

First-grade CloudSec-Pro Reliable Exam Topics Provide Prefect Assistance in CloudSec-Pro Preparation



P.S. Free & New CloudSec-Pro dumps are available on Google Drive shared by TestKingFree: <https://drive.google.com/open?id=1ac0vr11iyiT3dDMKEdd8JVmMBKB-49g>

These mock tests are specially built for you to assess what you have studied. These CloudSec-Pro Practice Tests are customizable, which means you can change the time and questions according to your needs. You can even access your previously given tests from the history, which helps you to overcome mistakes while giving the actual test next time.

Palo Alto Networks CloudSec-Pro Exam Syllabus Topics:

Topic	Details
Topic 1	<ul style="list-style-type: none"> Application Security: This domain covers security practices integrated throughout the software development lifecycle, including application security posture management, CI CD pipeline security, software composition analysis, IaC security, and secrets scanning. It also explores real-world application security use cases and scan management.

Topic 2	<ul style="list-style-type: none"> • Security Operations Center (SOC) Fundamentals: This domain covers the foundational components of a SOC, including team roles, tools, and technologies used in day-to-day security operations. It also addresses how AI • ML and threat intelligence support incident response, categorization, and prioritization.
Topic 3	<ul style="list-style-type: none"> • Cortex Fundamentals: This domain focuses on the core features of the Cortex Cloud platform, including indicator types, log management, asset inventory, compliance, and data protection. It also covers how to create reports and dashboards and how data sources are ingested into the platform.
Topic 4	<ul style="list-style-type: none"> • Cloud Runtime Security: This domain addresses the protection of cloud workloads during active operation, covering cloud workload protection, detection and response, web application and API security, and vulnerability management. It also includes the processes involved in deploying and managing security agents.
Topic 5	<ul style="list-style-type: none"> • Cloud Posture Security: This domain examines the tools and practices used to assess and manage cloud security posture, spanning CSPM, KSPM, AI-SPM, and DSPM. It also covers agentless scanning, identity security, vulnerability management, unified compliance, and the role of Posture Security Management Modules.

>> **CloudSec-Pro Reliable Exam Topics** <<

100% Pass High Hit-Rate Palo Alto Networks - CloudSec-Pro - Palo Alto Networks Cloud Security Professional Reliable Exam Topics

In order to ensure the quality of our CloudSec-Pro actual exam, we have made a lot of efforts. Our company spent a great deal of money on hiring hundreds of experts and they formed a team to write the work. The qualifications of these experts are very high. They have rich knowledge and rich experience on the CloudSec-Pro Study Guide. So they know every detail about the CloudSec-Pro exam questions and can make it better. With our CloudSec-Pro learning guide, you will be bound to pass the exam.

Palo Alto Networks Cloud Security Professional Sample Questions (Q192-Q197):

NEW QUESTION # 192

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

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

Answer: A,C,E

Explanation:

https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin-compute/continuous_integration/set_policy_ci_plugins

NEW QUESTION # 193

Web-Application and API Security (WAAS) provides protection for which two protocols? (Choose two.)

- A. HTTP
- B. Tomcat Web Connector via AJP
- C. TLS
- D. SSH

Answer: A,C

Explanation:

Web-Application and API Security (WAAS) is a feature within Prisma Cloud that focuses on protecting web applications and APIs from various threats and vulnerabilities. The primary protocols it provides protection for are HTTP (Hypertext Transfer Protocol) and TLS (Transport Layer Security). HTTP is the foundation of data communication for the World Wide Web, and TLS is a cryptographic protocol designed to provide communications security over a computer network. While SSH (Secure Shell) is a protocol for secure remote login and other secure network services, and Tomcat Web Connector via AJP (Apache JServ Protocol) is used for Tomcat server communication, they are not the primary focus of WAAS protection.

NEW QUESTION # 194

Which RQL will trigger the following audit event activity?

- A. event from cloud.audit_logs where operation IN ('GetBucketWebsite', 'PutBucketWebsite', 'DeleteBucketWebsite')
- B. event from cloud.audit_logs where operation IN('cloudsql.instances.update','cloudsql.sslCerts.create', 'cloudsql.instances.create','cloudsq
- **C. event from cloud.audit_logs where operation ConsoleLogin AND user = 'root'**
- D. event from cloud.audit_logs where cloud.service = s3.amazonaws.com' AND json.rule = \$.userAgent contains 'parrot1

Answer: C

Explanation:

The correct RQL to trigger the audit event activity shown is Option A. This RQL is designed to capture events from cloud audit logs where a ConsoleLogin operation occurs by the 'root' user. The given audit event details match this RQL's criteria, which specifies the operation type and the user involved in the event.

NEW QUESTION # 195

Which Prisma Cloud policy type detects port scanning activities in a customer environment?

- A. Port Scan
- **B. Anomaly**
- C. Config
- D. Network

Answer: B

Explanation:

In the context of Prisma Cloud, the policy type that is specifically designed to detect unusual activities, such as port scanning, within a customer's environment is classified under "Anomaly." Anomaly-based policies leverage advanced analytics and machine learning algorithms to identify patterns and behaviors that deviate from the norm, which could indicate potential security threats like port scanning attempts. By detecting such anomalies, these policies help organizations proactively identify and respond to potential reconnaissance activities by attackers seeking to discover open ports and vulnerable services.

NEW QUESTION # 196

Which API calls can scan an image named myimage: latest with twistcli and then retrieve the results from Console?

- **A. \$ twistcli images scan --address --user --password --details \myimage: latest**
- B. \$ twistcli images scan --address --user --password --console \myimage: latest
- C. \$ twistcli images scan --address --user --password \myimage: latest
- D. \$ twistcli images scan --address --user --password --verbose \myimage: latest

Answer: A

Explanation:

You can have twistcli generate a detailed report for each scan. The following procedure shows you how to scan an image with twistcli, and then retrieve the results from Console.

https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin-compute/tools/twistcli_scan_images

