# CompTIA Security+ (SY0-601) Certification Practice Test (Sample)

## Study Guide


**Everything you need from our exam experts!**

# 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**

# 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 two technologies are being utilized to allow users to access their desktop and information systems across thin clients with smart cards?**

   **A. COPE and TOTP**

   **B. VDI and RFID**

   **C. GPS and BYOD**

   **D. VDI and COPE**

2. **What can security administrators use to assess system configurations against compliance baselines?**

   **A. SOAR playbook**

   **B. Security control matrix**

   **C. Risk management framework**

   **D. Benchmarks**

3. **In monitoring an industrial system, which mitigation strategy is BEST for alerts while ensuring operational security?**

   **A. Segmentation**

   **B. Firewall whitelisting**

   **C. Containment**

   **D. Isolation**

4. **What term refers to applications and systems used within an organization without consent or approval?**

   **A. Shadow IT**

   **B. OSINT**

   **C. Dark web**

   **D. Insider threats**

5. **Which configuration provides the greatest security benefit for devices used internationally by staff who travel extensively?**

   **A. Configuring an always-on VPN**

   **B. Implementing application whitelisting**

   **C. Requiring web traffic to pass through an on-premises content filter**

   **D. Setting the antivirus DAT update schedule to weekly**

**6. A security analyst is reviewing historical logs for specific activities outlined in a security advisory. What is the analyst doing?**

**A. A packet capture**

**B. User behavior analysis**

**C. Threat hunting**

**D. Credentialed vulnerability scanning**

**7. What is an effective method to prevent data leakage in a company using cloud services?**

**A. Implementing a DLP solution**

**B. Using a firewall only**

**C. Restricting internet access**

**D. Enforcing device controls**

**8. What forensic technique should be used to ensure the admissibility of evidence when authorities are collecting evidence for fraud?**

**A. Order of volatility**

**B. Data recovery**

**C. Chain of custody**

**D. Non-repudiation**

**9. To allow PII to be shared securely without compromising security, which action should be taken regarding DLP policies?**

**A. Allow all PII**

**B. Allow all ports used by the application**

**C. Whitelist the application with specific PII**

**D. Encrypt the PII within the application**

**10. What approach should be taken to ensure secure remote work for employees?**

**A. Implement a personal VPN for all staff**

**B. Require regular software updates only**

**C. Use company-issued devices for work**

**D. Enforce multifactor authentication**

# Answers

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

# Explanations

## 1. Which two technologies are being utilized to allow users to access their desktop and information systems across thin clients with smart cards?

**A. COPE and TOTP**

**B. VDI and RFID**

**C. GPS and BYOD**

**D. VDI and COPE**

**The correct response highlights Virtual Desktop Infrastructure (VDI) and Radio Frequency Identification (RFID) as the technologies that facilitate user access to desktop environments through thin clients paired with smart cards. Virtual Desktop Infrastructure is a vital technology that enables users to access a virtualized desktop environment from various devices, including thin clients. This means that users can connect to their desktop interfaces and applications hosted on a remote server, thus allowing for greater flexibility and mobility while maintaining centralized management of data and applications. Radio Frequency Identification, on the other hand, is a technology used for authentication. When integrated with smart cards, RFID provides a secure method for users to authenticate themselves and gain access to the virtual desktops. Smart cards can store user credentials and, when paired with RFID readers, enable easy and secure access to systems without the need for manual password entry. The other options involve technologies that do not specifically pertain to the combination of accessing desktop environments through thin clients and smart cards. For example, COPE (Corporate Owned, Personally Enabled) relates to device management policies rather than direct access technologies, while TOTP (Time-based One-Time Password) focuses on a mechanism for generating one-time passcodes for authentication, not the infrastructure for desktop access. Similarly, GPS (Global Positioning**

## 2. What can security administrators use to assess system configurations against compliance baselines?

**A. SOAR playbook**

**B. Security control matrix**

**C. Risk management framework**

**D. Benchmarks**

**Security administrators can use benchmarks to assess system configurations against compliance baselines because benchmarks provide standards or best practices for security configurations established by reputable organizations. These benchmarks serve as reference points to determine whether the current system configurations adhere to required security policies and compliance regulations. By comparing the actual settings and configurations of a system with the established benchmarks, administrators can identify any discrepancies or areas that need improvement to meet compliance standards. This process helps ensure the system maintains a robust security posture in alignment with industry standards. The other choices serve different purposes within the security domain. For example, a SOAR playbook is focused on orchestrating and automating security operations responses, while a security control matrix outlines the controls implemented and their effectiveness. The risk management framework provides a structured approach to managing risk but does not directly assess compliance against configurations.**

## 3. In monitoring an industrial system, which mitigation strategy is BEST for alerts while ensuring operational security?

