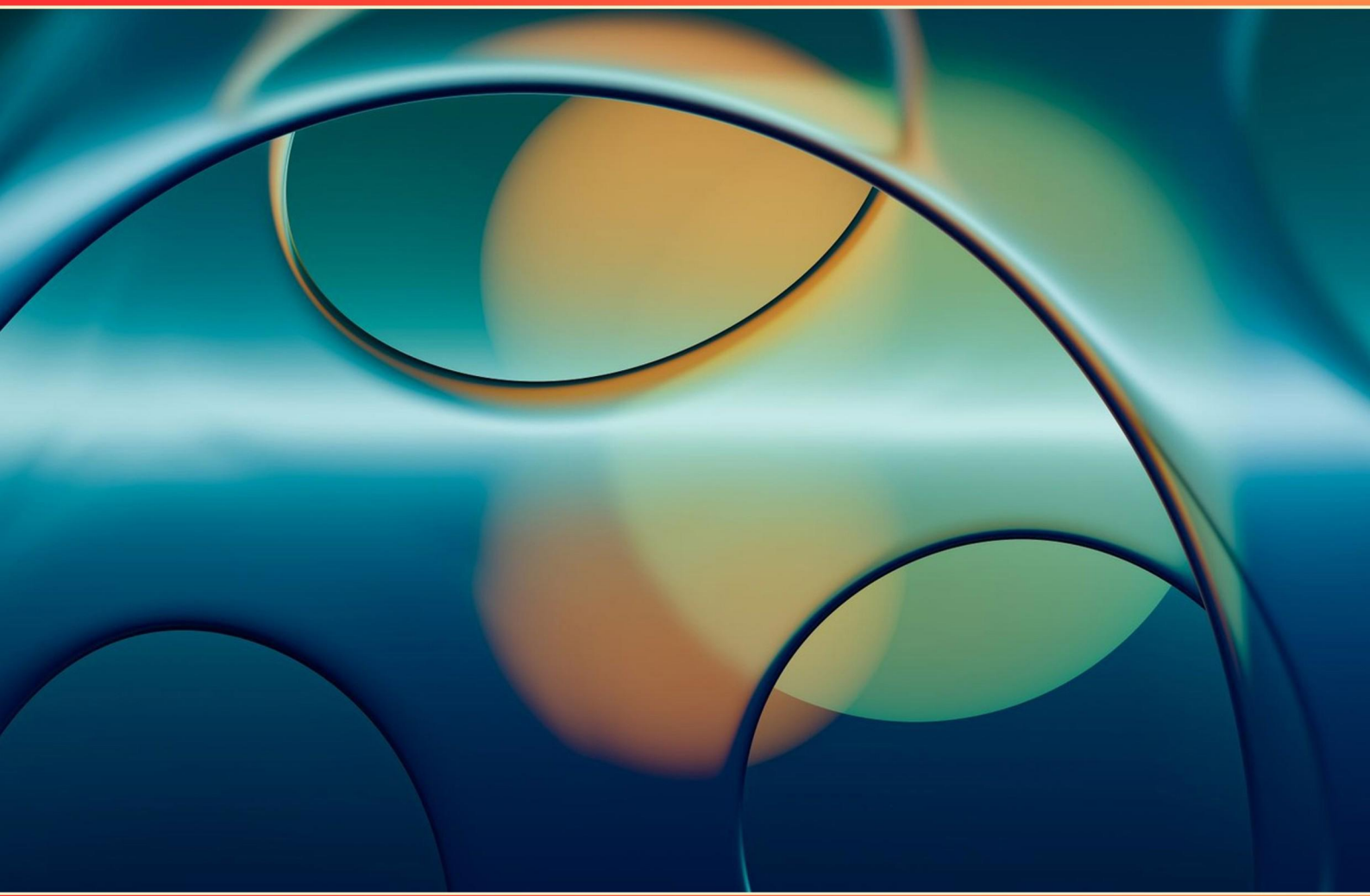
PSE CORTEX PROFESSIONAL PRACTICE TEST (SAMPLE)

