GOOGLE SECOPS PROFESSIONAL ENGINEER PRACTICE TEST (SAMPLE)

STUDY GUIDE

SAMPLE STUDY GUIDE WITH LIMITED QUESTIONS

VISIT US ONLINE FOR THE FULL VERSION STUDY GUIDE

https://googlesecopsproengr.examzify.com

Table of Contents

Copyright 1

Table of Contents 2

Introduction 3

How to Use This Guide 4

Questions 5

Answers 9

Explanations 11

Next Steps 17

Introduction

Preparing for a certification exam can feel overwhelming, but with the right tools, it becomes an opportunity to build confidence, sharpen your skills, and move one step closer to your goals. At Examzify, we believe that effective exam preparation isn't just about memorization, it's about understanding the material, identifying knowledge gaps, and building the test-taking strategies that lead to success.

This guide was designed to help you do exactly that.

Whether you're preparing for a licensing exam, professional certification, or entry-level qualification, this book offers structured practice to reinforce key concepts. You'll find a wide range of multiple-choice questions, each followed by clear explanations to help you understand not just the right answer, but why it's correct.

The content in this guide is based on real-world exam objectives and aligned with the types of questions and topics commonly found on official tests. It's ideal for learners who want to:

- Practice answering questions under realistic conditions,
- Improve accuracy and speed,
- Review explanations to strengthen weak areas, and
- Approach the exam with greater confidence.

We recommend using this book not as a stand-alone study tool, but alongside other resources like flashcards, textbooks, or hands-on training. For best results, we recommend working through each question, reflecting on the explanation provided, and revisiting the topics that challenge you most.

Remember: successful test preparation isn't about getting every question right the first time, it's about learning from your mistakes and improving over time. Stay focused, trust the process, and know that every page you turn brings you closer to success.

Let's begin.

How to Use This Guide

This guide is designed to help you study more effectively and approach your exam with confidence. Whether you're reviewing for the first time or doing a final refresh, here's how to get the most out of your Examzify study guide:

1. Start with a Diagnostic Review

Skim through the questions to get a sense of what you know and what you need to focus on. Your goal is to identify knowledge gaps early.

2. Study in Short, Focused Sessions

Break your study time into manageable blocks (e.g. 30 – 45 minutes). Review a handful of questions, reflect on the explanations.

3. Learn from the Explanations

After answering a question, always read the explanation, even if you got it right. It reinforces key points, corrects misunderstandings, and teaches subtle distinctions between similar answers.

4. Track Your Progress

Use bookmarks or notes (if reading digitally) to mark difficult questions. Revisit these regularly and track improvements over time.

5. Simulate the Real Exam

Once you're comfortable, try taking a full set of questions without pausing. Set a timer and simulate test-day conditions to build confidence and time management skills.

6. Repeat and Review

Don't just study once, repetition builds retention. Re-attempt questions after a few days and revisit explanations to reinforce learning. Pair this guide with other Examzify tools like flashcards, and digital practice tests to strengthen your preparation across formats.

There's no single right way to study, but consistent, thoughtful effort always wins. Use this guide flexibly, adapt the tips above to fit your pace and learning style. You've got this!

Questions

1. **A SecOps report export to a BigQuery dataset runs successfully but the dataset remains empty. Which action should you take to fix the export with correct permissions?**

   A. Grant the SecOps service account dataEditor on the dataset.

   B. Grant the user who scheduled the report roles/bigquery.dataEditor on the project.

   C. Grant the SecOps service account roles/iam.serviceAccountUser to itself.

   D. Set a retention period for the BigQuery export.

2. **Which configuration would you implement if your goal is to pull data and tag using an ingestion label per log source?**

   A. Configure feed management to pull data and configure an ingestion label per log source.

   B. Configure feed management to pull data from each location and configure a namespace per log source.

   C. Configure a Bindplane agent collecting Syslog from each location and configure a namespace per log source.

   D. Configure a Bindplane agent and an ingestion label per log source.

3. **When evaluating a new endpoint detection tool for SecOps integration, which step is most directly tied to interoperability with existing workflows?**

