

Palo Alto Networks CloudSec-Engineer

Palo Alto Networks Cloud Security Engineer



For More Information – Visit link below:

<https://www.examsboost.com/>

Product Version

- ✓ Up to Date products, reliable and verified.
- ✓ Questions and Answers in PDF Format.

Latest Version: 6.0

Question: 1

Dependency, secrets, infrastructure-as-code and image scanning are all enabled across a large estate, and the combined backlog has reached tens of thousands of open findings. The same underlying issue frequently appears three or four times from different scanners, and application teams say they cannot tell which of the findings are theirs to fix.

Which approach BEST addresses this?

- A. Publish a combined report from each scanner on a fixed schedule and ask every application team to search it for the repositories they own ahead of each release, escalating anything they cannot place
- B. Raise the severity threshold on each scanner until the number of open findings is small enough for a team to work through within a release cycle
- C. Correlate every scanner's output with application and ownership context — repository, service, owning team and deployed asset — so duplicates collapse and each finding is routed to its owner
- D. Consolidate on a single scanner for each artifact class so that no issue is reported twice and the total volume falls to what one tool produces

Answer: C

Question: 2

Secrets scanning flags a long-lived cloud credential committed to a repository that several teams contribute to. The commit is three weeks old, the repository is mirrored to a build cache and images built from it are already running in production.

What should the security engineering team do FIRST?

- A. Rewrite the repository history to purge the commit and force-push the cleaned branches to every mirror
- B. Add a pre-commit hook and a pipeline gate that stop a credential reaching the repository
- C. Rebuild and redeploy every image that was produced from the repository after the commit landed
- D. Revoke the credential and issue a replacement

Answer: D

Question: 3

A team is building a nightly job that pulls findings out of the platform into the organization's data warehouse. The job runs unattended from the scheduling system.

Which two practices apply to the credential that job presents?

(Choose two.)

- A. Reuse the credential presented by the identity integration, covering human and machine access with one identity.
- B. Attribute it to the named export service rather than to an engineer, and rotate it on a defined schedule.
- C. Embed it in the scheduling system's job definition, leaving the job with no external dependency at run time.
- D. Grant the credential an administrative scope for the first few runs and narrow it afterwards, once the job's own logs have shown which calls it actually makes.
- E. Scope it to the read operations the export performs and nothing wider.

Answer: B,E

Question: 4

The security engineering team at a multi-account organization has finished its agent rollout and now has to plan how runtime enforcement is turned on. Application teams own their own accounts and have asked not to be surprised by blocks.

Which enablement sequence should the team adopt?

- A. Turn prevention on everywhere at once and add exclusions as teams report false blocks.
- B. Stay in alert mode across the whole estate indefinitely and let the response team act on what it sees, since prevention in a shared estate risks blocking legitimate work.
- C. Enable prevention in production for the highest-severity rules immediately, then extend alerting to the remaining environments once the critical workloads are covered.
- D. Alert in every environment first, then switch non-production to prevent, then prevent in production for the rules that have proved high-confidence.

Answer: D

Question: 5

Data science teams at a retail organization have been creating managed AI services, notebooks and training datasets in their own accounts without involving security. Leadership asks the security engineering team to establish what AI is running across the estate and how exposed it is.

Which capability is scoped to that question?

- A. KSPM, which evaluates the clusters the training jobs are scheduled on and reports their configuration into the same queue.
- B. CIEM, which flags the over-permissioned service identities the new AI workloads were created with.
- C. AI-SPM, which brings models, notebooks and training data into inventory and then reports shadow services, publicly reachable models and over-permissioned AI identities.

D. DSPM, which discovers and classifies the data held in those accounts and therefore already covers the models, the notebooks and the service identities and applications that consume them.

Answer: C

Question: 6

In a financial services organization with several hundred cloud accounts, the number of workloads carrying a runtime agent has risen in each of the last three months. Over the same three months, the share of discovered workloads that carry one has fallen.

The monthly report to the security committee cites the rising agent count as evidence that the rollout is on track.