STUDY GUIDE



SAMPLE STUDY GUIDE WITH LIMITED QUESTIONS

VISIT US ONLINE FOR THE FULL VERSION STUDY GUIDE

https://psecortexpro.examzify.com

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. **What allows the use of predefined roles to assign access rights to Cortex XDR users?**

   A. Restrictions security profile

   B. Cloud Identity Engine

   C. Endpoint Groups

   D. Role-based Access Control (RBAC)

2. **Which deployment type supports installation of an engine on Windows, Mac OS, and Linux?**

   A. RPM

   B. SH

   C. DEB

   D. ZIP

3. **How do machine learning algorithms enhance operations in PSE Cortex?**

   A. They automate repetitive tasks and provide predictive insights

   B. They increase manual labor requirements

   C. They only function with small datasets

   D. They have minimal impact on overall performance

4. **What steps should an administrator take to confirm false positives in a security event?**

   A. Disable the "Prevent Malicious Child Process Execution" module

   B. Add specific processes to the whitelist

   C. Review parent and child processes and command line arguments

   D. Contact support for a security exception

5. **A General Purpose Dynamic Section can be added to which two layouts for incident types?**

   A. "Close" Incident Form

   B. Incident Summary

   C. Incident Quick View

   D. "New/Edit" Incident Form

6. What key benefit does the Cortex XDR platform offer for threat detection?

A. Requires minimal configuration

B. Provides unified visibility across endpoints

C. Only focuses on network traffic analysis

D. Relies solely on user intervention

7. What is the function of the "Acknowledge" command in the Cortex XSOAR War Room?

A. To close an incident

B. To track the progress of an investigation

C. To officially recognize a task has been reviewed

D. To escalate an issue for higher-level handling

8. Cortex XDR can schedule recurring scans of endpoints for malware. Identify two methods for initiating an on-demand malware scan?

A. Response > Action Center

B. The local console

C. Telnet

D. Endpoint > Endpoint Management

9. What is the role of cloud computing in PSE Cortex?

A. Providing scalable infrastructure for data storage and processing

B. Enhancing user interface and experience

C. Developing mobile applications for remote access

D. Implementing security protocols for client data

10. Which Cortex XDR capability extends investigations to an endpoint?

A. Log stitching

B. Causality Chain

C. Sensors

D. Live Terminal

Answers

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

Explanations

1. What allows the use of predefined roles to assign access rights to Cortex XDR users?

A. Restrictions security profile

B. Cloud Identity Engine

C. Endpoint Groups

D. Role-based Access Control (RBAC)

The use of predefined roles to assign access rights to Cortex XDR users is supported by Role-based Access Control (RBAC). RBAC is a crucial security feature that simplifies the management of user permissions by associating them with roles rather than individual users. Each role is defined with specific permission levels, which allows administrators to efficiently control access across various functionalities within the system. Assigning predefined roles enables organizations to implement a principle of least privilege, ensuring that users have no more access than necessary for their job functions. This structured approach not only enhances security by minimizing the risk of unauthorized access but also streamlines user management, as roles can be easily adjusted or updated without needing to change permissions for each individual user. In contrast, other options like the Restrictions security profile, Cloud Identity Engine, and Endpoint Groups play different roles in the security landscape but do not specifically cater to the assignment of access rights through predefined roles in the same way that RBAC does.

2. Which deployment type supports installation of an engine on Windows, Mac OS, and Linux?

A. RPM

B. SH

C. DEB

D. ZIP

The correct choice is the deployment type that supports installation of an engine on Windows, Mac OS, and Linux through a ZIP file format. The ZIP format is a widely recognized archive file format that can be easily utilized across multiple operating systems, allowing users to extract and access the necessary files regardless of whether they are using Windows, Mac OS, or Linux. When users choose this option, they benefit from its cross-platform compatibility, making it convenient to install the necessary engine on their system of choice without being restricted to a specific operating system's package format. This flexibility is particularly important for users who may switch between operating systems or work in diverse environments. In contrast, other deployment types, such as RPM, SH, and DEB, are associated with specific Linux distributions and may not be compatible with Windows or Mac OS. RPM (Red Hat Package Manager) and DEB (Debian Package) are primarily used in Red Hat and Debian-based systems, respectively, while SH is a shell script that can primarily run in Unix/Linux environments. Hence, they limit installation options to specific platforms rather than supporting a broader range of operating systems like ZIP does.

