Security Operations

CompTIA Security+ certification exam, SY0-801 (V8)

27% of the exam · 8 exam objectives · SY0-801

Security Operations is the largest domain at 27% of the exam. It covers the daily work of keeping an environment secure: choosing and applying controls, managing assets and vulnerabilities, monitoring and alerting, identity and access management, automation, incident response and the data used in investigations. Most objectives are scenario based, so practise picking the control or step that fits a described situation.

You should be able to: A laptop infected with ransomware is still connected to the network. Which incident response activity comes next, and what does it involve?

Every exam objective: the key point and the trap

4.1 Given a scenario, apply mitigating controls, techniques, and solutions to secure the environment.

Segmentation, access controls, hardening and sandboxing reduce what an attacker can reach and do; deception technology (honeypot, honeynet, honeyfile, honeytoken, canary account) places decoys that alert when touched.

Trap: Choosing a Layer 4 firewall rule for an application attack, or confusing detection (IDS) with prevention (IPS). Also mixing up SPF, DKIM and DMARC: only DMARC tells receivers what to do with failing mail.

4.2 Explain the security implications of proper hardware, software, and data asset management.

The asset management life cycle runs from planning and scoping, through acquisition and procurement, assignment and accounting, and monitoring and asset tracking, to disposal and decommissioning.

Trap: Treating asset management as a one-time inventory. Most failures happen after purchase: no owner recorded, no tracking, or drives sold without sanitization.

4.3 Given a scenario, perform tasks associated with vulnerability management.

Identification methods: vulnerability scanning, IPAM to know every address range to scan, CSPM for cloud misconfigurations and source code review for code flaws.

Trap: Closing a ticket as soon as a patch is installed, without verification. Also confusing a responsible disclosure policy (a reporting process) with a bug bounty (a reporting process with rewards).

4.4 Explain security alerting and monitoring concepts and tools.

Monitoring covers systems, applications and infrastructure.

Trap: Picking full packet capture when flow data (NetFlow) is enough, or SNMP when the need is log correlation (SIEM).

4.5 Given a scenario, apply concepts related to identity and access management.

Provision accounts with the access needed and deprovision promptly when the need ends; review permissions regularly (access review) to catch permission creep.

Trap: Mixing up SAML and OAuth (authentication assertions versus delegated authorization), and mandatory versus discretionary (who decides: the system or the owner).

4.6 Given a scenario, apply automation and orchestration solutions to secure operations.

Use cases for automation and scripting: user provisioning, resource provisioning, desired state management, anomaly detection and ticket management.

Trap: Assuming more automation is always better. Complexity, cost and process risks are real considerations, and automation without guardrails can cause an outage.

4.7 Summarize concepts associated with incident response activities.

Preparation: training, testing, tabletop exercises (discussion), simulations (realistic practice), playbooks and defined roles.

Trap: Calling reimaging containment (it is eradication and recovery), or calling a tabletop exercise a simulation (a tabletop is discussion only).

4.8 Given a scenario, use data, artifacts and sources to support a security investigation.

Log and trace data types: access and accounting (logical and physical), device, server, application, authentication, communication, audit, endpoint, network and metadata.

Trap: Shutting a system down before capturing memory, or relying on file dates instead of hashes to prove logs were not changed.

Key terms

SIEM: Security Information and Event Management

EDR: Endpoint Detection and Response

XDR: Extended Detection and Response

DMARC: Domain-based Message Authentication, Reporting, and Conformance

CSPM: Cloud Security Posture Management

SCAP: Security Content Automation Protocol

SAML: Security Assertions Markup Language

SOAR: Security Orchestration, Automation, and Response

IPFIX: Internet Protocol Flow Information Export

PIR: Post-incident Reporting

ExamDragon, examdragon.com/secplus. Independent exam preparation, not affiliated with or endorsed by CompTIA; written in our own words to the SY0-801 exam objectives. CompTIA and Security+ are trademarks of CompTIA, Inc.