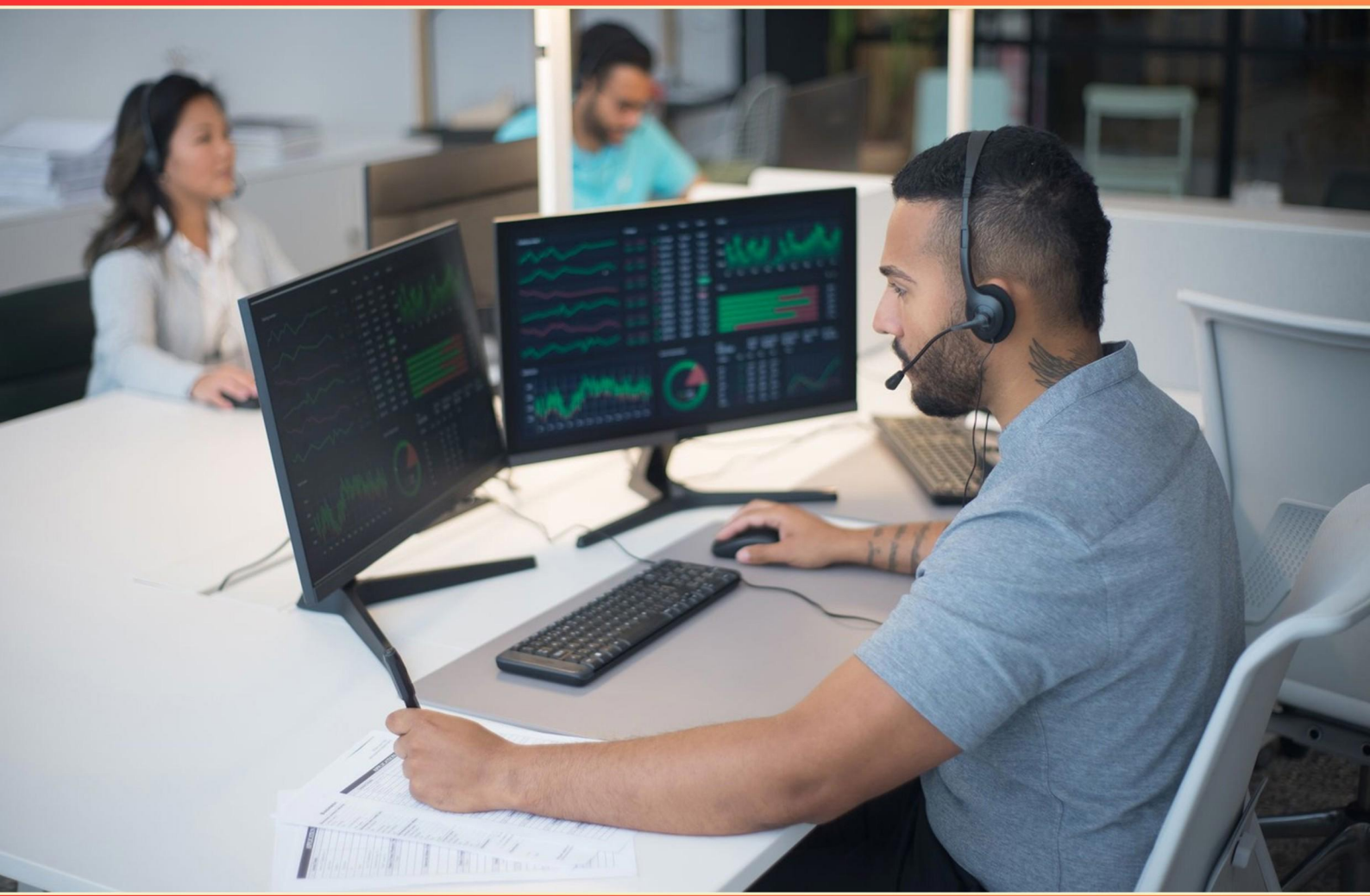
SECURITY OPERATIONS EXAM 3 PRACTICE (SAMPLE)

STUDY GUIDE



SAMPLE STUDY GUIDE WITH LIMITED QUESTIONS

VISIT US ONLINE FOR THE FULL VERSION STUDY GUIDE

https://securityops3.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.

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 are the stages of threat intelligence lifecycle and how should it be integrated into security operations?