3. How do machine learning algorithms enhance operations in PSE Cortex?

A. They automate repetitive tasks and provide predictive insights

B. They increase manual labor requirements

C. They only function with small datasets

D. They have minimal impact on overall performance

Machine learning algorithms are integral in enhancing operations within PSE Cortex by automating repetitive tasks and providing predictive insights. Automation increases efficiency by allowing systems to handle routine tasks without human intervention, thereby freeing up personnel to focus on more complex issues that require human intelligence and creativity. This streamlining of operations can lead to significant time savings and reduced error rates in data handling. Additionally, predictive insights derived from machine learning can enable organizations to foresee trends and make informed decisions. By analyzing historical data, these algorithms can identify patterns that might not be immediately visible to human analysts, which allows PSE Cortex to optimize resource allocation, enhance operational strategies, and improve overall effectiveness. The other options do not accurately reflect the contributions of machine learning in this context. Increased manual labor requirements or functionality limitations to small datasets contradict the very purpose of these algorithms. Lastly, stating that they have minimal impact on performance undermines the transformative effect that machine learning has on operational efficiency and decision-making in PSE Cortex.

4. What steps should an administrator take to confirm false positives in a security event?

A. Disable the "Prevent Malicious Child Process Execution" module

B. Add specific processes to the whitelist

C. Review parent and child processes and command line arguments

D. Contact support for a security exception

To effectively confirm false positives in a security event, reviewing parent and child processes along with command line arguments is crucial for the administrator. This step allows the administrator to analyze the context of the process execution, identify any legitimate processes that may have been flagged incorrectly, and assess the relationships between different processes. By understanding how processes are interlinked and the commands used to initiate them, the administrator can make informed decisions on whether they should be considered malicious. This process is essential in distinguishing between genuine threats and benign activities, ultimately leading to a more accurate security posture. Whitelisting specific processes can be a part of the solution after thorough vetting but relies on an understanding of what processes are truly safe in the environment. Hence, investigating the details of these processes is the foundational step required to address potential misclassifications effectively.

5. A General Purpose Dynamic Section can be added to which two layouts for incident types?

A. "Close" Incident Form

B. Incident Summary

C. Incident Quick View

D. "New/Edit" Incident Form

The correct choice is that a General Purpose Dynamic Section can be added to the Incident Summary layout. This selection is based on the functionality and purpose of Dynamic Sections within the context of incident management. A General Purpose Dynamic Section is designed to display varying fields and data depending on the context of the incident. The Incident Summary layout serves as an overview of the incident details, making it suitable for dynamic sections which can adapt to showcase different information based on the situation or specific incident configurations. In contrast, other layouts like the "Close" Incident Form, Incident Quick View, and "New/Edit" Incident Form have more defined purposes that typically do not accommodate the flexible nature of Dynamic Sections as effectively. The "Close" form is focused on finalizing incidents rather than displaying variable information, while the Quick View aims for quick access to essential information without the complexity of dynamic data updates. The "New/Edit" form is also structured to standardize the input process, which limits the ability to incorporate dynamically changing data fields.

6. What key benefit does the Cortex XDR platform offer for threat detection?

A. Requires minimal configuration

B. Provides unified visibility across endpoints

C. Only focuses on network traffic analysis

D. Relies solely on user intervention

The Cortex XDR platform offers unified visibility across endpoints, which is a critical benefit for effective threat detection. This unified visibility allows security teams to monitor and analyze data from various sources, including endpoints, networks, and cloud environments, from a single platform. By aggregating and correlating data across these different domains, Cortex XDR enables more comprehensive threat detection and quicker response times. This holistic view helps in identifying complex threats that may not be apparent when analyzing isolated components, leading to a more effective security posture. Other aspects of threat detection, such as relying solely on user intervention or focusing exclusively on network traffic, limit the scope and effectiveness of the security system. Additionally, minimal configuration might seem beneficial, but without a broader context of visibility, it doesn't address the nuances involved in sophisticated threat detection.

