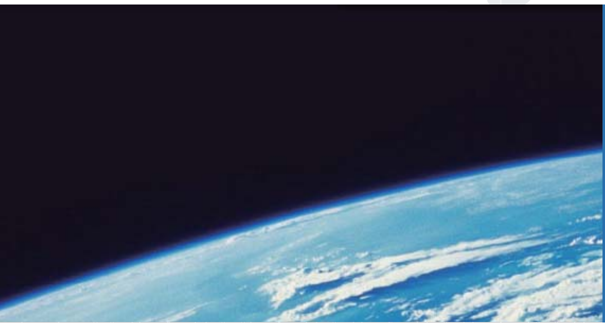
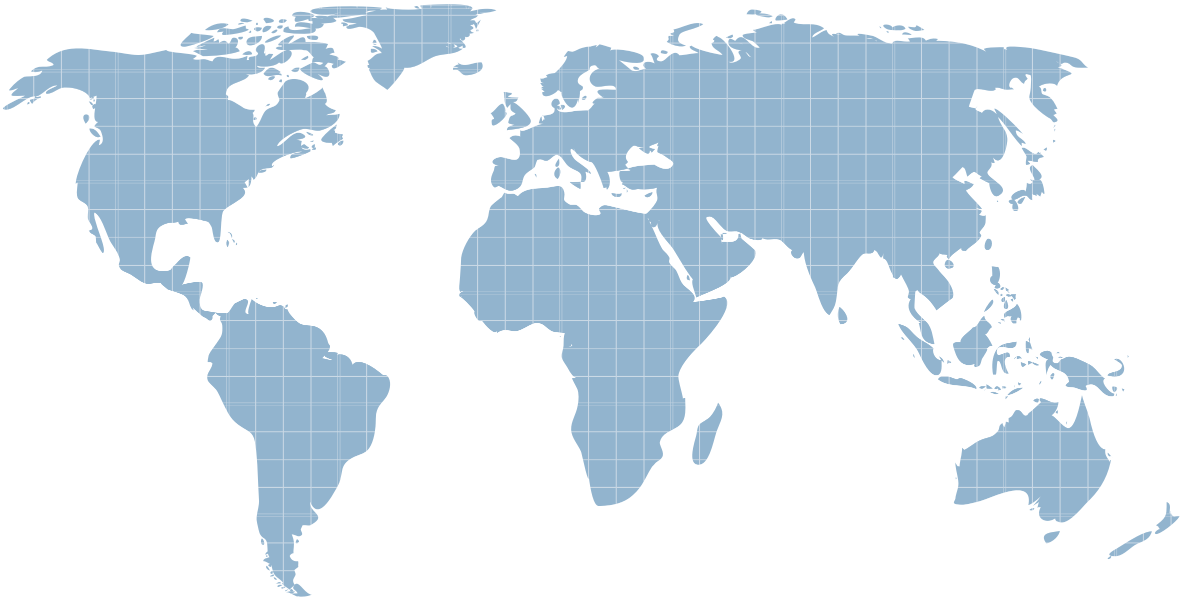


ITTEST

QUESTION & ANSWER

Guías de estudio precisos, Alta tasa de paso!



Ittest ofrece información actualizada de forma gratuita en un año!

http://www.ittest.es/

Exam: **PCCSE**

Title: Prisma Certified Cloud Security Engineer

Version: DEMO

1.Which three steps are involved in onboarding an account for Data Security? (Choose three.)
A. Create a read-only role with in-line policies
B. Create a Cloudtrail with SNS Topic
C. Enable Flow Logs
D. Enter the RoleARN and SNSARN
E. Create a S3 bucket
Answer: B,D,E

2.An administrator wants to enforce a rate limit for users not being able to post five (5) .tar.gz files within five (5) seconds.
What does the administrator need to configure?
A. A ban for DoS protection with an average rate of 5 and file extensions match on .tar.gz on WAAS
B. A ban for DoS protection with a burst rate of 5 and file extensions match on .tar.gz on
CNNF
C. A ban for DoS protection with a burst rate of 5 and file extensions match on .tar gz on
WAAS
D. A ban for DoS protection with an average rate of 5 and file extensions match on .tar.gz on CNNF
Answer: C

3.The security team wants to enable the “block” option under compliance checks on the host.
What effect will this option have if it violates the compliance check?
A. The host will be taken offline.
B. Additional hosts will be prevented form starting.
C. Containers on a host will be stopped.
D. No containers will be allowed to start on that host.
Answer: D
Explanation:
Reference:
https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin-compute/runtime_defense/runtime_defense_containers.html

4.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: D
Explanation:
Reference:
https://docs.twistlock.com/docs/enterprise_edition/compliance/manage_compliance.html

5.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: B,C,D

Explanation:

Reference:
https://docs.paloaltonetworks.com/prisma/prisma-cloud/19-11/prisma-cloud-compute-edition-admin/vulnerability_management/vuln_management_rules.html