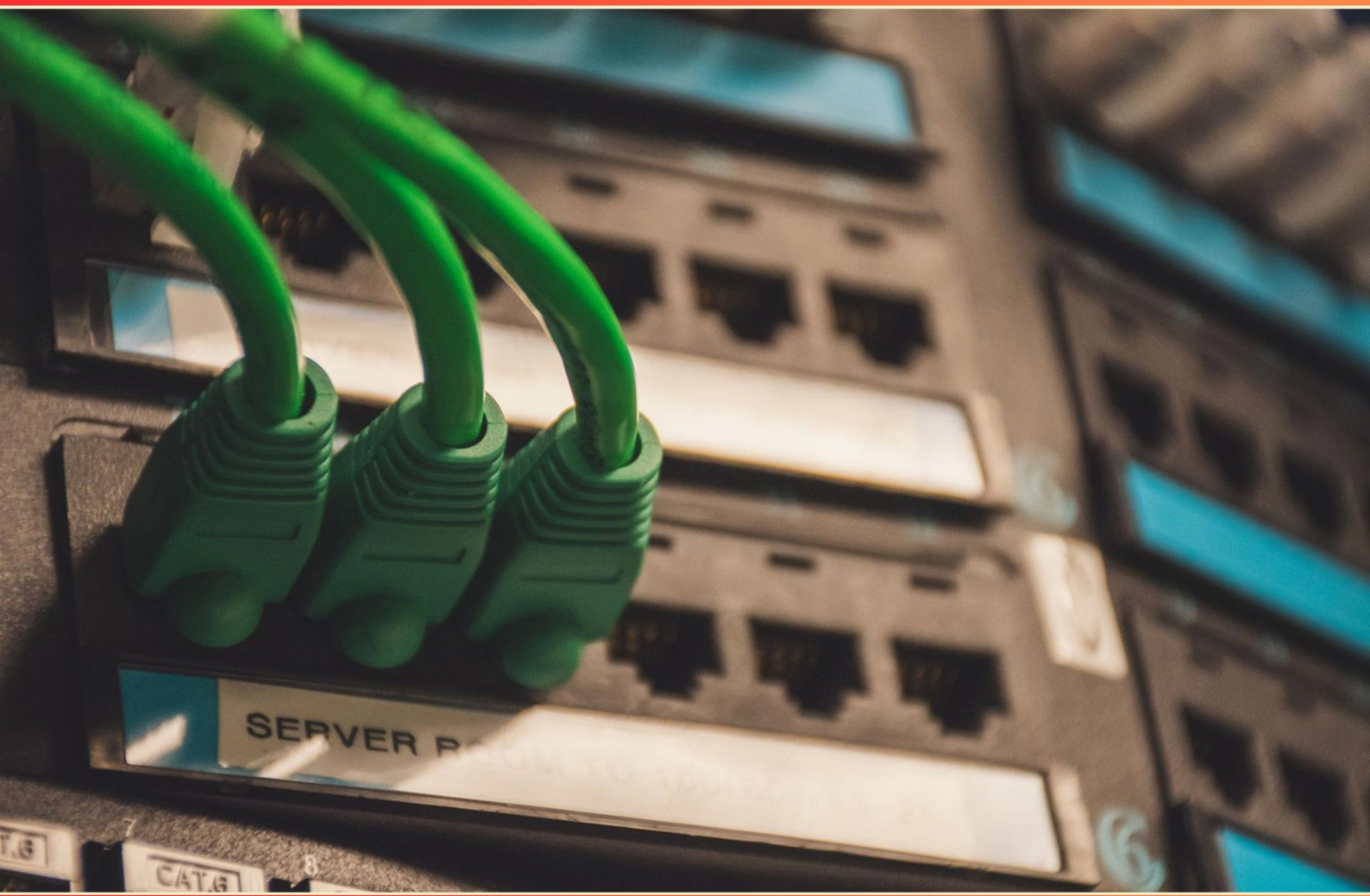
SECURITY BLUE TEAM LEVEL 1 PRACTICE TEST (SAMPLE)

STUDY GUIDE



SAMPLE STUDY GUIDE WITH LIMITED QUESTIONS

VISIT US ONLINE FOR THE FULL VERSION STUDY GUIDE

https://securityblueteamlvl1.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 15

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.

SAMPLE

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!

SAMPLE

Questions

SAMPLE

1. What is file carving in digital forensics?

A. Deleting files securely

B. Encrypting files on disk

C. A technique to recover files or fragments by identifying file signatures

D. Compressing large files

2. Which of the following signals would you examine in basic network traffic analysis to detect anomalous activity?

A. All of the above

B. Unusual DNS requests

C. Beacon-like patterns

D. Unusual ports

3. In the Threat Intelligence Lifecycle, which stage disseminates finished intelligence to the places it needs to go?

A. Planning & Direction

B. Collection

C. Dissemination

D. Feedback

4. What is CASB and why is it used?

A. Cloud Access Security Broker; provides visibility, data protection, and threat protection for use of cloud services

B. A type of firewall hardware

C. A tool for database backups

D. A VPN alternative

5. Threat Exposure Check involves using multiple tools to look for indicators of compromise retrieved from which sources?

