

Paloalto-Networks

Exam Questions PCCSE

Prisma Certified Cloud Security Engineer



NEW QUESTION 1

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?

- A. twistcli images scan --console-address <https://prisma-console.mydomain.local> -u cluster -p password123-- details myimage:latest
- B. twistcli images scan --console-address prisma-console.mydomain.local -u cluster -p password123 -- vulnerability-details myimage:latest
- C. twistcli images scan --address prisma-console.mydomain.local -u cluster -p password123--vulnerability- details myimage:latest
- D. twistcli images scan --address <https://prisma-console.mydomain.local> -u cluster -p password123 --details myimage:latest

Answer: C

NEW QUESTION 2

An administrator sees that a runtime audit has been generated for a host. The audit message is:

“Service postfix attempted to obtain capability SHELL by executing /bin/sh /usr/libexec/postfix/postfix- script.stop. Low severity audit, event is automatically added to the runtime model”

Which runtime host policy rule is the root cause for this runtime audit?

- A. Custom rule with specific configuration for file integrity
- B. Custom rule with specific configuration for networking
- C. Default rule that alerts on capabilities
- D. Default rule that alerts on suspicious runtime behavior

Answer: D

NEW QUESTION 3

Which option shows the steps to install the Console in a Kubernetes Cluster?

- A. Download the Console and Defender image Generate YAML for Defender Deploy Defender YAML using kubectl
- B. Download and extract release tarball Generate YAML for Console Deploy Console YAML using kubectl
- C. Download the Console and Defender image Download YAML for Defender from the document site Deploy Defender YAML using kubectl
- D. Download and extract release tarball Download the YAML for Console Deploy Console YAML using kubectl

Answer: B

NEW QUESTION 4

What is the behavior of Defenders when the Console is unreachable during upgrades?

- A. Defenders continue to alert, but not enforce, using the policies and settings most recently cached before upgrading the Console.
- B. Defenders will fail closed until the web-socket can be re-established.
- C. Defenders will fail open until the web-socket can be re-established.
- D. Defenders continue to alert and enforce using the policies and settings most recently cached before upgrading the Console.

Answer: D

NEW QUESTION 5

The security auditors need to ensure that given compliance checks are being run on the host. Which option is a valid host compliance policy?

- A. Ensure functions are not overly permissive.
- B. Ensure host devices are not directly exposed to containers.
- C. Ensure images are created with a non-root user.
- D. Ensure compliant Docker daemon configuration.

Answer: C

NEW QUESTION 6

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 Area

Unordered Options	Ordered Options
Add the custom compliance standard from the drop-down menu	
Create the custom compliance standard	
Edit the Policy	
Click on Compliance Standards	

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:
Diagram Description automatically generated

NEW QUESTION 7

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	

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:
A picture containing graphical user interface Description automatically generated

NEW QUESTION 8

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: C

NEW QUESTION 9

Which three types of classifications are available in the Data Security module? (Choose three.)

- A. Personally identifiable information
- B. Malicious IP
- C. Compliance standard
- D. Financial information

E. Malware

Answer: CDE

NEW QUESTION 10

An administrator needs to write a script that automatically deactivates access keys that have not been used for 30 days. In which order should the API calls be used to accomplish this task? (Drag the steps into the correct order from the first step to the last.) Select and Place:

Answer Area

Unordered Options	Ordered Options
POST https://api.prismacloud.io/login	
GET https://api.prismacloud.io/access_keys	
PATCH https://api.prismacloud.io/access_keys/<id>/status/<status>	

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

A picture containing graphical user interface Description automatically generated

NEW QUESTION 10

A customer is interested in PCI requirements and needs to ensure that no privilege containers can start in the environment. Which action needs to be set for “do not use privileged containers”?

- A. Prevent
- B. Alert
- C. Block
- D. Fail

Answer: A

NEW QUESTION 15

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

NEW QUESTION 18

Which type of compliance check is available for rules under Defend > Compliance > Containers and Images > CI?

