

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 three options are selectable in a CI policy for image scanning with Jenkins or twistcli? (Choose three.)

- A. Scope - Scans run on a particular host
- B. Credential
- C. Apply rule only when vendor fixes are available
- D. Failure threshold
- E. Grace Period

Answer: BDE

NEW QUESTION 4

How are the following categorized?

Backdoor account access Hijacked processes Lateral movement Port scanning

- A. audits
- B. incidents
- C. admission controllers
- D. models

Answer: B

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 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: AB

NEW QUESTION 7

Which port should a security team use to pull data from Console's API?

- A. 53
- B. 25

C. 8084
D. 8083

Answer: D

NEW QUESTION 8

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

Financial Information	Drag answer here	Data Security Service
Malware	Drag answer here	Wildfire Service
Health Information	Drag answer here	
Intellectual Property	Drag answer here	

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Diagram Description automatically generated

NEW QUESTION 9

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

NEW QUESTION 10

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 10

A customer wants to harden its environment from misconfiguration.
Prisma Cloud Compute Compliance enforcement for hosts covers which three options? (Choose three.)

- A. Docker daemon configuration files
- B. Docker daemon configuration
- C. Host cloud provider tags
- D. Host configuration
- E. Hosts without Defender agents

Answer: BCD

NEW QUESTION 11

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

NEW QUESTION 14

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: BCD

NEW QUESTION 18

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 21

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 23

What is the order of steps in a Jenkins pipeline scan?
(Drag the steps into the correct order of occurrence, from the first step to the last.)

Answer Area

Unordered Options	Ordered Options
Scan Image	
Publish Scan Details	
Build Image	
Commit to Registry	

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Table Description automatically generated with medium confidence

NEW QUESTION 26

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: BE

NEW QUESTION 28

Review this admission control policy:
match[{"msg": msg}] { input.request.operation == "CREATE" input.request.kind.kind == "Pod" input.request.resource.resource == "pods"
input.request.object.spec.containers[_].securityContext.privileged msg := "Privileged"
}
Which response to this policy will be achieved when the effect is set to “block”?

- A. The policy will block all pods on a Privileged host.
- B. The policy will replace Defender with a privileged Defender.
- C. The policy will alert only the administrator when a privileged pod is created.
- D. The policy will block the creation of a privileged pod.

Answer: C

NEW QUESTION 30

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 33

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 38

You are tasked with configuring a Prisma Cloud build policy for Terraform. What type of query is necessary to complete this policy?

- A. YAML
- B. JSON
- C. CloudFormation
- D. Terraform

Answer: B

NEW QUESTION 42

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 45

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

NEW QUESTION 46

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 50

The Prisma Cloud administrator has configured a new policy. Which steps should be used to assign this policy to a compliance standard?

- A. Edit the policy, go to step 3 (Compliance Standards), click + at the bottom, select the compliance standard, fill in the other boxes, and then click Confirm.
- B. Create the Compliance Standard from Compliance tab, and then select Add to Policy.
- C. Open the Compliance Standards section of the policy, and then save.
- D. Custom policies cannot be added to existing standards.

Answer: B

NEW QUESTION 55

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 58

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 option shows the steps required during the alert rule creation process to achieve this objective?

- A. Ensure the public cloud account is assigned to an account group Assign the confirmed account group to alert ruleSelect "select all policies" checkbox as part of the alert rule Confirm the alert rule
- B. Ensure the public cloud account is assigned to an account group Assign the confirmed account group to alert ruleSelect one or more policies checkbox as part of the alert rule Confirm the alert rule
- C. Ensure the public cloud account is assigned to an account group Assign the confirmed account group to alert ruleSelect one or more policies as part of the alert rule Add alert notifications Confirm the alert rule
- D. Ensure the public cloud account is assigned to an account group Assign the confirmed account group to alert ruleSelect "select all policies" checkbox as part of the alert rule Add alert notifications Confirm the alert rule

Answer: C

NEW QUESTION 61

.....

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](#)