



Paloalto-Networks

Exam Questions PCCSE

Prisma Certified Cloud Security Engineer

About ExamBible

[Your Partner of IT Exam](#)

Found in 1998

ExamBible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, ExamBible has its unique advantages that other companies could not achieve.

Our Advances

* 99.9% Uptime

All examinations will be up to date.

* 24/7 Quality Support

We will provide service round the clock.

* 100% Pass Rate

Our guarantee that you will pass the exam.

* Unique Gurantee

If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

NEW QUESTION 1

Which step is included when configuring Kubernetes to use Prisma Cloud Compute as an admission controller?

- A. copy the Console address and set the config map for the default namespace.
- B. create a new namespace in Kubernetes called admission-controller.
- C. enable Kubernetes auditing from the Defend > Access > Kubernetes page in the Console.
- D. copy the admission controller configuration from the Console and apply it to Kubernetes.

Answer: B

NEW QUESTION 2

A customer has a large environment that needs to upgrade Console without upgrading all Defenders at one time. What are two prerequisites prior to performing a rolling upgrade of Defenders? (Choose two.)

- A. manual installation of the latest twistcli tool prior to the rolling upgrade
- B. all Defenders set in read-only mode before execution of the rolling upgrade
- C. a second location where you can install the Console
- D. additional workload licenses are required to perform the rolling upgrade
- E. an existing Console at version n-1

Answer: BE

NEW QUESTION 3

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?

- A. 443
- B. 80
- C. 8080
- D. 8888

Answer: C

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

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 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 9

A customer finds that an open alert from the previous day has been resolved. No auto-remediation was configured. Which two reasons explain this change in alert status? (Choose two.)

- A. user manually changed the alert status.
- B. policy was changed.
- C. resource was deleted.
- D. alert was sent to an external integration.

Answer: CD

NEW QUESTION 10

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 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 14

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 19

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 21

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 22

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 24

A customer has a requirement to automatically protect all Lambda functions with runtime protection. What is the process to automatically protect all the Lambda functions?

- A. Configure a function scan policy from the Defend/Vulnerabilities/Functions page.
- B. Configure serverless radar from the Defend/Compliance/Cloud Platforms page.
- C. Configure a manually embedded Lambda Defender.
- D. Configure a serverless auto-protect rule for the functions.

Answer: D

NEW QUESTION 26

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 30

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 34

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 38

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 40

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 45

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 48

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 51

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 52

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: A

NEW QUESTION 56

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 58

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

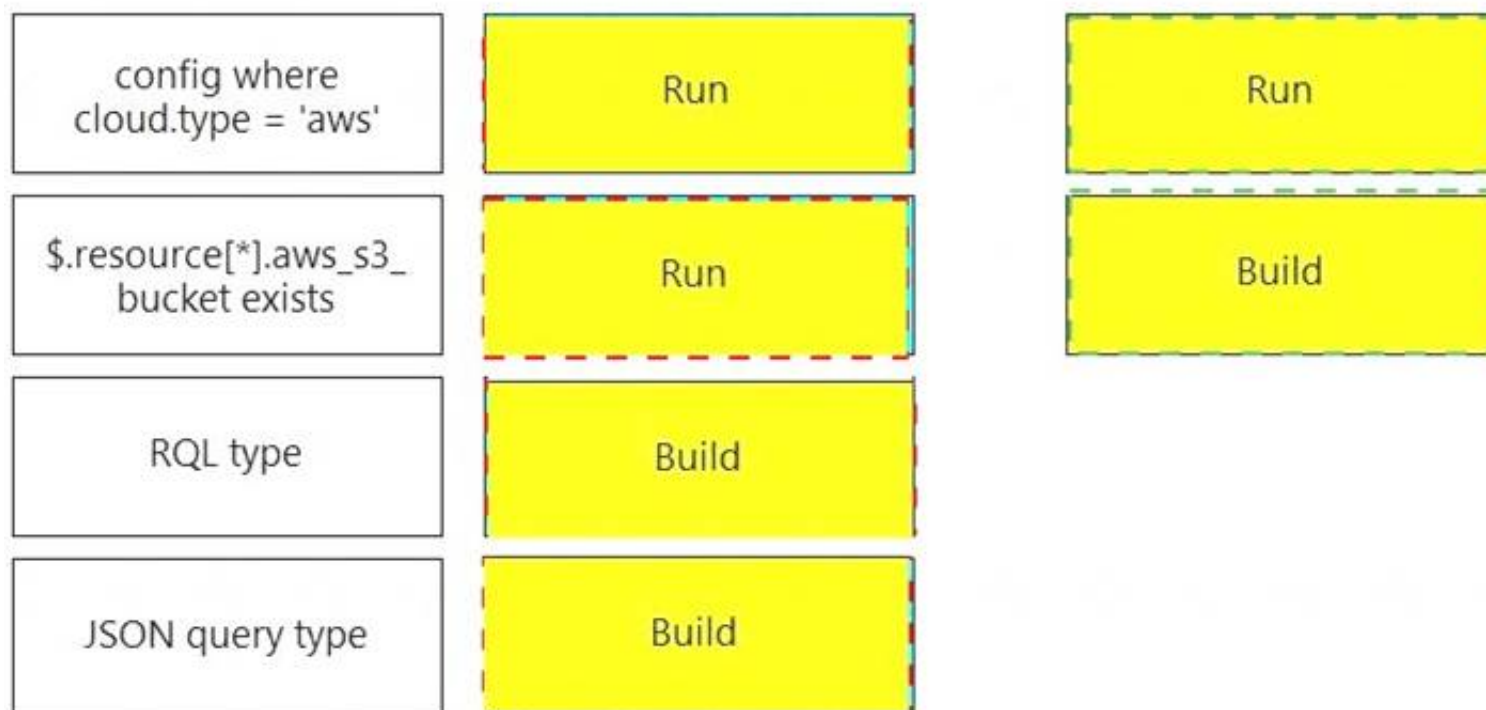
config where cloud.type = 'aws'	Drag answer here	Run
\$.resource[*].aws_s3_bucket exists	Drag answer here	Build
RQL type	Drag answer here	
JSON query type	Drag answer here	

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area



NEW QUESTION 63

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 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 69

Which statement about build and run policies is true?

- A. Build policies enable you to check for security misconfigurations in the IaC templates.
- B. Every type of policy has auto-remediation enabled by default.
- C. The four main types of policies are: Audit Events, Build, Network, and Run.
- D. Run policies monitor network activities in the environment and check for potential issues during runtime.

Answer: A

NEW QUESTION 72

A customer is reviewing Container audits, and an audit has identified a cryptominer attack. Which three options could have generated this audit? (Choose three.)

- A. The value of the mined currency exceeds \$100.
- B. High CPU usage over time for the container is detected.
- C. Common cryptominer process name was found.
- D. The mined currency is associated with a user token.
- E. Common cryptominer port usage was found.

Answer: BCD

NEW QUESTION 73

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 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 78

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 83

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 87

.....

Relate Links

100% Pass Your PCCSE Exam with ExamBible Prep Materials

<https://www.exambible.com/PCCSE-exam/>

Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - <https://www.exambible.com/>