A. Internal security logs only

B. A single vendor feed

C. Public vulnerability databases

D. Intelligence vendors, information sharing partners, government alerts, OSINT sources

SAMPLE

6. Why is time synchronization important in security monitoring?

A. Ensures accurate timestamps for logs, enabling proper event correlation and incident timelines.

B. Reduces network bandwidth usage.

C. Eliminates the need for backups.

D. Improves user authentication speed.

7. Which group is typically motivated by political or social causes rather than financial gain?

A. Nation-States/APTs

B. Hacktivists

C. Cyber Criminals

D. Insiders

8. What describes Hosted Malware?

A. Malware hosted on websites that users click to download

B. A malicious domain or compromised site hosting malware

C. Malware embedded in image files

D. Malware delivered via USB drives

9. In incident response, what is the primary goal of containment actions?

A. To eradicate the attacker from the environment.

B. To determine the root cause.

C. To limit the spread and impact of the incident.

D. To document evidence for legal action.

10. Hacktivists are typically motivated by social or political issues.

A. Financial gain

B. Personal grudges

C. Social or political issues

D. Random acts

SAMPLE

Answers

SAMPLE

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

SAMPLE

Explanations

SAMPLE

1. What is file carving in digital forensics?

A. Deleting files securely

B. Encrypting files on disk

C. A technique to recover files or fragments by identifying file signatures

D. Compressing large files

File carving in digital forensics is the process of recovering files or their fragments by scanning the raw data for known file signatures (magic numbers) and then reconstructing the file boundaries. This approach doesn't rely on the file system's metadata, so it's useful when the file system is damaged, missing, or when files have been deleted and their directory entries are gone. The technique looks for start and end markers of different file types and can piece together fragments that are dispersed across the storage medium, sometimes reconstructing a complete file from noncontiguous data blocks. For example, JPEGs have recognizable markers at the beginning and end, PDFs start with a distinct header, and PNGs begin with a specific byte sequence. Limitations exist: data can be misinterpreted if multiple files share similar signatures, and encrypted or highly compressed content may not reveal clear signatures to carve. Also, carved files can be incomplete or corrupted if the fragments aren't properly reconstructible. This approach is distinct from securely deleting data (which overwrites it), encrypting data (which hides content), or compressing data (which reduces size but isn't about recovering files from raw data).

2. Which of the following signals would you examine in basic network traffic analysis to detect anomalous activity?

A. All of the above

B. Unusual DNS requests

C. Beacon-like patterns

D. Unusual ports

In basic network traffic analysis, you look for signs where normal patterns break, especially around where traffic is flowing and what services are being used. Unusual ports stand out because many attackers use non-standard ports or unexpected ports to hide traffic or bypass simple filters. When you see traffic on ports that don't match what's typical for your environment, it's a strong red flag that something may be misconfigured, unauthorized, or probing your network. It's a clear, actionable signal you can flag for deeper inspection—check the source, destination, protocol, and payload to confirm what service or device is involved and whether it should be communicating on that port. Unusual DNS requests and beacon-like patterns can also indicate anomalies—DNS tunneling, exfiltration, or periodic malware beacons—but they generally require more context or baseline knowledge to interpret accurately and can generate more false positives in a basic setup. So while they're important, unusual port activity provides the most straightforward, high-signal cue for initial detected anomalous activity.

SAMPLE

3. In the Threat Intelligence Lifecycle, which stage disseminates finished intelligence to the places it needs to go?

A. Planning & Direction

B. Collection

C. Dissemination

D. Feedback

Dissemination is the stage where finished, validated intelligence is delivered to the people and systems that need it. After analysis turns raw data into actionable findings, it must be distributed through the right channels—alerts to security tools, dashboards for analysts, reports for leadership—at the right time and in the appropriate format so it can be acted upon. Planning & Direction sets what needs to be collected and prioritized; Collection is the gathering of data; Feedback closes the loop by evaluating usefulness and guiding improvements. So, the act of delivering the completed intelligence to its intended audience is what dissemination covers.

4. What is CASB and why is it used?

A. Cloud Access Security Broker; provides visibility, data protection, and threat protection for use of cloud services

B. A type of firewall hardware

C. A tool for database backups

D. A VPN alternative

Cloud Access Security Broker (CASB) sits between users and cloud services and enforces security policies as cloud apps are used. It gives you visibility into which cloud apps are in use (including shadow IT), protects data in the cloud through controls like data loss prevention and encryption, and provides threat protection through monitoring, anomaly detection, and policy enforcement. CASB helps with compliance by auditing activity and enforcing governance across SaaS, IaaS, and PaaS. It can be deployed in API-based or proxy-based modes and works to prevent risky access or data exfiltration by applying policies at access and data levels. For example, it can block uploading a sensitive file to an unsanctioned cloud app. So the best description is that CASB provides visibility, data protection, and threat protection for the use of cloud services. It's not a hardware firewall, not a database backup tool, and not a VPN alternative.