   A. Identify the tool in the SecOps Marketplace and verify support for necessary actions.

   B. Develop a custom integration with Python and Cloud Run to forward logs/orchestrate actions.

   C. Review documentation to identify if default parsers exist; determine whether logs are supported/ingestable.

   D. Identify hosting cloud provider.

4. **Which option would you implement to use a Bindplane agent collecting Syslog from each location and assign a namespace per log source to avoid IP aliasing?**

   A. Configure a Bindplane agent collecting Syslog from each location and configure a namespace per log source.

   B. Configure feed management to pull data from each location and configure a namespace per log source.

   C. Configure feed management to pull data and configure an ingestion label per log source.

   D. Configure a Bindplane agent and an ingestion label per log source.

5. Group B requires access to all data except the 'restricted' namespace. Which data access scope design would satisfy this?

A. Create a new data access scope to include all data with a 'restricted' label.

B. Create a new data access scope to allow excluding a specific namespace.

C. Use a global data access scope with no exclusions.

D. Create a new data access scope to allow all data and exclude 'restricted' namespace for Group B; assign in IAM.

6. To generate an alert when a binary hash first appears, which approach should you implement?

A. Enable the Applied Threat Intelligence - Curated Prioritization rule set.

B. Use Alerts & IOCs page with a filter on hashes and first_seen_time.

C. Write a rule to examine file-related events that join with derived context for hashes in the entity graph; compare timestamp to first_seen_time.

D. Use statistics in search on the current day and verify first_seen_time predates the day.

7. You observe multiple distinct, low-severity suspicious activities on a single internal server; no single event is a high-confidence IOC. You want ongoing heightened scrutiny. What should you do?

A. Schedule a daily SecOps report detailing all activity on this server.

B. Develop a server-specific YARA-L detection rule.

C. Add the server to a SecOps watchlist, and monitor closely.

D. Create a case, isolate the server, and escalate for forensics.

8. How should you configure two on-prem firewalls to forward logs to Google SecOps via Syslog?

A. Pull firewall logs using a SecOps feed integration.

B. Set the Google SecOps URL instance as the Syslog destination.

C. Deploy a third-party agent (e.g., Bindplane, NXLog) and set it as the Syslog destination.

D. Deploy a Google Ops Agent and set it as the Syslog destination.

9. Which approach should you take to generate a list of unknown command and control (C2) nodes within 24 hours?

A. Write a rule in Google SecOps that scans historic network outbound connections against ingested threat intel and run the rule as a retrohunt against the full tenant

B. Load network records into BigQuery to identify endpoints that are communicating with domains outside three standard deviations of normal

C. Review Security Health Analytics (SHA) findings in Security Command Center (SCC)

D. Write a YARA-L rule in Google SecOps that compares network traffic of endpoints to low prevalence domains against recent WHOIS registrations

10. When Container Threat Detection alerts that an added binary has been executed in a business-critical workload, which two actions are most appropriate?

A. Notify the workload owner. Follow the response playbook, and involve threat hunting to identify the root cause

B. Review the finding, investigate the pod and related resources, and research the related attack and response methods

C. Quarantine the cluster containing the running pod and delete the running pod

D. Silence the alert in the SCC console, as the alert is low severity

Answers

1. A
2. D
3. A
4. C
5. D
6. C
7. C
8. C
9. A
10. A

Explanations

1. A SecOps report export to a BigQuery dataset runs successfully but the dataset remains empty. Which action should you take to fix the export with correct permissions?

