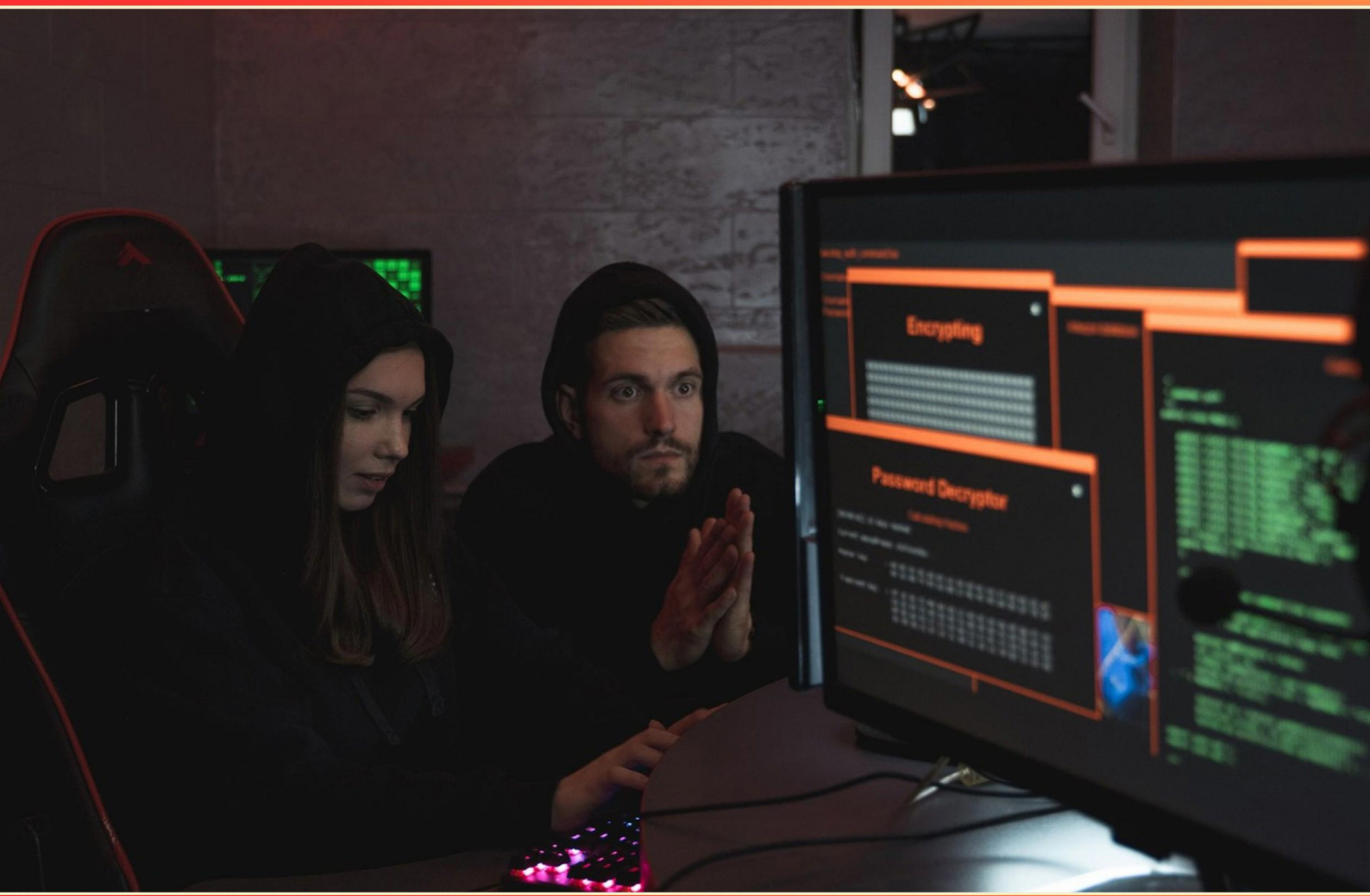
SPLUNK CERTIFIED CYBERSECURITY DEFENSE ANALYST PRACTICE EXAM (SAMPLE)