- A. Host
- B. Container
- C. Functions
- D. Image

Answer: B

NEW QUESTION 19

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

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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:
A picture containing table Description automatically generated

NEW QUESTION 24

An organization wants to be notified immediately to any “High Severity” alerts for the account group “Clinical Trials” via Slack. Which option shows the steps the organization can use to achieve this goal?

- A. * 1. Configure Slack Integration* 2. Create an alert rule and select “Clinical Trials” as the account group * 3.Under the “Select Policies” tab, filter on severity and select “High” * 4.Under the Set Alert Notification tab, choose Slack and populate the channel * 5.Set Frequency to “As it Happens”
- B. * 1. Create an alert rule and select “Clinical Trials” as the account group * 2.Under the “Select Policies” tab, filter on severity and select “High” * 3.Under the Set Alert Notification tab, choose Slack and populate the channel * 4.Set Frequency to “As it Happens”* 5.Set up the Slack Integration to complete the configuration
- C. * 1. Configure Slack Integration * 2.Create an alert rule* 3.Under the “Select Policies” tab, filter on severity and select “High” * 4.Under the Set Alert Notification tab, choose Slack and populate the channel* 5.Set Frequency to “As it Happens”
- D. * 1. Under the “Select Policies” tab, filter on severity and select “High” * 2.Under the Set Alert Notification tab, choose Slack and populate the channel * 3.Set Frequency to “As it Happens”* 4.Configure Slack Integration * 5.Create an Alert rule

Answer: B

NEW QUESTION 26

Order the steps involved in onboarding an AWS Account for use with Data Security feature.

Answer Area

Unordered Options	Ordered Options
Enter RoleARN and SNSARN	
Create Stack	
Enter SNS Topic in CloudTrail	
Create CloudTrail with S3 as storage	

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:
Table Description automatically generated with medium confidence

NEW QUESTION 29

You wish to create a custom policy with build and run subtypes. Match the query types for each example. (Select your answer from the pull-down list. Answers

may be used more than once or not at all.)

Answer Area

config where cloud.type = 'aws'	Drag answer here	Run
\$.resource[*].aws_s3_ bucket exists	Drag answer here	Build
RQL type	Drag answer here	
JSON query type	Drag answer here	

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

config where cloud.type = 'aws'	Run	Run
\$.resource[*].aws_s3_ bucket exists	Run	Build
RQL type	Build	
JSON query type	Build	

NEW QUESTION 30

The administrator wants to review the Console audit logs from within the Console.
Which page in the Console should the administrator use to review this data, if it can be reviewed at all?

- A. Navigate to Monitor > Events > Host Log Inspection
- B. The audit logs can be viewed only externally to the Console
- C. Navigate to Manage > Defenders > View Logs
- D. Navigate to Manage > View Logs > History

Answer: D

NEW QUESTION 34

Which option identifies the Prisma Cloud Compute Edition?

- A. Package installed with APT
- B. Downloadable, self-hosted software
- C. Software-as-a-Service (SaaS)
- D. Plugin to Prisma Cloud

Answer: B

NEW QUESTION 36

A customer has Prisma Cloud Enterprise and host Defenders deployed.
What are two options that allow an administrator to upgrade Defenders? (Choose two.)

- A. with auto-upgrade, the host Defender will auto-upgrade.
- B. auto deploy the Lambda Defender.
- C. click the update button in the web-interface.
- D. generate a new DaemonSet file.

Answer: AD

NEW QUESTION 38

Given an existing ECS Cluster, which option shows the steps required to install the Console in Amazon ECS?

- A. The console cannot natively run in an ECS cluste
- B. A onebox deployment should be used.
- C. Download and extract the release tarballEnsure that each node has its own storage for Console data Create the Console task definition Deploy the task definition
- D. Download and extract release tarball Download task from AWS Create the Console task definition Deploy the task definition
- E. Download and extract the release tarballCreate an EFS file system and mount to each node in the cluster Create the Console task definition Deploy the task definition

Answer: D

NEW QUESTION 41

Which three types of buckets exposure are available in the Data Security module? (Choose three.)

