Security Operations Exam 3 Practice (Sample)

Study Guide

Everything you need from our exam experts!

Table of Contents

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. **Which volatile data sources should be collected during an in-progress incident?**

   A. **RAM memory (processes, network connections, injection artifacts); open network connections/sockets; running services and processes.**

   B. **Disk-based event logs and archived files**

   C. **Full memory dump only**

   D. **Network traffic data collected only from the perimeter firewall**

2. **What security service sits between cloud consumers and cloud providers to enforce security policies, provide visibility, DLP, and shadow IT detection?**

   A. **WAF**

   B. **VPN Gateway**

   C. **SIEM Solutions**

   D. **CASB - Cloud Access Security Broker**

3. **In incident response, which action is used to remove the root cause of an incident?**

   A. **Containment**

   B. **Recovery**

   C. **Reimaging**

   D. **Remediation**

4. **How does EDR complement traditional antivirus?**

   A. **It records endpoint behaviors to enable proactive threat hunting and containment, not just signature-based alerts.**

   B. **It replaces all network firewalls and VPNs.**

   C. **It automatically fixes all malware without human intervention.**

   D. **It performs vulnerability scanning across the entire enterprise.**

5. Which set of tools includes Strings, whois, VirusTotal, hashing, and hex editors?

A. Staging Areas and Data Exfiltration

B. Shadow AI

C. Strings, whois, VirusTotal, hashing, hex editors

D. Session Management - protection

6. Which statement describes the purpose of 'Strings' in binary analysis?

A. Scans for SQL vulnerabilities

B. Modifies binary code

C. Extracts text from binaries

D. Generates encryption keys

7. What is the primary purpose of a SOC playbook?

A. The primary purpose of a SOC playbook is to document detection and response steps for typical incidents.

B. It is for long-term financial planning.

C. It replaces all incident response plans.

D. It provides legal advice.

8. Which tool captures live network traffic for analysis and can be used defensively for troubleshooting and offensively for credential harvesting?

A. Proxy

B. VPN

C. Intrusion Detection System

D. Network Sniffers

9. Which Unix tool can monitor real-time resource usage to detect anomalies such as cryptojacking?

A. ps

B. top

C. ls

D. grep

10. Which mitigation is commonly used to defend against Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks?

A. Code optimization

B. Traffic scrubbing

C. User authentication

D. Data deduplication

Answers

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

Explanations

1. Which volatile data sources should be collected during an in-progress incident?

A. RAM memory (processes, network connections, injection artifacts); open network connections/sockets; running services and processes.

B. Disk-based event logs and archived files

C. Full memory dump only

D. Network traffic data collected only from the perimeter firewall

In an in-progress incident, volatile data—data that vanishes if the system is rebooted or shut down—needs to be captured first to see the system's live state. RAM holds the current execution state, including which processes are running, current network connections, and any injected or decrypted artifacts active in memory. Capturing open network connections and sockets reveals who the host is talking to in real time, which can expose command-and-control activity, lateral movement, or data exfiltration. The set of running services and processes shows what is actively loaded and may highlight malicious processes masquerading as legitimate ones or unusual startup items. Together, these volatile sources give a real-time snapshot of the attack as it unfolds and what evidence could disappear if the system changes state. Disk-based event logs and archived files are important for post-incident analysis, but they are not volatile data and don't reflect the live in-progress state. A full memory dump is useful, but limiting collection to only a memory dump misses the broader live context provided by active network connections and running processes. Network data from the perimeter firewall alone misses host-side activity and hidden processes.

2. What security service sits between cloud consumers and cloud providers to enforce security policies, provide visibility, DLP, and shadow IT detection?