STUDY GUIDE



SAMPLE STUDY GUIDE WITH LIMITED QUESTIONS

VISIT US ONLINE FOR THE FULL VERSION STUDY GUIDE

https://
splunkcybersecuritydefenseanalyst.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 information is displayed in the ES Identity Domain dashboards?**

   A. Network traffic and security issues

   B. Asset and identity data

   C. Incident resolutions

   D. Background process insights

2. **What is the primary goal of applying security controls as part of risk mitigation?**

   A. To enhance productivity

   B. To reduce the likelihood of breaches

   C. To improve business continuity

   D. To analyze security data

3. **Which type of information does the description field in a risk modifier provide?**

   A. General usage of the risk property

   B. An explanation of the risk modifier

   C. Statistical data summary

   D. Log event timestamps

4. **What is the primary purpose of email compromise attacks in organizations?**

   A. Network infiltration

   B. Theft of money or information

   C. Unauthorized data leaks

   D. Gaining access to user accounts

5. **What is an Adaptive Response Action in Splunk Enterprise Security?**

   A. A method for data visualization

   B. Actions taken in response to notable events or correlation search results

   C. A technique for data encryption

   D. An assessment tool for user behavior analytics

SAMPLE

6. What term refers to any entity representing potential security threats tracked by Splunk Enterprise Security?

A. Threat Indicator

B. Security Asset

C. Risk Object

D. Vulnerability

7. What action does Risk Avoidance primarily focus on?

A. Mitigating identified risks

B. Completely eliminating risks

C. Monitoring risk levels

D. Transferring risk responsibilities

8. What is a primary purpose of the makeresults command in Splunk?

A. To archive data

B. To generate test data for dashboards

C. To return errors in searches

D. To import external data sources

9. What type of malware is described as ransomware?

A. A type of malware that steals personal data

B. A type of malware that encrypts files for ransom payment

C. A type of malware that displays unwanted advertisements

D. A type of malware that replicates itself to disrupt services

10. What type of data formats are supported for output when using the makeresults command?

A. HTML and XML

B. CSV and JSON

C. Text and Markdown

D. PDF and Text

SAMPLE

Answers

SAMPLE

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

SAMPLE

Explanations

SAMPLE

1. What information is displayed in the ES Identity Domain dashboards?

A. Network traffic and security issues

B. Asset and identity data

C. Incident resolutions

D. Background process insights

The correct answer highlights that the ES Identity Domain dashboards specifically display asset and identity data. These dashboards are designed to give visibility into the relationships between users, their identities, and the assets they interact with within an organization's environment. By focusing on this data, the dashboards provide insights into who is accessing what resources, the status of those assets, and the potential risks associated with identity management. This information is crucial for understanding the security posture regarding user access and identity management, enabling security teams to identify potential vulnerabilities and enforce stronger controls. The other options touch on relevant aspects of security monitoring but do not embody the central focus of the ES Identity Domain dashboards. Network traffic and security issues pertain more broadly to general network and security monitoring, while incident resolutions are about addressing specific security events. Background process insights are less relevant in the context of identity and asset management, as they focus instead on internal operations rather than the relationships between users and their access rights.

2. What is the primary goal of applying security controls as part of risk mitigation?

A. To enhance productivity

B. To reduce the likelihood of breaches

C. To improve business continuity

D. To analyze security data

The primary goal of applying security controls as part of risk mitigation is to reduce the likelihood of breaches. Security controls are implemented to identify vulnerabilities, protect sensitive data, and minimize potential threats that could exploit these weaknesses. By proactively addressing risks through security measures, organizations can create a safer environment that ultimately lowers the chances of a successful cyber-attack or data breach. While enhancing productivity, improving business continuity, and analyzing security data can all be benefits of a robust security posture, they are not the primary focus when it comes to risk mitigation. The main objective is centered on preventing incidents that could harm the organization, its data, and its stakeholders by making it more challenging for attackers to succeed. Therefore, the reduction of breach likelihood serves as a cornerstone of effective risk management strategies in cybersecurity.