A. Planning, collection, processing, analysis, dissemination, and feedback.

B. Initiation, execution, review, and closure.

C. Detection, response, recovery, and renewal.

D. Acquisition, normalization, distribution, and archiving.

2. In ABAC, which factors are used to determine access decisions?

A. User roles only

B. Resource ownership only

C. Environment and resource state only

D. User attributes, resource attributes, and environment attributes

3. What is zero-trust architecture and what are its core components relevant to operations?

A. A security model that trusts internal network; core components: static access controls

B. A security model requiring verification for every access request. Core components: strong authentication, continuous authorization, device posture checks, micro-segmentation, and least-privilege access

C. A model focusing on perimeter firewall only

D. An architecture for offline systems

4. What is a common mitigation for legacy systems lacking patches?

A. Upgrade hardware

B. Isolation from the network

C. Expose to Internet

D. Disable Logging

5. Explain the importance of chain of custody during digital forensics investigations and what can happen if it's broken.

A. Maintaining the chain of custody preserves evidence integrity and admissibility; breaking it can render evidence unusable.

B. Chain of custody is optional for digital evidence.

C. Chain of custody only applies to physical objects, not digital data.

D. Breaking chain of custody improves admissibility.

SAMPLE

6. Which statement best describes the purpose of an incident response runbook and its essential elements?

A. Runbooks provide only general incident goals with no step-by-step actions.

B. Runbooks document the organization's policy but not operational procedures.

C. Runbooks provide step-by-step actions for responders during incidents and include scope, roles, contact lists, escalation paths, containment steps, eradication guidelines, evidence handling, communication plans, and recovery procedures.

D. Runbooks are primarily training materials not used during live incidents.

7. Which term refers to attacks involving psychological manipulation to trick users, including phishing, vishing, baiting, and tailgating?

A. Shadow AI

B. Staging Areas and Data Exfiltration

C. Social Engineering attacks

D. Stakeholders

8. What is the role of business continuity planning (BCP) in security operations and how does it relate to disaster recovery?

A. BCP is primarily about IT system backups.

B. DR focuses on business process continuity.

C. BCP and DR are unrelated.

D. BCP ensures critical business functions continue during disruptions; DR focuses on restoring IT systems. They are complementary.

9. Which framework comprises Preparation, Detection & Analysis, Containment/Eradication/Recovery, and Post-Incident Activity?

A. NIST Cybersecurity Framework

B. PDCA Cycle

C. OODA Loop

D. NIST Incident Response Life Cycle

10. Which testing approach represents a realistic end-to-end drill that may involve red teams?

A. Full Simulation

B. Tabletop

C. Mock

D. Checklist Review

SAMPLE

Answers

SAMPLE

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

SAMPLE

Explanations

SAMPLE

1. What are the stages of threat intelligence lifecycle and how should it be integrated into security operations?

A. Planning, collection, processing, analysis, dissemination, and feedback.

B. Initiation, execution, review, and closure.

C. Detection, response, recovery, and renewal.

D. Acquisition, normalization, distribution, and archiving.

The stages of threat intelligence lifecycle are planning, collection, processing, analysis, dissemination, and feedback. Start with planning to define what intelligence is needed based on business risk, assets, and threat landscape, setting clear requirements and timelines that align with security operations. Then collect data from multiple sources—internal telemetry like logs and alerts, external feeds, OSINT, commercial feeds, and even relevant dark web intel—ensuring the data is timely and relevant. Processing comes next, where you normalize, deduplicate, and enrich that data, turning raw indicators into a structured, usable dataset with context such as asset associations and geography. Analysis is the step where trained analysts interpret the data, assess credibility and relevance, map tactics, techniques, and procedures to frameworks like MITRE ATT&CK, and produce actionable intelligence that describes who the threat is, what they're doing, and why it matters. Dissemination then delivers this intelligence to the right people in the right format—briefing emails, dashboards, intel reports, or integrated alerts in SIEM/SOAR systems—so SOC teams and incident responders can act quickly. Finally, feedback closes the loop: measure usefulness, capture outcomes, refine requirements, and adjust data sources and methods, so future intelligence is more accurate and timely. Integrating this into security operations means feeding intelligence into daily work. Threat feeds enrich alerts, hunting plans, and detections; playbooks and automation can incorporate IOCs, YARA rules, or ATT&CK mappings to accelerate response; analysts can use intelligence to prioritize incidents and tailor mitigations; and the cycle should continually inform risk assessments, patch programs, and user education. Other lifecycle models described by the distractors resemble general project management or incident response stages and don't capture the full, repeatable flow from defining needs through to actionable, operational intelligence and feedback, which is why they're less appropriate for threat intelligence integration.

