CompTIA Security+ SYO 701 Practice Test

Section: CompTIA Security Plus Certification Exams • **Total Questions:** 10 • **Format:** Verified Q&A

1. Which of the following is the most likely benefit of conducting an internal audit?

(A) Findings are reported to shareholders.
(B) Reports are not formal and can be reassigned.
(C) Control gaps are identified for remediation.
(D) The need for external audits is eliminated.

2. Which of the following would enable a data center to remain operational through a multiday power outage?

(A) Generator
(B) Uninterruptible power supply
(C) Replication
(D) Parallel processing

3. A security analyst is evaluating a SaaS application that the human resources department would like to implement. The analyst requests a SOC 2 report from the SaaS vendor. Which of the following processes is the analyst most likely conducting?

(A) Internal audit
(B) Penetration testing
(C) Attestation
(D) Due diligence

4. Which of the following best explains a concern with OS-based vulnerabilities?

(A) An exploit would give an attacker access to system functions that span multiple applications.
(B) The OS vendor's patch cycle is not frequent enough to mitigate the large number of threats.
(C) Most users trust the core operating system features and may not notice if the system has been compromised.
(D) Exploitation of an operating system vulnerability is typically easier than any other vulnerability.

5. Which of the following is a benefit of vendor diversity?

(A) Patch availability
(B) Zero-day resiliency
(C) Secure configuration guide applicability
(D) Load balancing

---

6. The Chief Information Security Officer (CISO) has determined the company is non-compliant with local data privacy regulations. The CISO needs to justify the budget request for more resources. Which of the following should the CISO present to the board as the direct consequence of non-compliance?

(A) Fines
(B) Reputational damage
(C) Sanctions
(D) Contractual implications

---

7. Which of the following would best prepare a security team for a specific incident response scenario?

(A) Situational awareness
(B) Risk assessment
(C) Root cause analysis
(D) Tabletop exercise

---

8. Which of the following is a benefit of launching a bug bounty program? (Select two).

(A) Transference of risk to a third party
(B) Reduction in the number of zero-day vulnerabilities
(C) Increased security awareness for the workforce
(D) Reduced cost of managing the program
(E) Quicker discovery of vulnerabilities
(F) Improved patch management process

---

9. Which of the following mitigation techniques would a security analyst most likely use to avoid bloatware on devices?

(A) Disabled ports/protocols
(B) Application allow list
(C) Default password changes
(D) Access control permissions

---

10. A systems administrator configures a new application. The next day, a security analyst reviews the logs and identifies multiple accounts that had been created overnight with administrative privileges and connections from different countries. Which of the following solutions would have prevented this incident?

(A) Applying input validation

(B) Changing the default credentials

(C) Installing a honeynet

(D) Deploying a WAF