

RELIAQUEST SECURITY ANALYST / GREYMATTER SPECIALIST PRACTICE TEST (SAMPLE) STUDY GUIDE



SAMPLE STUDY GUIDE WITH LIMITED QUESTIONS

VISIT US ONLINE FOR
THE FULL VERSION STUDY GUIDE

<https://reliaquestsecanalgreymatter.examzify.com>



Copyright © 2026 by Examzify - A Kaluba Technologies Inc. product.

ALL RIGHTS RESERVED.

No part of this book may be reproduced or transferred in any form or by any means, graphic, electronic, or mechanical, including photocopying, recording, web distribution, taping, or by any information storage retrieval system, without the written permission of the author.

Notice: Examzify makes every reasonable effort to obtain accurate, complete, and timely information about this product from reliable sources.

SAMPLE

Table of Contents

Copyright	1
Table of Contents	2
Introduction	3
How to Use This Guide	4
Questions	5
Answers	8
Explanations	10
Next Steps	16

SAMPLE

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

SAMPLE

- 1. Which statement correctly describes the difference between GET and POST in HTTP?**
 - A. GET retrieves data from a resource; POST submits data to be processed to a resource.
 - B. GET submits data to be processed; POST retrieves data from a resource.
 - C. GET and POST both only retrieve data from a resource.
 - D. POST is used to decrypt data.
- 2. How would you go about identifying malicious activity?**
 - A. Review IDS/IPS logs
 - B. Analyze network traffic with WireShark
 - C. Run antivirus software
 - D. Review SIEM logs
- 3. Which HTTP status code range corresponds to informational responses?**
 - A. 100-199
 - B. 200-299
 - C. 300-399
 - D. 500-599
- 4. Differentiate between IOCs and TTPs and how Greymatter uses them in detections.**
 - A. IOCs describe observable artifacts like hashes, IPs, and domains; TTPs are attacker techniques and behaviors; Greymatter uses IOCs for known indicators and TTPs for behavior-based detections across techniques
 - B. IOCs are attacker techniques; TTPs are network indicators
 - C. They are the same concept and used interchangeably
 - D. IOCs are only used for historical analysis and never in live detections
- 5. What is a proxy server and what is its primary function?**
 - A. A firewall that blocks all traffic
 - B. A DNS resolver that translates domain names to IPs
 - C. A load balancer that distributes traffic to multiple servers
 - D. A proxy server sits between a user and the internet, forwarding requests and masking the user's identity

- 6. Which proxy sits in front of a web server to distribute requests and improve reliability?**
- A. Web Proxy
 - B. Forward Proxy
 - C. Reverse Proxy
 - D. Caching Proxy
- 7. Which input pattern is commonly associated with SQL injection attempts?**
- A. OR 1=1 --
 - B. SELECT * FROM users
 - C. Hello
 - D. 123456
- 8. What data pattern indicates exfiltration in Greymatter?**
- A. Inbound traffic spikes from trusted sources
 - B. Normal data transfer patterns
 - C. Frequent data backups to cloud storage
 - D. Unusual outbound data volumes, destinations, and times; correlate with endpoint and cloud data; use data loss prevention signals and DLP-integrated events.
- 9. Which TCP/IP layer ensures reliable data transmission (TCP) or fast transmission (UDP)?**
- A. Application Layer
 - B. Internet Layer
 - C. Network Access Layer
 - D. Transport Layer
- 10. Which incident metrics are commonly used to evaluate performance, and how should their trends be interpreted?**
- A. MTTR, MTTA, FP rate, detection coverage, mean time to containment, case closure rate; interpret trends to identify process gaps, training needs, or tool tuning requirements.
 - B. Only MTTR matters; other metrics are irrelevant.
 - C. FP rate should be ignored; only containment time matters.
 - D. Detection coverage is a security budget metric, not a performance metric.

Answers

SAMPLE

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

SAMPLE

Explanations

SAMPLE

1. Which statement correctly describes the difference between GET and POST in HTTP?

- A. GET retrieves data from a resource; POST submits data to be processed to a resource.**
- B. GET submits data to be processed; POST retrieves data from a resource.
- C. GET and POST both only retrieve data from a resource.
- D. POST is used to decrypt data.

HTTP methods separate retrieval from submission: GET retrieves data from a resource, while POST sends data to the server to be processed. GET puts any input in the URL as query parameters, making it clear, easily bookmarkable, and generally safe and idempotent (repeating the request shouldn't cause side effects). It's ideal for fetching or viewing data. POST carries data in the request body, which is why it's used for submitting forms or sending larger payloads to be processed by the server—actions that can create or modify resources. Repeating a POST can have side effects, like creating multiple records, which is why it's not considered idempotent by default. Also, data in the URL with GET is visible in browser history and logs, whereas POST keeps data in the body (though both require HTTPS to protect sensitive information). That's why the statement that GET retrieves data from a resource and POST submits data to be processed to a resource is the correct description. The other options mix up the roles, imply both are just retrieval, or incorrectly describe POST as decrypting data.