A. Grant the SecOps service account dataEditor on the dataset.

B. Grant the user who scheduled the report roles/bigquery.dataEditor on the project.

C. Grant the SecOps service account roles/iam.serviceAccountUser to itself.

D. Set a retention period for the BigQuery export.

The key idea is that the identity performing the export must have write access to the target dataset. The SecOps export runs under a service account, and if that service account doesn't have permission to write data into the dataset, the export can complete without actually inserting any rows, leaving the dataset empty. Granting the SecOps service account the Data Editor role on the dataset gives it the necessary rights to insert and manage data within that dataset, enabling the export to populate it as expected. This is the precise, least-privilege permission needed for the write operation. The other options don't address the problem: assigning a user on the project doesn't change the service account's dataset permissions; granting serviceAccountUser to itself doesn't grant write access; and setting a retention period has no impact on whether data can be written to the dataset.

2. Which configuration would you implement if your goal is to pull data and tag using an ingestion label per log source?

A. Configure feed management to pull data and configure an ingestion label per log source.

B. Configure feed management to pull data from each location and configure a namespace per log source.

C. Configure a Bindplane agent collecting Syslog from each location and configure a namespace per log source.

D. Configure a Bindplane agent and an ingestion label per log source.

The main idea is to tag logs at ingestion so you can identify and route each source's data consistently. An ingestion label is attached to data as it enters the system, serving as a per-source tag that you can rely on for filtering, routing, and applying source-specific policies. A Bindplane agent runs at each log source to pull logs (like Syslog) and forward them into the ingestion pipeline. When you pair a Bindplane agent with an ingestion label for that log source, you achieve both pulling data from every location and tagging it appropriately at ingestion. Other approaches either rely on a different mechanism for organizing data (like a namespace) rather than tagging at ingestion, or omit the agent needed to pull data from each source, making per-source tagging less straightforward.

3. When evaluating a new endpoint detection tool for SecOps integration, which step is most directly tied to interoperability with existing workflows?

A. Identify the tool in the SecOps Marketplace and verify support for necessary actions.

B. Develop a custom integration with Python and Cloud Run to forward logs/orchestrate actions.

C. Review documentation to identify if default parsers exist; determine whether logs are supported/ingestable.

D. Identify hosting cloud provider.

Interoperability with your SecOps workflows is about whether the new tool can be controlled and triggered by the automation and playbooks you already use. The best first check is to look in the SecOps Marketplace for the tool and verify that it supports the actions your workflows require. If it exposes the same actions—such as creating or updating incidents, enriching alerts, or triggering remediation playbooks—the tool can slot into your existing SOAR, ticketing, and automation pipelines with minimal extra work. That direct compatibility means you don't have to rewrite or build custom integrations to fit your current processes, which keeps automation consistent and reduces friction. Building a custom integration, while useful, adds bespoke code, maintenance, and potential drift from standard actions, so it's more of a follow-up step if the marketplace-supplied actions don't cover what you need. Checking for default parsers and log ingestion concerns data formats and how logs are parsed, but it doesn't guarantee the tool will participate in your automated workflows. Simply identifying the hosting provider doesn't address how the tool will integrate into your runbooks or incident-response actions.

4. Which option would you implement to use a Bindplane agent collecting Syslog from each location and assign a namespace per log source to avoid IP aliasing?

A. Configure a Bindplane agent collecting Syslog from each location and configure a namespace per log source.

B. Configure feed management to pull data from each location and configure a namespace per log source.

C. Configure feed management to pull data and configure an ingestion label per log source.

D. Configure a Bindplane agent and an ingestion label per log source.

The idea being tested is how to keep log streams from different locations separate so they don't collide when IPs overlap. The right approach is to pull data using feed management and tag each log source with a unique ingestion label. That label acts as a namespace for the incoming data, so every log entry carries a clear origin tag that keeps streams distinct, even if the physical IPs are the same across locations. Using feed management to pull from each location centralizes the collection point, and assigning an ingestion label per log source provides a stable, scalable way to route and segregate data in the destination. This makes it easy to manage access, lineage, and retention for each source, and it prevents data from different sites from being mixed just because they share an IP address. Other approaches would rely on deploying agents or separate namespaces per source, which can be more cumbersome to maintain at many sites and may introduce more chances for misconfiguration. The labeling approach gives a clean, centralized mechanism to enforce isolation across all sources.