5. Threat Exposure Check involves using multiple tools to look for indicators of compromise retrieved from which sources?

A. Internal security logs only

B. A single vendor feed

C. Public vulnerability databases

D. Intelligence vendors, information sharing partners, government alerts, OSINT sources

The idea being tested is that a thorough threat exposure check looks for indicators of compromise across a broad mix of sources, not just one place. Pulling IOCs from intelligence vendors, information-sharing partners, government alerts, and OSINT sources gives a wide view of active threats and campaigns. This diverse feed captures a range of indicators—malicious domains, IPs, file hashes, and TTPs—from vendors who aggregate telemetry, partners who share industry-specific intel, official government advisories, and open-source intelligence. Relying on a single source like internal logs or one vendor limits visibility and may miss new or broader threats. Public vulnerability databases are useful for vulnerabilities themselves but don't always provide the live IOC signals associated with active compromises. So the best approach is a multi-source intake that includes those intelligence channels, which is why that option is the correct one.

SAMPLE

6. Why is time synchronization important in security monitoring?

A. Ensures accurate timestamps for logs, enabling proper event correlation and incident timelines.

B. Reduces network bandwidth usage.

C. Eliminates the need for backups.

D. Improves user authentication speed.

Accurate timestamps across all systems are essential for security monitoring because they let you correctly order and link events from different devices. When clocks drift, a log from one host may appear earlier or later than related activity on another, making it hard to tell what happened first, how actions are connected, or how an incident unfolded. Time synchronization lets your SIEM correlate events and build a reliable incident timeline, which is crucial for detection, investigation, and response. It also supports forensics and legal considerations by ensuring evidence is timestamped consistently. The other options miss the core purpose: time synchronization doesn't primarily reduce bandwidth, eliminate backups, or speed up authentication, and those benefits don't directly help with coordinating events across an environment.

7. Which group is typically motivated by political or social causes rather than financial gain?

A. Nation-States/APTs

B. Hacktivists

C. Cyber Criminals

D. Insiders

Hacktivists are driven by political or social goals, using cyber actions to promote a cause or raise awareness rather than to make money. Their primary aim is impact on public perception or policy, not financial gain, so they might deface sites, leak information, or disrupt services to spotlight an issue. While nation-state actors can have political aims, their activities are typically aligned with strategic objectives for a government, including espionage or broad influence, and money is not their main driver. Cyber criminals focus on profits like ransom, theft, or fraud, and insiders can be motivated by a range of factors that aren't exclusively ideological. So the group most associated with political or social motivation is hacktivists.

8. What describes Hosted Malware?

A. Malware hosted on websites that users click to download

B. A malicious domain or compromised site hosting malware

C. Malware embedded in image files

D. Malware delivered via USB drives

Hosted malware means the attacker places the malicious payload on a remote host so it can be served to victims from that location. A malicious domain or a compromised site hosting the malware fits this idea perfectly because the site acts as the delivery point, storing the payload and distributing it to users who visit or interact with it. This setup enables techniques like drive-by downloads or exploit-driven redirects, where simply visiting the site can trigger the delivery of the malware. Why the other ideas don't fit as well: embedding malware in image files is a different tactic (steganography or payload concealment within media), and malware delivered via USB drives involves physical media rather than a remote hosting site. The description about malware hosted on websites that users click to download is close, but the defining feature of hosted malware is that the malicious code is hosted on a domain or compromised site acting as the hosting point for the payload.

SAMPLE

9. In incident response, what is the primary goal of containment actions?

A. To eradicate the attacker from the environment.

B. To determine the root cause.

C. To limit the spread and impact of the incident.

D. To document evidence for legal action.

Containment aims to stop the incident from spreading and to limit its impact. The goal is to quickly isolate affected systems and block further access or propagation so the organization can investigate safely, preserve evidence, and plan eradication and recovery without the attacker moving to additional targets. For example, isolating compromised machines, blocking malicious traffic, or segmenting the network are typical containment actions. The other steps—removing the attacker, determining the root cause, and collecting evidence for legal action—are important but part of later stages; containment's immediate priority is preventing additional damage and narrowing the scope of the incident.

10. Hacktivists are typically motivated by social or political issues.

A. Financial gain

B. Personal grudges

C. Social or political issues

D. Random acts

Hacktivism is driven by using hacking as a form of activism. The core idea is that social or political concerns motivate the actions, with the aim of protesting, raising awareness, or pressuring organizations or governments to change policies. Because the goal is ideological advocacy, the methods are chosen to maximize visibility for the cause—such as website defacement, information leaks, or coordinated DDoS activity—rather than to steal money or cause random disruption. That's why the motivation line up with social or political issues. In contrast, financial gain points to criminal profit, personal grudges point to revenge, and random acts lack a consistent objective tied to a protest or campaign.

SAMPLE

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://securityblueteamlvl1.examzify.com

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

SAMPLE