SAMPLE

3. Which type of information does the description field in a risk modifier provide?

A. General usage of the risk property

B. An explanation of the risk modifier

C. Statistical data summary

D. Log event timestamps

The description field in a risk modifier is specifically designed to provide an explanation of the risk modifier itself. This field offers context and details about the purpose and function of the risk modifier within the overall risk assessment framework. By containing descriptive content, it aids analysts and security professionals in understanding the specific attributes or implications of the risk being modified. This clarity is essential for effective risk management, as it allows users to make informed decisions based on the nature of the risk being evaluated or influenced. Understanding the details provided in the description field can help in aligning the risk modifier with organizational policies and response strategies, ultimately enhancing the organization's cybersecurity posture.

4. What is the primary purpose of email compromise attacks in organizations?

A. Network infiltration

B. Theft of money or information

C. Unauthorized data leaks

D. Gaining access to user accounts

The primary purpose of email compromise attacks in organizations is primarily focused on the theft of money or information. These attacks typically exploit social engineering techniques to manipulate individuals into providing sensitive information, such as login credentials or financial data. Attackers often impersonate trusted contacts, leading victims to either inadvertently disclose important information or authorize transfers of funds. Email compromise can also involve various tactics, such as spear-phishing, where a specifically targeted email prompts the receiver to take an action that can result in financial loss or data exposure. In this context, the objective aligns more closely with financial gain or acquiring valuable data rather than just gaining access to user accounts or causing unauthorized data leaks. While gaining access to user accounts may be a tactic utilized during these attacks, the overarching goal remains to achieve monetary or informational theft, making it the fundamental purpose of these types of incidents.

SAMPLE

5. What is an Adaptive Response Action in Splunk Enterprise Security?

A. A method for data visualization

B. Actions taken in response to notable events or correlation search results

C. A technique for data encryption

D. An assessment tool for user behavior analytics

An Adaptive Response Action in Splunk Enterprise Security refers specifically to the actions that can be automatically triggered in response to notable events or results from correlation searches. This feature allows security analysts to establish predefined responses to certain conditions based on the data they receive, enhancing their ability to react swiftly to potential threats. Implementing Adaptive Response Actions enables automated responses such as alerting, creating tickets, or executing commands to mitigate threats, thus promoting a proactive security posture. It supports incident management by providing a structured framework for dealing with security events in real time, further streamlining the workflow for security operations teams. The other options do not align with the concept of Adaptive Response Actions. For instance, the method for data visualization, a technique for data encryption, and assessment tools for user behavior analytics do not involve the immediate, adaptable responses facilitated by Adaptive Response Actions that focus specifically on responding to security incidents as they occur.

6. What term refers to any entity representing potential security threats tracked by Splunk Enterprise Security?

A. Threat Indicator

B. Security Asset

C. Risk Object

D. Vulnerability

The term that best describes any entity representing potential security threats tracked by Splunk Enterprise Security is "Threat Indicator." This term encompasses a range of information that can indicate malicious activity or potential vulnerabilities in a system. In the context of cybersecurity, threat indicators can include IP addresses associated with malicious activities, specific file hashes, URLs, or techniques known to be used by threat actors. Using "Threat Indicator" allows organizations to systematically track, analyze, and respond to these potential threats, enabling better detection and response strategies. This concept is central to threat intelligence, where the aggregation and analysis of threat data facilitate a proactive stance against cyber threats. In contrast, while "Security Asset" refers to any asset that has security importance, including hardware and software, it does not specifically pertain to threats. "Risk Object" is a more general concept often related to assessing potential risks but does not directly identify entities that indicate threats. "Vulnerability" refers to weaknesses in a system that could be exploited by threats but is not itself an entity representing a threat. Each of these terms has its place in the cybersecurity lexicon, but "Threat Indicator" specifically addresses the tracking of potential security threats within Splunk.