5. Group B requires access to all data except the 'restricted' namespace. Which data access scope design would satisfy this?

A. Create a new data access scope to include all data with a 'restricted' label.

B. Create a new data access scope to allow excluding a specific namespace.

C. Use a global data access scope with no exclusions.

D. Create a new data access scope to allow all data and exclude 'restricted' namespace for Group B; assign in IAM.

Fine-grained access control with data scopes lets you grant broad access while explicitly excluding certain areas. The best design here is to create a data access scope that permits all data but excludes the restricted namespace, then assign that scope to Group B in IAM. This directly gives Group B access to everything except the restricted namespace, satisfying the requirement. Why this works: it combines an inclusive scope (all data) with a clear exclusion (the restricted namespace), enforcing the exact limitation through IAM. Creating a scope that includes restricted data would violate the constraint. A scope that excludes a namespace without tying it to the specific restricted one could be ambiguous, and a global scope with no exclusions would grant access to the restricted data as well. Attaching the scope in IAM ensures consistent enforcement across resources for the group.

6. To generate an alert when a binary hash first appears, which approach should you implement?

A. Enable the Applied Threat Intelligence - Curated Prioritization rule set.

B. Use Alerts & IOCs page with a filter on hashes and first_seen_time.

C. Write a rule to examine file-related events that join with derived context for hashes in the entity graph; compare timestamp to first_seen_time.

D. Use statistics in search on the current day and verify first_seen_time predates the day.

Detecting the first appearance of a binary hash relies on tying each file event to the hash's first_seen_time in the derived hash context within the entity graph, then triggering when that event occurs at the same time as the hash's first_seen_time. By writing a rule that joins file-related events with the hash's derived context and compares the event timestamp to first_seen_time, you capture the exact moment the hash is observed for the first time in your environment, and you can alert immediately. The other approaches don't directly enable that real-time first-seen alert. A threat intelligence rule set focuses on known indicators rather than discovering and alerting on new appearances. The Alerts & IOCs page with a filter is a manual, ad-hoc view rather than an automatic alert. Using day-based statistics and first_seen_time predating the day is retrospective and not tied to the specific first occurrence of the hash, so it won't reliably trigger at the moment a hash first appears.

7. You observe multiple distinct, low-severity suspicious activities on a single internal server; no single event is a high-confidence IOC. You want ongoing heightened scrutiny. What should you do?

A. Schedule a daily SecOps report detailing all activity on this server.

B. Develop a server-specific YARA-L detection rule.

C. Add the server to a SecOps watchlist, and monitor closely.

D. Create a case, isolate the server, and escalate for forensics.

When you have multiple low-severity suspicious activities on a single internal server and no single event stands out as a strong IOC, the priority is to increase visibility without disrupting operations. Adding the server to a SecOps watchlist and monitoring it closely lets you track related activity, correlate events over time, and escalate if patterns or thresholds emerge. This approach provides focused oversight while preserving service availability, and it can scale as more data comes in. The other options either generate excessive noise (a daily report of all activity), rely on a specific detection rule that may not exist yet, or are too disruptive too soon (isolation and forensics) given the low-severity signals.