A. WAF

B. VPN Gateway

C. SIEM Solutions

D. CASB - Cloud Access Security Broker

Cloud Access Security Broker (CASB) sits between cloud consumers and cloud providers to enforce security policies, provide visibility into cloud usage, deliver data loss prevention, and detect shadow IT. It acts as the security control point across SaaS, IaaS, and PaaS, able to monitor who is accessing what data, apply policy-driven protections, and surface unsanctioned applications. CASB can enforce access controls, encryption, and threat protection, often via in-line or API-based deployments, giving organizations control over data as it moves to and from cloud services. This combination of policy enforcement, visibility, DLP, and shadow IT detection is not the primary function of a WAF, VPN gateway, or SIEM, making CASB the best fit for the described role.

3. In incident response, which action is used to remove the root cause of an incident?

A. Containment

B. Recovery

C. Reimaging

D. Remediation

Remediation focuses on removing the underlying weakness that allowed the incident to occur, so the issue won't happen again. This involves fixing the actual vulnerability or misconfiguration, applying patches, changing insecure configurations, updating access controls, revoking or strengthening credentials, and implementing new processes or controls to prevent recurrence. Containment stops the incident from spreading by isolating affected systems, but it doesn't fix the underlying flaw. Recovery aims to bring operations back to normal after containment, often by restoring systems and data, yet it doesn't eliminate the root cause itself. Reimaging cleans a compromised machine, removing visible malware from that host, but it may skip broader fixes needed to prevent a repeat across the environment.

4. How does EDR complement traditional antivirus?

A. It records endpoint behaviors to enable proactive threat hunting and containment, not just signature-based alerts.

B. It replaces all network firewalls and VPNs.

C. It automatically fixes all malware without human intervention.

D. It performs vulnerability scanning across the entire enterprise.

EDR extends antivirus by continuously monitoring and recording endpoint behaviors to enable proactive threat hunting and rapid containment, rather than relying solely on signature-based alerts. It gathers rich telemetry from processes, file and registry activity, memory, network connections, and user actions, giving security teams a detailed view of what's happening on each endpoint. This behavioral data makes it possible to spot unknown or fileless threats that don't match existing signatures, trace an attack's progression, and understand how it moved through the environment. With this context, teams can act quickly to contain or remediate—such as isolating a compromised device or stopping malicious activity—without waiting for a signature update. While traditional antivirus focuses on known malware patterns, EDR provides the visibility and response capabilities to address advanced or evolving threats. The other options don't fit because EDR is not meant to replace all network security appliances like firewalls or VPNs, it doesn't automatically fix every piece of malware without some human or policy-driven intervention, and vulnerability scanning is a different function that assesses weaknesses rather than monitoring ongoing endpoint activity.

5. Which set of tools includes Strings, whois, VirusTotal, hashing, and hex editors?

A. Staging Areas and Data Exfiltration

B. Shadow AI

C. Strings, whois, VirusTotal, hashing, hex editors

D. Session Management - protection

These tools form a defender's toolkit for investigating suspicious artifacts. Strings lets you pull readable text from binaries, revealing clues like embedded URLs or API calls. Whois helps map the origin of infrastructure by showing domain ownership and registration details, which aids in tracing attacker infrastructure. VirusTotal aggregates many antivirus engines and community reports, giving quick insight into whether a file, hash, or URL is known malware. Hashing creates fixed-length fingerprints to verify integrity or compare against known-good baselines or reported malicious hashes. Hex editors let you inspect and edit the raw bytes of a file, essential for low-level analysis and uncovering hidden payloads. Together, these are the exact kinds of tools a security analyst uses for malware analysis, threat hunting, or incident response. The other choices describe concepts or domains rather than a concrete toolset, so they don't fit as the set of tools listed.

6. Which statement describes the purpose of 'Strings' in binary analysis?

A. Scans for SQL vulnerabilities

B. Modifies binary code

C. Extracts text from binaries

D. Generates encryption keys

In binary analysis, Strings refers to the practice of extracting human-readable text embedded inside an executable or library. This is valuable because binaries often contain messages, error strings, URLs, file paths, API names, or even hard-coded credentials that reveal what the program does and how it operates. By listing these strings, an analyst gains quick, actionable clues about the program's behavior without running it. This is a read-only activity that helps identify potential touchpoints, endpoints, or secrets. It isn't about modifying the binary, generating keys, or scanning for SQL vulnerabilities, which are separate analysis tasks.