**A. Segmentation**

**B. Firewall whitelisting**

**C. Containment**

**D. Isolation**

**Segmentation is the best choice for monitoring an industrial system while maintaining operational security. This approach involves separating different parts of the network or system, which helps to limit the exposure of critical components to potential threats. By segmenting the network, you can create distinct environments for various functions or processes, allowing for more refined monitoring and alerting mechanisms. When segmentation is employed, alerts can be finely tuned to specific segments, ensuring that any anomalous activity can be quickly identified and addressed without compromising the overall security posture of the entire system. This tailored monitoring improves the visibility of potential security incidents, enabling faster response times while safeguarding operational processes. Other strategies like firewall whitelisting, containment, and isolation also have their merits in securing systems. Whitelisting focuses on allowing only trusted entities access, which is effective but may not provide the granularity needed for monitoring alerts. Containment generally addresses how to manage security incidents after they occur but does not inherently improve alert mechanisms. Isolation can create an environment where certain parts of the system are cut off to prevent further risk, but it can also lead to challenges in monitoring and operational efficiency. Thus, segmentation stands out as the most effective strategy for both alerting and maintaining operational security in an industrial setting.**

## 4. What term refers to applications and systems used within an organization without consent or approval?

**A. Shadow IT**

**B. OSINT**

**C. Dark web**

**D. Insider threats**

**The term that refers to applications and systems used within an organization without consent or approval is known as Shadow IT. This practice occurs when employees or departments adopt technology solutions independently, often for convenience or to meet specific needs, bypassing the organization's formal IT governance. Shadow IT can introduce various risks, such as data breaches, compliance violations, and potential security vulnerabilities, as these unauthorized applications may not adhere to the organization’s security protocols or undergo necessary vetting. Understanding Shadow IT is critical for organizations to manage their security posture effectively. While attempts may be made by IT departments to control and regulate technology use, the prevalence of Shadow IT can challenge these efforts, making it essential for organizations to promote awareness and establish guidelines that allow employees to use approved technologies safely.**

## 5. Which configuration provides the greatest security benefit for devices used internationally by staff who travel extensively?

**A. Configuring an always-on VPN**

**B. Implementing application whitelisting**

**C. Requiring web traffic to pass through an on-premises content filter**

**D. Setting the antivirus DAT update schedule to weekly**

**Configuring an always-on VPN provides the greatest security benefit for devices used internationally by staff who travel extensively because it ensures that all data transmitted from the device is encrypted and routed through a secure tunnel to a trusted network. This is crucial for remote workers who may connect to public or unsecured networks while traveling, which are often targets for cyberattacks. By using an always-on VPN, employees can protect sensitive information from eavesdropping and man-in-the-middle attacks, as their data is encrypted end-to-end. It also helps maintain privacy and security by masking the user's IP address. This consistent level of security is particularly important for international travel, where the risk of data interception is heightened. In contrast, while implementing application whitelisting helps control which applications may run on a device, it does not specifically address the security challenges posed by traveling and using various networks. Requiring web traffic to pass through an on-premises content filter can provide some level of security, but it may not be practical or effective for employees accessing the internet from different locations globally. Lastly, setting the antivirus DAT update schedule to weekly, while important for maintaining updated protection against known threats, does not provide real-time security or encryption, making it less effective for securing devices in transit**

## 6. A security analyst is reviewing historical logs for specific activities outlined in a security advisory. What is the analyst doing?

**A. A packet capture**

**B. User behavior analysis**

**C. Threat hunting**

**D. Credentialed vulnerability scanning**

**The activity described involves reviewing historical logs to identify specific activities that are related to a particular security advisory, which indicates an active investigation into potential security threats or indicators of compromise. This process corresponds with threat hunting. Threat hunting involves proactively searching through networks and sets of data to identify and mitigate threats that may evade existing security measures. By analyzing historical logs, the security analyst can uncover patterns, anomalies, or malicious behavior that corresponds to the advisories, thereby enhancing the organization's security posture. In contrast, packet capture refers to the process of collecting network packets to analyze traffic, while user behavior analysis focuses on understanding and analyzing user activities for unusual behaviors. Credentialed vulnerability scanning involves checking systems for vulnerabilities but does not include the proactive searching associated with threat hunting. Thus, threat hunting is the most appropriate term for the activity of reviewing historical logs in this context.**

