the deployment page configure the cloud credential in Console and allow cloud discovery to auto-protect the Kubernetes nodes.
* From the deployment page in Console, choose twistlock-console for Console identifier, and run the curl | bash script on the master Kubernetes node.
* From the deployment page in Console, choose twistlock-console for Console identifier, generate DaemonSet file, and apply DaemonSet to the twistlock namespace.

NO.119 Which alerts are fixed by enablement of automated remediation?
* All applicable open alerts regardless of when they were generated, with alert status updated to “resolved”
* Only the open alerts that were generated before the enablement of remediation, with alert status updated to “resolved”
* All applicable open alerts regardless of when they were generated, with alert status updated to “dismissed”
* Only the open alerts that were generated after the enablement of remediation, with alert status updated to “resolved”
When automated remediation is enabled in Prisma Cloud, it is designed to address all applicable open alerts, regardless of when they were generated. The system automatically applies remediation actions to resolve the identified security issues or compliance

violations that triggered the alerts. Once the remediation actions are successfully completed, the system updates the status of the affected alerts to “resolved,” indicating that the security issues have been addressed. This feature helps streamline the remediation process, reducing the manual effort required by security teams and ensuring that security issues are promptly resolved to maintain the integrity and security of the cloud environment.

NO.120 Which statement accurately characterizes SSO Integration on Prisma Cloud?
* Prisma Cloud supports IdP initiated SSO, and its SAML endpoint supports the POST and GET methods.
* Okta, Azure Active Directory, PingID, and others are supported via SAML.
* An administrator can configure different Identity Providers (IdP) for all the cloud accounts that Prisma Cloud monitors.
* An administrator who needs to access the Prisma Cloud API can use SSO after configuration.

NO.121 A customer is reviewing Container audits, and an audit has identified a cryptominer attack. Which three options could have generated this audit? (Choose three.)
* The value of the mined currency exceeds $100.
* High CPU usage over time for the container is detected.
* Common cryptominer process name was found.
* The mined currency is associated with a user token.
* Common cryptominer port usage was found.

NO.122 Which component(s), if any, will Palo Alto Networks host and run when a customer purchases Prisma Cloud Enterprise Edition?
* Defenders
* Console
* Jenkins
* twistcli

In Prisma Cloud Enterprise Edition, Palo Alto Networks hosts and runs the Console component. The Console serves as the central management interface for Prisma Cloud, allowing customers to configure policies, view alerts, and manage their cloud security posture without the need to host this component themselves.

NO.123 Which Prisma Cloud policy type can protect against malware?
* Event
* Network
* Config
* Data

The “Data” policy type in Prisma Cloud is specifically designed to protect against threats related to data, including malware. These policies focus on securing data at rest and in transit, implementing data loss prevention (DLP) mechanisms, and scanning data stores and payloads for malicious content. By employing data policies, Prisma Cloud ensures that data stored within cloud environments is safeguarded against unauthorized access, exfiltration, and malware, thereby maintaining the integrity and confidentiality of sensitive information.

NO.124 You are an existing customer of Prisma Cloud Enterprise. You want to onboard a public cloud account and immediately see all of the alerts associated with this account based off ALL of your tenant’s existing enabled policies. There is no requirement to send alerts from this account to a downstream application at this time.

Which options shows the steps required during the alert rule creation process to achieve this objective?
* Ensure the public cloud account is assigned to an account group

Assign the confirmed account group to alert rule

Select one or more policies as part of the alert rule

Add alert notifications

Confirm the alert rule
* Ensure the public cloud account is assigned to an account group

Assign the confirmed account group to alert rule

Select one or more policies checkbox as part of the alert rule

Confirm the alert rule
* Ensure the public cloud account is assigned to an account group

Assign the confirmed account group to alert rule

Select “select all policies” checkbox as part of the alert rule

Confirm the alert rule
* Ensure the public cloud account is assigned to an account group

Assign the confirmed account group to alert rule

Select “select all policies” checkbox as part of the alert rule

Add alert notifications

Confirm the alert rule

NO.125 Given a default deployment of Console, a customer needs to identify the alerted compliance checks that are set by default Where should the customer navigate in Console?
* Defend > Compliance
* Manage > Compliance
* Monitor > Compliance
* Custom > Compliance

NO.126 A security team is deploying Cloud Native Application Firewall (CNAF) on a containerized web application. The application is running an NGINX container. The container is listening on port 8080 and is mapped to host port 80.

Which port should the team specify in the CNAF rule to protect the application?
* 443
* 80
* 8080
* 8888

PCCSE Exam Questions and Valid PMP Dumps PDF: https://www.dumpsmaterials.com/PCCSE-real-torrent.html]