- A. Public
- B. Private
- C. International
- D. Differential
- E. Conditional

Answer: CDE

NEW QUESTION 43

Which options show the steps required to upgrade Console when using projects?

- A. Upgrade all Supervisor Consoles Upgrade Central Console
- B. Upgrade Central ConsoleUpgrade Central Console Defenders
- C. Upgrade Defender Upgrade Central Console Upgrade Supervisor Consoles
- D. Upgrade Central Console Upgrade all Supervisor Consoles

Answer: A

NEW QUESTION 48

What is an example of an outbound notification within Prisma Cloud?

- A. AWS Inspector
- B. Qualys
- C. Tenable
- D. PagerDuty

Answer: D

NEW QUESTION 52

Which options show the steps required after upgrade of Console?

- A. Uninstall Defenders Upgrade Jenkins Plugin Upgrade twistcli where applicableAllow the Console to redeploy the Defender
- B. Update the Console image in the Twistlock hosted registry Update the Defender image in the Twistlock hosted registry Uninstall Defenders
- C. Upgrade Defenders Upgrade Jenkins Plugin Upgrade twistcli where applicable
- D. Update the Console image in the Twistlock hosted registry Update the Defender image in the Twistlock hosted registry Redeploy Console

Answer: C

NEW QUESTION 57

A DevOps lead reviewed some system logs and notices some odd behavior that could be a data exfiltration attempt. The DevOps lead only has access to vulnerability data in Prisma Cloud Compute, so the DevOps lead passes this information to SecOps.

Which pages in Prisma Cloud Compute can the SecOps lead use to investigate the runtime aspects of this attack?

- A. The SecOps lead should investigate the attack using Vulnerability Explorer and Runtime Radar.
- B. The SecOps lead should use Incident Explorer and Compliance Explorer.
- C. The SecOps lead should use the Incident Explorer page and Monitor > Events > Container Audits.
- D. The SecOps lead should review the vulnerability scans in the CI/CD process to determine blame.

Answer: B

NEW QUESTION 62

Which “kind” of Kubernetes object is configured to ensure that Defender is acting as the admission controller?

- A. MutatingWebhookConfiguration
- B. DestinationRules
- C. ValidatingWebhookConfiguration
- D. PodSecurityPolicies

Answer: C

NEW QUESTION 66

A customer has Defenders connected to Prisma Cloud Enterprise. The Defenders are deployed as a DaemonSet in OpenShift. How should the administrator get a report of vulnerabilities on hosts?

- A. Navigate to Monitor > Vulnerabilities > CVE Viewer
- B. Navigate to Defend > Vulnerabilities > VM Images
- C. Navigate to Defend > Vulnerabilities > Hosts
- D. Navigate to Monitor > Vulnerabilities > Hosts

Answer: D

NEW QUESTION 71

An administrator has access to a Prisma Cloud Enterprise. What are the steps to deploy a single container Defender on an ec2 node?

- A. Pull the Defender image to the ec2 node, copy and execute the curl | bash script, and start the Defender to ensure it is running.
- B. Execute the curl | bash script on the ec2 node.
- C. Configure the cloud credential in the console and allow cloud discovery to auto-protect the ec2 node.
- D. Generate DaemonSet file and apply DaemonSet to the twistlock namespace.

Answer: D

NEW QUESTION 75

A security team has been asked to create a custom policy. Which two methods can the team use to accomplish this goal? (Choose two.)

- A. add a new policy
- B. clone an existing policy
- C. disable an out-of-the-box policy
- D. edit the query in the out-of-the-box policy

Answer: AB

NEW QUESTION 77

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

NEW QUESTION 78

.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questions and Answers in PDF Format

PCCSE Practice Exam Features:

- * PCCSE Questions and Answers Updated Frequently
- * PCCSE Practice Questions Verified by Expert Senior Certified Staff
- * PCCSE Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- * PCCSE Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

100% Actual & Verified — Instant Download, Please Click
[Order The PCCSE Practice Test Here](#)