## 7. What is an effective method to prevent data leakage in a company using cloud services?

**A. Implementing a DLP solution**

**B. Using a firewall only**

**C. Restricting internet access**

**D. Enforcing device controls**

**Implementing a Data Loss Prevention (DLP) solution is a proactive approach to preventing data leakage in organizations that utilize cloud services. DLP solutions are designed to monitor and control the movement of sensitive data across networks, endpoints, and cloud environments. They help organizations to identify, classify, and protect confidential information by enforcing policies that restrict data sharing and transmission based on predefined security criteria. DLP solutions typically include features such as content inspection, encryption, and user alerts, which work together to ensure that sensitive data is not shared inappropriately—whether via email, cloud storage, or other means. This capability is especially critical in cloud environments, where the risk of accidental or malicious data exposure can be higher due to accessibility and shared user resources. While other methods like using a firewall, restricting internet access, and enforcing device controls can contribute to overall security, they may not directly address the specific issue of preventing data leakage. For instance, firewalls primarily focus on managing incoming and outgoing network traffic based on security rules, but they do not typically monitor data content. Restricting internet access can limit exposure but may hinder legitimate business operations. Enforcing device controls is essential for endpoint security but may not control data once it leaves the organization's environment. Thus, a**

## 8. What forensic technique should be used to ensure the admissibility of evidence when authorities are collecting evidence for fraud?

**A. Order of volatility**

**B. Data recovery**

**C. Chain of custody**

**D. Non-repudiation**

**The correct answer emphasizes the importance of maintaining the chain of custody when collecting evidence for fraud cases. Chain of custody refers to the process of handling and documenting evidence from the moment it is collected until it is presented in a court of law. This procedure is critical because it establishes the integrity and authenticity of the evidence, ensuring that it has not been altered, tampered with, or contaminated during the investigation. In legal contexts, evidence must be demonstrably reliable to be considered admissible. By maintaining a clear and thorough chain of custody, investigators can provide a reliable record of who handled the evidence, when it was handled, and the conditions under which it was stored. This documentation is essential for proving the evidence's integrity in court and for bolstering the prosecution's case against an individual accused of fraud. While the other options have their own significance in the realm of digital forensics and security, they don't directly address the requirements for evidence admissibility in a courtroom setting. For instance, order of volatility relates to the sequence in which evidence should be collected based on its volatility, and data recovery addresses retrieving lost or deleted data. Non-repudiation refers to assuring that someone cannot deny the validity of their signature or the sending of a message, which is**

## 9. To allow PII to be shared securely without compromising security, which action should be taken regarding DLP policies?

**A. Allow all PII**

**B. Allow all ports used by the application**

**C. Whitelist the application with specific PII**

**D. Encrypt the PII within the application**

**Whitelisting the application with specific PII is a strategic approach to adhering to data loss prevention (DLP) policies while maintaining security effectively. This action involves explicitly permitting certain applications to handle personally identifiable information (PII) under controlled conditions. By specifying which applications are allowed to process and share PII, organizations can mitigate the risk of unauthorized access and ensure that only trusted processes interact with sensitive data. This method also enables organizations to maintain oversight and control over how PII is used, potentially incorporating other security measures such as encryption or monitoring within the whitelisted applications. This provides a layered security approach to managing sensitive information, ensuring compliance with relevant regulations and decreasing the likelihood of data breaches. In contrast, allowing all PII or all ports used by the application could lead to significant vulnerabilities, as it does not restrict access or usage and could expose sensitive data to unauthorized entities. Encrypting PII within the application is a good security practice, but it does not inherently control which applications can access or share the data, nor does it limit the scope of potential exposure. Therefore, whitelisting offers a more tailored and responsible approach to managing and sharing PII securely.**

## 10. What approach should be taken to ensure secure remote work for employees?

**A. Implement a personal VPN for all staff**

**B. Require regular software updates only**

**C. Use company-issued devices for work**

**D. Enforce multifactor authentication**

**Using multifactor authentication (MFA) is a critical approach to ensuring secure remote work for employees. MFA adds an extra layer of security by requiring not just a password but also another form of verification, such as a text message code, biometric recognition, or an authenticator app. This means that even if a password is compromised, unauthorized access to sensitive information or company resources is mitigated by the need for an additional factor of authentication. This significantly reduces the risk of account breaches, especially in remote work scenarios where employees may access company resources from various locations and devices. The other options, while they can be part of a comprehensive security strategy, do not provide the same level of immediate security against unauthorized access. Implementing a personal VPN enhances privacy and helps secure the internet connection, but it does not directly protect against credential theft. Requiring regular software updates is important for keeping systems secure, but it addresses vulnerabilities rather than access control. Utilizing company-issued devices helps manage and secure endpoints, but if unauthorized access can occur on those devices, the risk remains. MFA brings a proactive measure to protect sensitive information significantly better than these other methods alone.**

# 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://comptiasecplussy0601.examzify.com**

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