What should the engineer tell the committee?

- A. The estate is growing faster than the rollout, and the widening gap is itself the finding to report
- B. The agent count is the wrong measure of progress, so the report should track the runtime detections each account raises instead
- C. The rollout is proceeding as designed, and the falling share reflects resources that a runtime agent does not protect
- D. Discovery is over-reporting, so the inventory should be narrowed to the accounts in scope

Answer: A

Question: 7

An organization's pipeline has failed the build on any finding of any severity since the gate was introduced. A review finds a documented skip step now present in most services' pipeline configuration, and the scan running on only a small minority of builds.

Leadership has proposed tightening the severity policy further.

Which two considerations should MOST influence the response?

(Choose two.)

- A. The skip step shows the delivery teams are not treating the severities seriously, which is an argument for a stricter policy.
- B. Recording every skipped build as an accepted risk keeps the policy intact while the teams work down the backlog.
- C. The control is protecting nothing as it stands, because a gate that is skipped on most builds stops no artifact from reaching release.
- D. The proportion of builds on which the gate was overridden is the measurement that shows its threshold needs re-tuning.
- E. Moving the check to the developers' editors restores build speed without giving up coverage of the same findings.

Answer: C,D

Question: 8

On a Monday morning no member of the security team can sign in to the console; the browser is handed to the identity provider and the attempt then fails. The scheduled export jobs that call the platform's API ran overnight and completed, and the runtime agents across the estate are still reporting. The identity team carried out planned maintenance over the weekend.

Which two conclusions does the scope of the failure support?
(Choose two.)

- A. The tenant has been suspended or its subscription has lapsed, so every authenticated path into the platform is being refused.
- B. The agents' own certificates have to be re-issued alongside the human sign-in path, because both trust the certificate the identity team replaced.
- C. Network reachability to the console has been lost, which is why no session can be established.
- D. The failure is confined to the federated sign-in path, since the programmatic and agent paths authenticate by a different mechanism and are unaffected.
- E. The identity provider's signing certificate is the first thing to examine, as a replaced signing key breaks assertion validation while leaving every other path working.

Answer: D,E

Question: 9

Console sign-in at a software organization is already federated to the corporate identity provider, but roles are still granted by assigning them to each federated user by hand. Engineers who move between teams keep the access their previous team needed, and two leavers were found still holding roles a month after their last day.

Which change BEST addresses this?

- A. Introduce a quarterly access review in which each team lead re-certifies the individual role assignments held by everyone reporting to them, with unclaimed assignments removed.
- B. Drive role assignment from identity-provider group membership so that a move or a departure changes console access at the provider.
- C. Shorten the console session lifetime so that a user whose provider account has been disabled loses console access when their current session expires.
- D. Require the joiner, mover and leaver process to raise a console role change ticket for each move or departure.

Answer: B

Question: 10

During a design review, a security engineering team plans an integration with the organization's SOAR platform so that certain findings trigger an automated containment workflow. A reviewer asks how this integration changes what the platform knows about the estate.

Which statement correctly describes the SOAR integration's role?

- A. It consumes the findings the platform produces and acts on them in an external workflow, not supplying data the platform analyzes.
- B. It supplies additional asset and identity context to the platform, which joins that context onto existing findings when it correlates them into risks.
- C. It acts as the identity source for platform access, mapping automation users onto platform roles.
- D. It takes over routing decisions from the alert rules, so which findings are raised is decided outside the platform.

Answer: A

Thank You for Trying Our Product

For More Information – **Visit link below:**

<https://www.examsboost.com/>

15 USD Discount Coupon Code:

G74JA8UF

FEATURES

- ✓ **90 Days Free Updates**
- ✓ **Money Back Pass Guarantee**
- ✓ **Instant Download or Email Attachment**
- ✓ **24/7 Live Chat Support**
- ✓ **PDF file could be used at any Platform**
- ✓ **50,000 Happy Customer**



Visit us at: <https://www.examsboost.com/test/cloudsec-engineer>