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
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 2
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 3
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 4
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 5
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 6
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 7
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 8
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 9
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 10
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 10
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 15
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 16
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?

A. Disable the policy
B. Set the Alert Disposition to Conservative
C. Change the Training Threshold to Low
D. Set Alert Disposition to Aggressive

Answer: C

NEW QUESTION 19
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 21
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 26
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 28
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 31
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 33
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 38
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?

A. an event within the cloud account

B. network traffic to the S3 bucket
C. configuration of the S3 bucket
D. anomalous behaviors

Answer: B

NEW QUESTION 40
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 43
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 46
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 48
.....

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/