

PCCSE^{Q&As}

Prisma Certified Cloud Security Engineer

Pass Palo Alto Networks PCCSE Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

<https://www.pass2lead.com/pccse.html>

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Palo Alto Networks Official Exam Center

- ⚙️ **Instant Download** After Purchase
- ⚙️ **100% Money Back** Guarantee
- ⚙️ **365 Days** Free Update
- ⚙️ **800,000+** Satisfied Customers



QUESTION 1

What is the most reliable and extensive source for documentation on Prisma Cloud APIs?

- A. prisma.pan.dev
- B. docs.paloaltonetworks.com
- C. Prisma Cloud Administrator's Guide
- D. Live Community

Correct Answer: A

<https://prisma.pan.dev/api/cloud/>

QUESTION 2

An administrator sees that a runtime audit has been generated for a container.

The audit message is:

`"/bin/ls launched and is explicitly blocked in the runtime rule. Full command: ls -latr"`

Which protection in the runtime rule would cause this audit?

- A. Networking
- B. File systems
- C. Processes
- D. Container

Correct Answer: C

QUESTION 3

Where are Top Critical CVEs for deployed images found? Vulnerabilities Code Repositories

- A. Defend

Correct Answer: C

https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin-compute/vulnerability_management/vuln_explorer

QUESTION 4

Based on the following information, which RQL query will satisfy the requirement to identify VM hosts deployed to organization public cloud environments exposed to network traffic from the internet and affected by Text4Shell RCE (CVE2022-42889) vulnerability?

Network flow logs from all virtual private cloud (VPC) subnets are ingested to the Prisma Cloud Enterprise Edition tenant. All virtual machines (VMs) have Prisma Cloud Defender deployed.

- A. network from vpc.flow_record where bytes > 0 AND dest.resource IN (resource where finding.type IN (\\Host Vulnerability\\) AND finding.source IN (\\Prisma Cloud\\) AND finding.name IN (\\CVE-2022-42889\\)) AND source.publicnetwork IN (\\Internet IPs\\, \\Suspicious IPs\\)
- B. config from vpc.flow_record where bytes > 0 AND dest.resource IN (resource where finding.type IN (\\Host Vulnerability\\) AND finding.source IN (\\Prisma Cloud\\) AND finding.name IN (\\CVE-2022-42889\\)) AND source.publicnetwork = (\\Internet IPs\\ or \\Suspicious IPs\\)
- C. network from vpc.flow_record where bytes > 0 AND finding.type IN (\\Host Vulnerability\\) AND finding.source IN (\\Prisma Cloud\\) AND finding.name IN (\\CVE-2022-42889\\) AND source.publicnetwork = \\Internet IPs\\
- D. config from cloud.resource where cloud.type = \\aws\\ AND api.name = \\aws-ec2-describe-instances\\ AND json.rule = publicIpAddress exists AND finding.type IN (\\Host Vulnerability\\) AND finding.source IN (\\Prisma Cloud\\) AND finding.name IN (\\CVE-2022-42889\\)

Correct Answer: A

QUESTION 5

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

Correct Answer: AB

Reference: <https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin/prisma-cloud-policies/manage-prisma-cloud-policies>