

Paloalto-Networks

Exam Questions PCCSE

Prisma Certified Cloud Security Engineer



NEW QUESTION 1

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 2

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 3

The security team wants to target a CNAF policy for specific running Containers. How should the administrator scope the policy to target the Containers?

- A. scope the policy to Image names.
- B. scope the policy to namespaces.
- C. scope the policy to Defender names.
- D. scope the policy to Host names.

Answer: B

NEW QUESTION 4

The InfoSec team wants to be notified via email each time a Security Group is misconfigured. Which Prisma Cloud tab should you choose to complete this request?

- A. Notifications
- B. Policies
- C. Alert Rules
- D. Events

Answer: B

NEW QUESTION 5

You have onboarded a public cloud account into Prisma Cloud Enterprise. Configuration Resource ingestion is visible in the Asset Inventory for the onboarded account, but no alerts are being generated for the configuration assets in the account.

Config policies are enabled in the Prisma Cloud Enterprise tenant, with those policies associated to existing alert rules. ROL statements on the investigate matching those policies return config resource results successfully.

Why are no alerts being generated?

- A. The public cloud account is not associated with an alert notification.
- B. The public cloud account does not have audit trail ingestion enabled.
- C. The public cloud account does not access to configuration resources.
- D. The public cloud account is not associated with an alert rule.

Answer: A

NEW QUESTION 6

A customer has a requirement to scan serverless functions for vulnerabilities. Which three settings are required to configure serverless scanning? (Choose three.)

- A. Defender Name
- B. Region
- C. Credential
- D. Console Address
- E. Provider

Answer: BCE

NEW QUESTION 7

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 8

Which method should be used to authenticate to Prisma Cloud Enterprise programmatically?

- A. single sign-on
- B. SAML
- C. basic authentication
- D. access key

Answer: D

NEW QUESTION 9

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 10

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

Which statement is true regarding CloudFormation templates?

- A. Scan support does not currently exist for nested references, macros, or intrinsic functions.
- B. A single template or a zip archive of template files cannot be scanned with a single API request.
- C. Request-Header-Field 'cloudformation-version' is required to request a scan.
- D. Scan support is provided for JSON, HTML and YAML formats.

Answer: A

NEW QUESTION 12

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 14

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 18

Which container scan is constructed correctly?

- A. twistcli images scan -u api -p api --address https://us-west1.cloud.twistlock.com/us-3-123456789 -- container myimage/latest
- B. twistcli images scan --docker-address https://us-west1.cloud.twistlock.com/us-3-123456789 myimage/ latest
- C. twistcli images scan -u api -p api --address https://us-west1.cloud.twistlock.com/us-3-123456789--details myimage/latest
- D. twistcli images scan -u api -p api --docker-address https://us-west1.cloud.twistlock.com/us-3-123456789 myimage/latest

Answer: B

NEW QUESTION 21

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?

- A. Target section within an Alert Rule.
- B. Notification Template section within Alerts.
- C. Users section within Settings.
- D. Set Alert Notification section within an Alert Rule.

Answer: A

NEW QUESTION 24

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 29

Which statement accurately characterizes SSO Integration on Prisma Cloud?

- A. Prisma Cloud supports IdP initiated SSO, and its SAML endpoint supports the POST and GET methods.

- B. Okta, Azure Active Directory, PingID, and others are supported via SAML.
- C. An administrator can configure different Identity Providers (IdP) for all the cloud accounts that Prisma Cloud monitors.
- D. An administrator who needs to access the Prisma Cloud API can use SSO after configuration.

Answer: A

NEW QUESTION 31

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 33

What are two ways to scan container images in Jenkins pipelines? (Choose two.)

- A. twistcli
- B. Jenkins Docker plugin
- C. Compute Jenkins plugin
- D. Compute Azure DevOps plugin
- E. Prisma Cloud Visual Studio Code plugin with Jenkins integration

Answer: BE

NEW QUESTION 37

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: B

NEW QUESTION 40

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 44

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: B

NEW QUESTION 48

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 49

The development team wants to fail CI jobs where a specific CVE is contained within the image. How should the development team configure the pipeline or policy to produce this outcome?

- A. Set the specific CVE exception as an option in Jenkins or twistcli.
- B. Set the specific CVE exception as an option in Defender running the scan.
- C. Set the specific CVE exception as an option using the magic string in the Console.
- D. Set the specific CVE exception in Console's CI policy.

Answer: C

NEW QUESTION 50

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 54

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 58

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

NEW QUESTION 62

A customer wants to turn on Auto Remediation.
Which policy type has the built-in CLI command for remediation?

- A. Anomaly
- B. Audit Event
- C. Network
- D. Config

Answer: D

NEW QUESTION 64

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

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

Answer: A

NEW QUESTION 65

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 66

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

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

Answer: D

NEW QUESTION 69

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 70

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 75

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 80

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 84

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 87

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 89

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: C

NEW QUESTION 93

A security team notices a number of anomalies under Monitor > Events. The incident response team works with the developers to determine that these anomalies are false positives.

What will be the effect if the security team chooses to Relearn on this image?

- A. The model is deleted, and Defender will relearn for 24 hours.
- B. The anomalies detected will automatically be added to the model.
- C. The model is deleted and returns to the initial learning state.
- D. The model is retained, and any new behavior observed during the new learning period will be added to the existing model.

Answer: B

NEW QUESTION 98

.....

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](#)