7. What is the primary purpose of a SOC playbook?

A. The primary purpose of a SOC playbook is to document detection and response steps for typical incidents.

B. It is for long-term financial planning.

C. It replaces all incident response plans.

D. It provides legal advice.

A SOC playbook is a structured guide that standardizes how the team detects and responds to typical security incidents. Its primary purpose is to document the exact detection criteria and the step-by-step actions analysts should take to contain, eradicate, and recover from common threats. This includes clear roles, decision points, escalation paths, and links to related runbooks and tooling, so responses are fast, consistent, and aligned with the incident response process. A playbook acts as practical, repeatable instructions that improve speed and accuracy during incidents and also serves as training and reference material. It isn't meant to replace the overall incident response plan, it isn't for long-term financial planning, and it doesn't provide legal advice.

8. Which tool captures live network traffic for analysis and can be used defensively for troubleshooting and offensively for credential harvesting?

A. Proxy

B. VPN

C. Intrusion Detection System

D. Network Sniffers

Capturing live network traffic for analysis is what network sniffers do. They monitor a network segment by putting an interface into promiscuous mode or using a mirror/tap to copy packets as they flow, letting you inspect headers, payloads, timings, and protocol behavior in real time. This makes them incredibly useful for defensive troubleshooting—you can see where delays occur, identify misconfigurations, and diagnose failures by watching actual traffic patterns as they happen. They also carry inherent risk: if traffic includes plaintext credentials, a sniffer can reveal them, which attackers might exploit for credential harvesting. Encryption greatly mitigates this risk because readable passwords won't be in the captured data. Other tools don't provide the same full-wire visibility. A proxy forwards and potentially logs traffic but doesn't give you the complete picture of everything on the network segment. A VPN encrypts traffic between endpoints, hiding its contents from local sniffing. An intrusion detection system monitors and analyzes traffic for signs of malicious activity rather than capturing and inspecting every packet. So, the ability to capture and analyze live network traffic on the wire is what makes network sniffers the best fit.

9. Which Unix tool can monitor real-time resource usage to detect anomalies such as cryptojacking?

A. ps

B. top

C. ls

D. grep

The idea is to watch how system resources are being used in real time so you can spot anomalies like a hidden miner consuming CPU cycles. The Unix tool that provides a live, constantly updating view of all running processes and their resource usage is top. It shows per-process CPU and memory usage, system load, and overall resource trends, all updated continuously. Because a cryptomining program typically uses a large share of CPU for extended periods, you can spot it quickly by looking for a process consuming unusually high CPU that doesn't correspond to legitimate activity. You can sort the display by CPU usage to bring heavy processors to the top and drill into which program is responsible, which makes it an effective first-line detector. Other commands like ps give a static snapshot of processes, and ls or grep have different, non-monitoring roles. They won't continuously reflect real-time activity or highlight spikes in resource use, which is why top is the best fit for monitoring and detecting such anomalies as they happen.

10. Which mitigation is commonly used to defend against Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks?

A. Code optimization

B. Traffic scrubbing

C. User authentication

D. Data deduplication

Mitigating DoS and DDoS attacks hinges on cleaning the traffic before it reaches the target. Traffic scrubbing does exactly that: your inbound traffic is routed through scrubbing centers where malicious or anomalous packets are filtered out, and only clean, legitimate traffic is sent on to the destination. This approach is well suited to DoS floods, which overwhelm bandwidth or resources, because the scrubbing service can absorb and discard the excess malicious traffic at scale, then pass normal traffic through. With Distributed attacks, distributing and redirecting traffic to multiple scrubbers allows the defender to filter across a wide geographic and network footprint, reducing impact on the origin. Code optimization focuses on performance of software, not on stopping harmful traffic floods. User authentication won't help when attackers don't need valid credentials or when floods attack availability rather than access control. Data deduplication improves storage efficiency, not network-layer denial of service.

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!