SAMPLE

7. What action does Risk Avoidance primarily focus on?

A. Mitigating identified risks

B. Completely eliminating risks

C. Monitoring risk levels

D. Transferring risk responsibilities

Risk Avoidance primarily focuses on completely eliminating risks by changing plans to sidestep potential threats or vulnerabilities. This concept means that instead of accepting the risks and implementing risk mitigation strategies, organizations choose to alter their processes or avoid certain actions altogether that might lead to exposure. For example, if a company identifies that launching a product in a particular market poses significant cybersecurity risks, they might decide not to enter that market at all. By doing so, they eliminate the risks associated with that specific venture. This approach is particularly valuable when risks are deemed too high and the potential negative impacts are significant. While other options discuss various risk management strategies—such as mitigating, monitoring, or transferring risks—none of these capture the essence of risk avoidance, which is entirely centered on eliminating the risk itself rather than managing or sharing it in some way.

8. What is a primary purpose of the makeresults command in Splunk?

A. To archive data

B. To generate test data for dashboards

C. To return errors in searches

D. To import external data sources

The primary purpose of the makeresults command in Splunk is to generate test data for dashboards and searches. This command is particularly useful for testing and developing search queries, visualizations, and dashboards without needing real data. By creating a handful of synthetic events, analysts can quickly see how their search logic works in practice, ensuring that it behaves as expected before applying it to live data. This capability is fundamental in the development environment where you might want to simulate different conditions or visualize how data could look based on specific parameters. The flexibility it offers allows for rapid iterations in dashboard design and functionality testing, contributing significantly to an efficient development process. In contrast, archiving data, returning errors in searches, or importing external data sources involve different functionalities and processes in Splunk. These are not the primary focus of the makeresults command, highlighting its specialized role in testing and development.

SAMPLE

9. What type of malware is described as ransomware?

A. A type of malware that steals personal data

B. A type of malware that encrypts files for ransom payment

C. A type of malware that displays unwanted advertisements

D. A type of malware that replicates itself to disrupt services

Ransomware is a specific category of malware designed to encrypt a victim's files, rendering them inaccessible until a ransom is paid to the perpetrator. This form of attack exploits the victim's urgency or desperation to regain access to their data, often accompanied by threats to delete the encrypted files if payment is not made within a certain timeframe. In the context of the available choices, the correct identification of ransomware as malware that encrypts files for ransom payment highlights its distinctive purpose and functionality compared to other types of malware. For instance, malware that steals personal data focuses on exfiltrating information without necessarily holding it hostage. Those types of malware are typically designed for data theft rather than encryption for ransom. Similarly, the option that describes malware displaying unwanted advertisements pertains to adware, which aims to generate revenue through intrusive ads rather than coercing victims for ransom. Finally, malware that replicates itself to disrupt services aligns with characteristics of worms or disruptive viruses, which do not involve encrypting files or demanding payment. Thus, the focus of ransomware was accurately captured as the type that specifically encrypts files with the intention of obtaining a ransom.

10. What type of data formats are supported for output when using the makeresults command?

A. HTML and XML

B. CSV and JSON

C. Text and Markdown

D. PDF and Text

The makeresults command in Splunk is used to generate sample events for testing and experimentation. When using this command, it can produce output in various formats, with CSV and JSON being two of the most commonly utilized formats for structured data representation. CSV (Comma-Separated Values) is widely used for data exchange and is easily readable by spreadsheet applications. JSON (JavaScript Object Notation), on the other hand, is a lightweight data format that is easy for humans to read and write and easy for machines to parse and generate. Both formats support structured data representation, making them suitable outputs for a command designed to create sample events effectively. While other options may involve output formats that can be used in certain contexts, they do not represent the primary formats associated with the makeresults command. The focus on CSV and JSON reflects increased interoperability and ease of use in data processing workflows commonly employed in data analysis and cybersecurity contexts.

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://splunkcybersecuritydefenseanalyst.examzify.com

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

SAMPLE