8. How should you configure two on-prem firewalls to forward logs to Google SecOps via Syslog?

A. Pull firewall logs using a SecOps feed integration.

B. Set the Google SecOps URL instance as the Syslog destination.

C. Deploy a third-party agent (e.g., Bindplane, NXLog) and set it as the Syslog destination.

D. Deploy a Google Ops Agent and set it as the Syslog destination.

The key idea is that on prem devices—like firewalls—send their logs via Syslog to a local collector, which then forwards them into Google SecOps. A third party agent such as BindPlane or NXLog serves as that Syslog destination, receiving the firewall's Syslog messages, handling any formatting and reliability concerns, and securely pushing them to Google SecOps. This bridging role is essential because most network devices don't speak Google SecOps ingestion protocols directly and aren't designed to be managed as direct Syslog endpoints for cloud services. Using a dedicated agent ensures compatibility, secure transport (often TLS), and reliable delivery, while also allowing you to normalize or filter logs as needed. The Google Ops Agent, while powerful for host-based log collection on Google Cloud or on supported on prem servers, isn't intended to act as a Syslog endpoint for network appliances. Directly pointing firewalls to a SecOps URL or having SecOps pull logs from devices isn't the typical, reliable path for on prem devices, which is why the bridging approach with a third party agent is the recommended solution.

9. Which approach should you take to generate a list of unknown command and control (C2) nodes within 24 hours?

A. Write a rule in Google SecOps that scans historic network outbound connections against ingested threat intel and run the rule as a retrohunt against the full tenant

B. Load network records into BigQuery to identify endpoints that are communicating with domains outside three standard deviations of normal

C. Review Security Health Analytics (SHA) findings in Security Command Center (SCC)

D. Write a YARA-L rule in Google SecOps that compares network traffic of endpoints to low prevalence domains against recent WHOIS registrations

To find unknown C2 nodes quickly, you want to hunt across your historical data using known malicious indicators. Writing a rule in Google SecOps that scans historic outbound connections against ingested threat intel and running it as a retrohunt against the full tenant lets you search all prior network activity at scale. Retrohunt gives you access to the entire data history, not just what's happening in real time, so endpoints that reached out to known C2 domains or IPs can be surfaced quickly—even if they weren't flagged earlier. By anchoring the scan to ingested threat intel, you directly target potential C2 communications, producing a precise list of affected endpoints within a 24-hour window. This approach is faster and more reliable for catching known-bad infrastructure connections across the whole environment than waiting for real-time anomalies or relying on configuration checks or domain-based heuristics that may be slower or noisy.

10. When Container Threat Detection alerts that an added binary has been executed in a business-critical workload, which two actions are most appropriate?

A. Notify the workload owner. Follow the response playbook, and involve threat hunting to identify the root cause

B. Review the finding, investigate the pod and related resources, and research the related attack and response methods

C. Quarantine the cluster containing the running pod and delete the running pod

D. Silence the alert in the SCC console, as the alert is low severity

When a container security alert indicates that a new binary was executed in a business-critical workload, the priority is to engage the right people quickly and follow a guided, repeatable response. Notifying the workload owner ensures that the business unit affected is aware of the risk, can assess impact, and coordinates the necessary resources for mitigation. At the same time, following the established response playbook preserves a structured, auditable track of actions, containment steps, evidence collection, and communication. Bringing in threat hunting to identify the root cause helps determine how the compromise occurred, whether other components are affected, and what indicators of compromise to look for, enabling faster containment and a more thorough remediation. Investigating the pod or related resources is important, but without notifying the owner and adhering to a formal playbook (including threat hunting), actions can be misaligned with business priorities and may miss broader indicators of compromise. Quarantining the cluster and deleting the pod can be too disruptive and may destroy evidence or hinder root-cause analysis. Silencing the alert is inappropriate for an active incident, as it prevents timely triage and coordinated response.

Next Steps

Congratulations on reaching the final section of this guide. You've taken a meaningful step toward passing your certification exam and advancing your career.

As you continue preparing, remember that consistent practice, review, and self-reflection are key to success. Make time to revisit difficult topics, simulate exam conditions, and track your progress along the way.

If you need help, have suggestions, or want to share feedback, we'd love to hear from you. Reach out to our team at hello@examzify.com.

Or visit your dedicated course page for more study tools and resources:

https://googlesecopsproengr.examzify.com

We wish you the very best on your exam journey. You've got this!