

 Google Discussions

## Exam Professional Cloud Security Engineer All Questions

View all questions & answers for the Professional Cloud Security Engineer exam

[Go to Exam](#)

### EXAM PROFESSIONAL CLOUD SECURITY ENGINEER TOPIC 1 QUESTION 188 DISCUSSION

Actual exam question from Google's Professional Cloud Security Engineer

Question #: 188

Topic #: 1

[\[All Professional Cloud Security Engineer Questions\]](#)

A company is using Google Kubernetes Engine (GKE) with container images of a mission-critical application. The company wants to scan the images for known security issues and securely share the report with the security team without exposing them outside Google Cloud.

What should you do?




- A. 1. Enable Container Threat Detection in the Security Command Center Premium tier.  
2. Upgrade all clusters that are not on a supported version of GKE to the latest possible GKE version.  
3. View and share the results from the Security Command Center.
- B. 1. Use an open source tool in Cloud Build to scan the images.  
2. Upload reports to publicly accessible buckets in Cloud Storage by using gsutil.  
3. Share the scan report link with your security department.
- C. 1. Enable vulnerability scanning in the Artifact Registry settings.  
2. Use Cloud Build to build the images.  
3. Push the images to the Artifact Registry for automatic scanning.  
4. View the reports in the Artifact Registry.
- D. 1. Get a GitHub subscription.  
2. Build the images in Cloud Build and store them in GitHub for automatic scanning.  
3. Download the report from GitHub and share with the Security Team.

[Show Suggested Answer](#)

## Comments

Type your comment...

Submit



  **espressoboy** Highly Voted  1 year, 4 months ago

C Seems like the best fit. I initially chose A but:

"The service evaluates all changes and remote access attempts to detect runtime attacks in near-real time." : <https://cloud.google.com/security-command-center/docs/concepts-container-threat-detection-overview>

This has nothing to do with KNOWN security Vulns in images

   upvoted 6 times



  **Pime13** Most Recent  7 months, 2 weeks ago

**Selected Answer: C**

Option A involves enabling Container Threat Detection in the Security Command Center Premium tier, upgrading clusters, and viewing and sharing results from the Security Command Center. While this option provides robust threat detection and security insights, it is more focused on detecting threats and anomalies rather than specifically scanning container images for known vulnerabilities.

Option C is more directly aligned with the requirement to scan container images for known security issues and securely share the report within Google Cloud. It leverages the Artifact Registry's built-in vulnerability scanning feature, which is specifically designed for this purpose.

   upvoted 1 times

  **dija123** 10 months ago

**Selected Answer: C**

100% C

   upvoted 1 times

  **Andrei\_Z** 1 year, 4 months ago

**Selected Answer: C**

it is C

   upvoted 1 times

  **ArizonaClassics** 1 year, 5 months ago

C. Enable vulnerability scanning in Artifact Registry, use Cloud Build, push images for scanning, view reports: This option fulfills all the requirements. It scans images for vulnerabilities using Google Cloud's Artifact Registry and allows viewing of reports securely within the Google Cloud environment. Cloud Build can also be used to build the images before they are pushed for scanning, which adds an extra layer of validation.

   upvoted 2 times

  **cyberpunk21** 1 year, 5 months ago

**Selected Answer: C**

i am going with option C all things considered like cost, time and all. option A sounds sound but to implement we need to update the tier and the security issues are already known so not worth it with option C we can do vuln scan without paying extra

   upvoted 2 times

  **ymkk** 1 year, 5 months ago

**Selected Answer: A**

<https://cloud.google.com/security-command-center/docs/concepts-container-threat-detection-overview>

   upvoted 2 times

  **Nachtwaker** 10 months, 3 weeks ago

Don't agree, should be C since it is requesting scans from images (so not running container images). The images are static, stored in container registry, not (yet) deployed in GKE.

   upvoted 1 times

  **a190d62** 1 year, 5 months ago

**Selected Answer: C**

Selected Answer: C

C:

B & D are out due to fact that exposes the results of the scan

A & C remains - but to be honest I don't see how updating GKE to the latest version (A) would provide me better vulnerability scan result

👍 ↩ 🚩 upvoted 2 times

🗄️ 👤 **akilaz** 1 year, 5 months ago

"To detect potential threats to your containers, make sure that your clusters are on a supported version of Google Kubernetes Engine (GKE)"

<https://cloud.google.com/security-command-center/docs/how-to-use-container-threat-detection>

Additionally Answer C doesn't include sharing the report. So in my opinion A

👍 ↩ 🚩 upvoted 3 times

🗄️ 👤 **a190d62** 1 year, 5 months ago

and (never forget about it people) link:

<https://cloud.google.com/artifact-registry/docs/analysis>

👍 ↩ 🚩 upvoted 1 times



## Platform

> Home

> All Exams

> Examtopics PRO

> Training Courses



© 2024 ExamTopics