2. How would you go about identifying malicious activity?

- A. Review IDS/IPS logs**
- B. Analyze network traffic with WireShark
- C. Run antivirus software
- D. Review SIEM logs

Network threats are best spotted where they first manifest: in the traffic that traverses your environment. IDS/IPS logs are designed exactly for this—they monitor ongoing network traffic for suspicious patterns and known attack signatures, and they raise alerts with details like source and destination, timing, and the specific rule that was triggered. That direct, centralized visibility lets you spot malicious activity quickly and start containment or investigation promptly. While other tools help, they serve different purposes. Analyzing traffic with a packet sniffer like WireShark is invaluable for deep, manual investigation of a suspected incident on a specific host or small segment, but it isn't scalable for broad network monitoring and real-time detection. Antivirus software on endpoints can catch malware, but it focuses on hosts rather than overall network behavior and may miss covert or new-network-based activity. Reviewing SIEM logs is excellent for correlating events across multiple data sources, but the immediate indicators you need to act on usually originate from the network detection provided by IDS/IPS. In practice, use IDS/IPS logs as the first signal to identify potential malicious activity, then corroborate with SIEM, and if needed, perform targeted investigations with packet captures or endpoint tooling.

3. Which HTTP status code range corresponds to informational responses?

- A. 100-199**
- B. 200-299
- C. 300-399
- D. 500-599

Informational responses are provisional messages from the server that acknowledge receipt of the request and indicate that processing will continue. These codes live in the 1xx range (100–199). Examples include 100 Continue, 101 Switching Protocols, 102 Processing, and 103 Early Hints. They are not final results; the actual response body and final status come later. This is distinct from the other ranges: 2xx means the request succeeded, 3xx means redirection, 4xx means a client error, and 5xx means a server error. So the range that corresponds to informational responses is the 1xx, i.e., 100–199.

4. Differentiate between IOCs and TTPs and how Greymatter uses them in detections.

- A. IOCs describe observable artifacts like hashes, IPs, and domains; TTPs are attacker techniques and behaviors; Greymatter uses IOCs for known indicators and TTPs for behavior-based detections across techniques**
- B. IOCs are attacker techniques; TTPs are network indicators
- C. They are the same concept and used interchangeably
- D. IOCs are only used for historical analysis and never in live detections

Distinguishing observable artifacts from attacker tactics helps you understand how detections are built. IOCs are observable artifacts that indicate compromise or malicious activity, such as file hashes, IP addresses, domains, URLs, file names, or registry keys. TTPs describe attacker techniques and behaviors—the methods actors use to achieve their goals, like phishing, credential dumping, lateral movement, or command-and-control patterns. Greymatter uses IOCs to recognize known indicators that appear in telemetry and logs, giving quick, signature-like detections for established threats. It uses TTPs for behavior-based detections, looking for patterns of activity across techniques rather than relying on a single indicator. This enables detection across multiple stages of an intrusion and across different campaigns, catching variants that share techniques but not the same IOCs. Historically oriented uses aren't accurate because IOCs are actively used in live detections too, not just post-incident analysis. And treating IOCs and TTPs as the same thing or as interchangeable isn't correct because one is about concrete artifacts, the other about attacker methods and behaviors.

5. What is a proxy server and what is its primary function?

- A. A firewall that blocks all traffic
- B. A DNS resolver that translates domain names to IPs
- C. A load balancer that distributes traffic to multiple servers
- D. A proxy server sits between a user and the internet, forwarding requests and masking the user's identity**

A proxy server acts as an intermediary between a user and the internet. When a user makes a request, the proxy receives that request, forwards it to the destination server on behalf of the user, and then relays the response back to the user. This setup means the destination server often sees the proxy's address instead of the user's, effectively masking the user's identity. Proxies can also provide caching to speed up repeat requests, enforce security or access policies by inspecting or blocking certain traffic, and generate logs for monitoring and auditing. The other options describe different network functions. A firewall's job is to block or allow traffic based on rules rather than simply forwarding requests; a DNS resolver translates domain names to IP addresses but does not act as an intermediary that forwards requests on behalf of the user; a load balancer distributes incoming requests across multiple servers to balance load rather than focusing on masking identity or policy enforcement.

6. Which proxy sits in front of a web server to distribute requests and improve reliability?

- A. Web Proxy
- B. Forward Proxy
- C. Reverse Proxy**
- D. Caching Proxy

A reverse proxy is placed in front of one or more web servers and presents a single entry point to clients. It receives each client request, then forwards it to the most appropriate backend server, effectively distributing the load. This setup boosts reliability because if one backend server fails, the reverse proxy can route traffic to healthy servers and perform health checks. It also often handles TLS termination, security, and can cache or optimize traffic to improve performance, all while keeping the backend servers hidden from direct client access. Other proxy types don't fit this role: a forward proxy sits on the client side to access external resources, not in front of a web server to balance inbound traffic; a caching proxy focuses on storing copies of content for future requests; a generic web proxy term is too ambiguous to specify the front-end load-balancing function.