7. What is the function of the "Acknowledge" command in the Cortex XSOAR War Room?

A. To close an incident

B. To track the progress of an investigation

C. To officially recognize a task has been reviewed

D. To escalate an issue for higher-level handling

The "Acknowledge" command in the Cortex XSOAR War Room serves the important function of officially recognizing that a task has been reviewed. When users acknowledge a task, it indicates that they have examined the details and are aware of it, which facilitates better collaboration among team members during an incident response. This action helps to ensure that all team members are informed about the progress of investigations and that the tasks at hand are monitored systematically. Acknowledging a task can also prevent confusion regarding who is overseeing particular issues, enhancing accountability within the response team.

8. Cortex XDR can schedule recurring scans of endpoints for malware. Identify two methods for initiating an on-demand malware scan?

A. Response > Action Center

B. The local console

C. Telnet

D. Endpoint > Endpoint Management

Initiating an on-demand malware scan in Cortex XDR can be accomplished in several effective ways, and the choice indicating the Action Center is indeed one of the recognized methods. The Action Center within the Response section serves as a hub where security teams can monitor alerts and manage responses to security incidents, including manually triggering scans. This provides a user-friendly interface where analysts can ensure endpoints are checked for malware when deemed necessary, without waiting for scheduled scans. In addition to using the Action Center, another valid method for initiating on-demand scans is through the local console. This allows for direct interaction with the endpoint, enabling users to execute scans based on real-time requirements—such as when an immediate threat is suspected or after an alert has been raised. While telecommunication protocols like Telnet may be useful for various administrative tasks, they are not designed for initiating malware scans within Cortex XDR. Similarly, the Endpoint Management section focuses more on overseeing the configurations and statuses of endpoints rather than executing on-demand actions. Thus, the methods chosen for initiating scans reflect the appropriate operational capabilities within Cortex XDR designed for security management and incident response.

9. What is the role of cloud computing in PSE Cortex?

A. Providing scalable infrastructure for data storage and processing

B. Enhancing user interface and experience

C. Developing mobile applications for remote access

D. Implementing security protocols for client data

The role of cloud computing in PSE Cortex primarily centers around providing scalable infrastructure for data storage and processing. This is essential for handling large volumes of data efficiently and allows for flexible resource allocation. Businesses can scale their resources up or down based on demand, which is a critical advantage in managing varying workloads and ensuring optimal performance. Cloud computing facilitates the management of big data and complex calculations without the need for substantial local infrastructure. This scalability ensures that PSE Cortex can accommodate growth, manage spikes in traffic, and handle extensive data analytics in real time. Additionally, by leveraging cloud resources, organizations can focus more on their core business activities rather than managing hardware and infrastructure, which optimizes overall efficiency and productivity. The other options address different aspects of technology and development but do not directly capture the fundamental reason why cloud computing is integral to PSE Cortex's capabilities in terms of data management and processing power.

10. Which Cortex XDR capability extends investigations to an endpoint?

A. Log stitching

B. Causality Chain

C. Sensors

D. Live Terminal

The correct answer is "Live Terminal." This capability is essential for extending investigations to an endpoint because it allows security teams to interact with the endpoint in real-time. Through Live Terminal, investigators can run commands, collect data, and perform live forensics directly on the host machine, which is crucial for responding to and understanding potential threats or breaches. The functionality of Live Terminal allows for more in-depth investigation processes, as it provides immediate access to the endpoint's operating environment. This is particularly valuable when analyzing suspicious activities or confirming the presence of malware, as it helps in gathering critical evidence that may not be available through traditional logging or data collection methods. Other capabilities, such as log stitching and causality chain, focus on correlating data and establishing the sequence of events in a broader context, rather than providing direct interaction with the endpoint. Sensors are essential for gathering data and monitoring, but they do not offer the same level of investigatory access as Live Terminal does. Therefore, Live Terminal stands out as the capability that directly facilitates investigations at the endpoint level.

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://psecortexpro.examzify.com

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