2. In ABAC, which factors are used to determine access decisions?

A. User roles only

B. Resource ownership only

C. Environment and resource state only

D. User attributes, resource attributes, and environment attributes

ABAC makes access decisions by evaluating multiple attributes across three areas: who the user is, what the resource is, and the context of the request. User attributes include things like identity, role, department, and clearance. Resource attributes cover properties such as owner, classification, sensitivity, and type. Environment attributes encompass the context of the access request, like time of day, location, network security, and device health. This combination lets policies specify nuanced rules, such as: a user in a particular role can access certain resources only during business hours on a trusted network, and only if the resource has a matching sensitivity level. That's why using all three attribute types is the essence of ABAC. Relying on only one aspect—such as user roles, or ownership, or environmental state alone—fails to capture the full, flexible access control that ABAC aims to provide.

SAMPLE

3. What is zero-trust architecture and what are its core components relevant to operations?

A. A security model that trusts internal network; core components: static access controls

B. A security model requiring verification for every access request. Core components: strong authentication, continuous authorization, device posture checks, micro-segmentation, and least-privilege access

C. A model focusing on perimeter firewall only

D. An architecture for offline systems

Zero-trust architecture treats every access request as untrusted until proven otherwise, requiring verification for every access attempt regardless of location. In operations this means enforcing policies that continuously validate who is requesting access, what they're trying to reach, and the state of the device and context at the moment of access. The core components that enable this are strong authentication (often multi-factor), continuous authorization that re-evaluates permissions as context changes, device posture checks to ensure the requesting device is compliant and healthy, micro-segmentation to limit lateral movement by enforcing granular network segments, and least-privilege access to ensure users and services have only the minimal rights needed. Together, these elements support dynamic, policy-based control rather than relying on a trusted internal network perimeter. Choosing options that rely on trusting internal networks with static controls, focusing only on a perimeter firewall, or addressing offline systems misses the ongoing verification, contextual decisions, and granular enforcement that zero-trust requires.

4. What is a common mitigation for legacy systems lacking patches?

A. Upgrade hardware

B. Isolation from the network

C. Expose to Internet

D. Disable Logging

Isolating unpatched legacy systems from the network is a common mitigation because it directly reduces the attack surface and limits what an attacker can reach or do if a vulnerability is present. When patches aren't available or a system is past its supported life, placing it in a tightly controlled network segment with strict access rules restricts traffic to only what's truly necessary. This containment helps prevent exploitation from spreading laterally and minimizes potential impact, making it a practical compensating control in such scenarios. Other options don't provide the same protective effect. Upgrading hardware might help performance or compatibility in some cases, but it doesn't address the underlying vulnerability if the software isn't patched. Exposing the system to the Internet would dramatically increase risk, not mitigate it. Disabling logging removes essential visibility into incidents, making it harder to detect and respond to any breach.

SAMPLE

5. Explain the importance of chain of custody during digital forensics investigations and what can happen if it's broken.

A. Maintaining the chain of custody preserves evidence integrity and admissibility; breaking it can render evidence unusable.

B. Chain of custody is optional for digital evidence.

C. Chain of custody only applies to physical objects, not digital data.

D. Breaking chain of custody improves admissibility.

Chain of custody is the documented, chronological record of who has handled digital evidence, where it has been, and how it has been preserved. In digital forensics, this trail matters because data can be easily copied, altered, or corrupted, often without obvious signs. By maintaining a clear chain, investigators demonstrate that the evidence presented is the same data collected from its source and has remained intact and untainted along the way. This preserves the evidence's integrity and supports its admissibility in court, since a proven provenance helps establish authenticity and accountability. If the chain is broken, the credibility of the evidence is questioned. Gaps in documentation or unlogged transfers give room for arguments that the data could have been altered, planted, or tampered with, making its authenticity suspect. As a result, the evidence can be challenged, possibly excluded, or given little weight in proceedings. To prevent this, investigators use measures like hash verifications, proper labeling, secure storage, access controls, and meticulous, time-stamped logging to show that each step in handling digital evidence was documented and preserved.

6. Which statement best describes the purpose of an incident response runbook and its essential elements?

A. Runbooks provide only general incident goals with no step-by-step actions.

B. Runbooks document the organization's policy but not operational procedures.

C. Runbooks provide step-by-step actions for responders during incidents and include scope, roles, contact lists, escalation paths, containment steps, eradication guidelines, evidence handling, communication plans, and recovery procedures.

