# CompTIA Security Plus 501 Practice Questions

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

**1. A Chief Information Security Officer (CISO) determines that a major security incident will cost the company $500,000. The CISO purchases insurance to pay $400,000 of this projected cost. Which of the following risk management strategies has the CISO adopted?**

**(A)** Acceptance
**(B)** Mitigation
**(C)** Avoidance
**(D)** Transference

**2. Which of the following threat actors would most likely deface the website of a high-profile music group?**

**(A)** Unskilled attacker
**(B)** Organized crime
**(C)** Nation-state
**(D)** Insider threat

**3. During an investigation, a security analyst discovers traffic going out to a command-and-control server. The analyst must find out if any data exfiltration has occurred. Which of the following would best help the analyst determine this?**

**(A)** Application log
**(B)** Metadata
**(C)** Network log
**(D)** Packet capture

**4. Which of the following is the best way to remove personal data from a social media account that is no longer being used?**

**(A)** Exercise the right to be forgotten
**(B)** Uninstall the social media application
**(C)** Perform a factory reset
**(D)** Terminate the social media account

**5. A company's antivirus solution is effective in blocking malware but often has false positives. The security team has spent a significant amount of time on investigations but cannot determine a root cause. The company is looking for a heuristic solution. Which of the following should replace the antivirus solution?**

**(A)** SIEM
**(B)** EDR
**(C)** DLP
**(D)** IDS

---

**6. Which of the following agreements defines response time, escalation points, and performance metrics?**

**(A)** BPA
**(B)** MOA
**(C)** NDA
**(D)** SLA

---

**7. Which of the following describes effective change management procedures?**

**(A)** Approving the change after a successful deployment
**(B)** Having a backout plan when a patch fails
**(C)** Using a spreadsheet for tracking changes
**(D)** Using an automatic change control bypass for security updates

---

**8. The security team notices that the Always On VPN solution sometimes fails to connect. This leaves remote users unprotected because they cannot connect to the on-premises web proxy. Which of the following changes will best provide web protection in this scenario?**

**(A)** Implement network access control.
**(B)** Configure the local gateway to point to the VPN.
**(C)** Create a public NAT to the on-premises proxy.
**(D)** Install a host-based content filtering solution.

---

**9. While reviewing a recent compromise a forensics team discovers that there are hard-coded credentials in the database connection strings. Which of the following assessment types should be performed during software development to prevent this from reoccurring?**

**(A)** Vulnerability scan
**(B)** Penetration test
**(C)** Static analysis
**(D)** Quality assurance

---

**10. While troubleshooting a firewall configuration, a technician determines that a 'deny any' policy should be added to the bottom of the ACL. The technician updates the policy, but the new policy causes several company servers to become unreachable. Which of the following actions would prevent this issue?**

**(A)** Documenting the new policy in a change request and submitting the request to change management

**(B)** Testing the policy in a non-production environment before enabling the policy in the production network

**(C)** Disabling any intrusion prevention signatures on the 'deny any' policy prior to enabling the new policy

**(D)** Including an 'allow any' policy above the 'deny any' policy