7. Which input pattern is commonly associated with SQL injection attempts?

- A. OR 1=1 --**
- B. SELECT * FROM users
- C. Hello
- D. 123456

SQL injection attempts often rely on turning a condition into something that's always true and then silencing the rest of the query with a comment. The input pattern `OR 1=1 --` does exactly that: it adds a tautology (`1=1`) to the query's logic so the `WHERE` clause evaluates true regardless of user input, and the `--` starts a comment so the remainder of the original SQL is ignored. This combination is a classic way attackers try to bypass authentication or reveal data in vulnerable applications. The other inputs don't modify the query structure in the same way. A plain string like `SELECT * FROM users` is an actual SQL statement, not an injected payload. Simple values like `Hello` or `123456` are just data and won't by themselves alter the query's logic unless they're improperly concatenated into a statement with quotes, which is what injection patterns aim to exploit.

8. What data pattern indicates exfiltration in Greymatter?

- A. Inbound traffic spikes from trusted sources
- B. Normal data transfer patterns
- C. Frequent data backups to cloud storage
- D. Unusual outbound data volumes, destinations, and times; correlate with endpoint and cloud data; use data loss prevention signals and DLP-integrated events.**

Exfiltration shows up when data leaves the environment in a way that doesn't fit normal behavior. The strongest signal is unusual outbound data volumes to destinations that aren't typical, and at odd times. When you connect that outbound activity with evidence from endpoints (what processes or users are involved) and cloud data (where the data is going in the cloud), and you see data loss prevention signals or DLP-integrated events flagging sensitive data, the pattern becomes a clear indicator of data being exfiltrated. This multi-source correlation is key because it turns a noisy outbound event into a credible threat signal, reducing false alarms and confirming that sensitive data is moving out of the environment. Inbound spikes from trusted sources and normal data transfer patterns don't indicate exfiltration because they align with legitimate, expected activity rather than outbound leakage. Frequent data backups to cloud storage could be legitimate operations as well, especially if they follow established schedules and trusted destinations; they don't inherently imply data leaving the network in an anomalous or unauthorized way unless paired with unusual outbound behavior and DLP cues.

9. Which TCP/IP layer ensures reliable data transmission (TCP) or fast transmission (UDP)?

- A. Application Layer
- B. Internet Layer
- C. Network Access Layer
- D. Transport Layer**

End-to-end data delivery characteristics are defined at the Transport Layer, where protocols can trade reliability for speed. TCP provides reliable, connection-oriented transmission with sequencing, acknowledgments, and retransmission to ensure data arrives correctly. UDP offers a fast, connectionless service with no guaranteed delivery or ordering, prioritizing low overhead. The Internet Layer handles routing and addressing (IP) but does not guarantee delivery, while the Network Access Layer is concerned with how data is framed and transmitted on the local link. So the capability to choose between reliable and fast transmission for these protocols sits at the Transport Layer.

10. Which incident metrics are commonly used to evaluate performance, and how should their trends be interpreted?

- A. MTTR, MTTA, FP rate, detection coverage, mean time to containment, case closure rate; interpret trends to identify process gaps, training needs, or tool tuning requirements.
- B. Only MTTR matters; other metrics are irrelevant.
- C. FP rate should be ignored; only containment time matters.
- D. Detection coverage is a security budget metric, not a performance metric.**

Evaluating incident response performance relies on a set of metrics that describe how quickly and effectively a team detects, acknowledges, contains, and resolves incidents, as well as how well the monitoring environment is covered. Metrics like mean time to respond (MTTR), mean time to acknowledge (MTTA), false-positive rate, detection coverage, mean time to containment, and case closure rate capture different parts of that performance picture. Interpreting trends in these metrics helps you spot where the process is strong or slipping: falling MTTR and MTTA indicate faster detection and initial action; shorter containment times show improved ability to stop damage quickly; a lower false-positive rate signals better alert quality and less wasted investigation; higher detection coverage means more of the environment or data sources are being monitored, reducing blind spots; and rising case closures reflect more efficient triage and resolution. The idea that detection coverage is solely a security budget metric isn't aligned with how these measurements are used to gauge performance. While budgets affect resource availability, detection coverage itself is about how much of the environment is actually monitored and how complete the telemetry is, which directly influences incident performance. If trends diverge (for example, delays in containment despite high coverage), that points to specific process gaps, training needs, or tool tuning requirements that should be addressed.

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://reliaquestsecanalgreymatter.examzify.com>

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

SAMPLE