D. Runbooks are primarily training materials not used during live incidents.

An incident response runbook is an operational, action-oriented guide that tells responders exactly what to do during an incident and who is responsible for each action. It moves beyond general goals to provide a clear, repeatable plan that coordinates the team under pressure. The essential elements include: - Scope: what is in and out of bounds for the incident response - Roles: who is doing what, so responsibilities are clear - Contact lists: who to reach for internal and external support - Escalation paths: when and to whom to escalate issues or decisions - Containment steps: actions to limit the impact and prevent spread - Eradication guidelines: how to remove the threat from the environment - Evidence handling: how to collect, preserve, and document for forensics - Communication plans: who is informed, what is communicated, and when - Recovery procedures: steps to restore services and verify normal operations This combination ensures responses are consistent, timely, and coordinated, minimizes confusion during high-stress incidents, supports proper evidence handling, and provides a foundation for post-incident review and improvement. Runbooks are used in live responses and are updated based on lessons learned, not merely as policy documents or training materials that aren't applied during actual incidents.

SAMPLE

7. Which term refers to attacks involving psychological manipulation to trick users, including phishing, vishing, baiting, and tailgating?

A. Shadow AI

B. Staging Areas and Data Exfiltration

C. Social Engineering attacks

D. Stakeholders

The key idea here is that the attacker relies on manipulating people rather than exploiting technical weaknesses. These methods—phishing, vishing, baiting, and tailgating—all depend on tricking users into taking actions they shouldn't, such as revealing passwords, clicking malicious links, or granting physical access. That broad category is called social engineering attacks, because it targets human psychology—trust, fear, urgency, curiosity—to achieve unauthorized access or information. Shadow AI would imply hidden or unobserved AI behavior, which isn't about deceiving people. Staging areas and data exfiltration describe how data is prepared and removed from a network, focusing on the mechanics of theft rather than manipulating individuals. Stakeholders are the people involved with a system or project, not a type of attack.

8. What is the role of business continuity planning (BCP) in security operations and how does it relate to disaster recovery?

A. BCP is primarily about IT system backups.

B. DR focuses on business process continuity.

C. BCP and DR are unrelated.

D. BCP ensures critical business functions continue during disruptions; DR focuses on restoring IT systems. They are complementary.

The main idea is resilience: business continuity planning ensures essential business functions keep running during any disruption, covering people, processes, facilities, and information needed to maintain operations. Disaster recovery is the IT-focused side of that effort, aiming to restore IT systems, data, and infrastructure after a disruption so the business can support its processes again. They are complementary: BCP defines what must be recovered and in what order to keep the business functioning, while DR provides the technical means to bring IT capacity back online to meet those needs. In security operations, this means BCP guides how operations continue during incidents (including communications and coordination), and DR outlines the steps to restore critical IT services after the incident.

SAMPLE

9. Which framework comprises Preparation, Detection & Analysis, Containment/Eradication/Recovery, and Post-Incident Activity?

A. NIST Cybersecurity Framework

B. PDCA Cycle

C. OODA Loop

D. NIST Incident Response Life Cycle

This question tests understanding of the structured sequence used to handle security incidents from start to finish. The framework that lists Preparation, Detection & Analysis, Containment/Eradication/Recovery, and Post-Incident Activity is the NIST Incident Response Life Cycle. It begins with Preparation—setting up the IR team, playbooks, tools, and communication plans so you're ready to act. Detection & Analysis follows, where incidents are identified, classified, and their scope and impact assessed to decide the appropriate response. Containment/Eradication/Recovery then focuses on limiting the damage, removing the attacker's access, restoring systems, and validating operations. Finally, Post-Incident Activity looks at lessons learned, updates to plans and controls, and improvements to prevent similar incidents in the future. The other frameworks don't define this exact sequence: the NIST Cybersecurity Framework is a broader risk-management model, PDCA is a generic continuous-improvement cycle, and the OODA Loop is a rapid decision-making cycle.

10. Which testing approach represents a realistic end-to-end drill that may involve red teams?

A. Full Simulation

B. Tabletop

C. Mock

D. Checklist Review

A full simulation is a live, end-to-end drill that tests the entire incident response chain—from initial detection through containment, eradication, and recovery—under realistic conditions. It often involves red teams acting as attackers to mimic real adversaries, pushing people, processes, and technology to respond as they would in a real incident. This level of realism validates how well runbooks are followed, how escalation and communications work, and how tools and teams coordinate under pressure, giving a true measure of readiness. Tabletop exercises are discussion-based and don't involve active systems or live operations, so they don't test actual responses in a real environment. Mock scenarios can be limited in scope and may not exercise the full sequence of events or cross-team collaboration. Checklist reviews focus on whether controls exist on paper rather than on how they perform in practice.

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://securityops3.examzify.com

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

SAMPLE