CompTIA Security Plus Simulation Questions

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

1. A company is concerned with supply chain compromise of new servers and wants to limit this risk. Which of the following should the company review first?

(A) Sanitization procedure
(B) Acquisition process
(C) Change management
(D) Asset tracking

2. Which of the following receives logs from various devices and services, and then presents alerts?

(A) SIEM
(B) SCADA
(C) SNMP
(D) SCAP

3. After a company was compromised, customers initiated a lawsuit. The company's attorneys have requested that the security team initiate a legal hold in response to the lawsuit. Which of the following describes the action the security team will most likely be required to take?

(A) Retain the emails between the security team and affected customers for 30 days.
(B) Retain any communications related to the security breach until further notice.
(C) Retain any communications between security members during the breach response.
(D) Retain all emails from the company to affected customers for an indefinite period of time.

4. An organization wants to deploy software in a container environment to increase security. Which of the following will limit the organization's ability to achieve this goal?

(A) Regulatory compliance
(B) Patch availability
(C) Kernel version
(D) Monolithic code

5. Which of the following vulnerabilities would likely be mitigated by setting up an MDM platform?

(A) TPM
(B) Buffer overflow
(C) Jailbreaking
(D) SQL injection

---

6. Which of the following vulnerabilities would a nation-state attacker most likely exploit?

(A) Zero-day
(B) SQL Injection
(C) Buffer overflow
(D) Cross-site scripting

---

7. Which of the following is the best reason to perform a tabletop exercise?

(A) To address audit findings
(B) To collect remediation response ×
(C) To update the IRP
(D) To calculate the ROI

---

8. A security manager needs an automated solution that will take immediate action to protect an organization against inbound malicious traffic. Which of the following is the best solution?

(A) UEM
(B) IPS
(C) WAF
(D) VPN

---

9. An employee from the accounting department logs in to the website used for processing the company's payments. After logging in, a new desktop application automatically downloads on the employee's computer and causes the computer to restart. Which of the following attacks has occurred?

(A) XSS
(B) Watering hole
(C) Typosquatting
(D) Buffer overflow

---

10. A security engineer must create detections for file staging techniques on web-facing servers. The company implements multiple tools and is most concerned about intellectual property theft. Which of the following tools does the company most likely use?

(A) EDR for indicator detections based on process names

(B) DLP for scanning and identification on endpoints

(C) SOAR for web crawling plugins and data validation

(D) IPS for cleartext traffic inspection of network payloads