CYSA+ STUDY SHEET · DOMAIN 1.0

Security Operations

CompTIA Cybersecurity Analyst (CySA+) certification exam, CS0-004

34% of the exam · 6 exam objectives · CS0-004

Security Operations is the daily work of a security operations center: understanding the systems, networks, identities and data it defends and the logs they produce (1.1), spotting indicators of malicious activity on networks, hosts, applications, cloud services, identities and email (1.2), and using tools from packet analyzers and SIEM to sandboxes and threat-intelligence platforms to confirm it (1.3). It then looks outward and forward: threat intelligence and threat hunting built on actors, TTPs, IoCs and threat modeling (1.4), efficient and standardized operations through playbooks, automation, enrichment and tool integration (1.5), and the safe use of AI, weighing its risks, governance and use cases (1.6).

You should be able to: A SIEM alert shows a workstation where Word started PowerShell, which then connected out every 60 seconds to a newly registered domain. Name one tool to confirm what the script does, say whether the beaconing is an atomic or a behavioral indicator, and give one control that keeps an AI assistant used in the investigation from leaking data or misleading the analyst.

Every exam objective: the key point and the trap

1.1 Explain concepts related to system and network architecture in security operations.

Logging concepts: ingestion brings events from every source into a central store such as a SIEM, parsed into common fields; configuration decides what each source records; integrity keeps logs from being changed, by sending them off the host promptly, protecting the store and hashing; time synchronization, usually NTP to one source, lets events from many devices line up; retention keeps logs as long as legal, regulatory and investigative needs require.

Trap: Treating containers like virtual machines. Containers share the host kernel, so a host kernel flaw or an over-privileged container can affect every container on that host.

1.2 Given a scenario, analyze indicators of potential malicious activity.

Network-related indicators: rogue devices are unauthorized hardware such as unknown MAC addresses or unlisted access points; enumeration is scanning hosts, ports, shares or directory objects; anomalous activity is traffic far from the baseline; activity on unexpected ports, such as a web server calling out on an odd port, often means a backdoor or command and control.

Trap: Calling built-in tools such as certutil or PowerShell unauthorized software. They ship with the operating system; the indicator is the unusual way they are used, which is living off the land.

1.3 Given a scenario, use tools to determine malicious activity.

Decoding and parsing: CyberChef chains operations such as Base64, hexadecimal, gzip and XOR into a recipe to reveal obfuscated text from scripts, logs and emails.

Trap: Uploading a sensitive or targeted sample to a public service such as VirusTotal. An upload can be seen by others, including the attacker; look up the hash first.

1.4 Explain threat intelligence and threat-hunting concepts.

Threat actors: an advanced persistent threat (APT) is a well-resourced actor, often state-sponsored, that keeps stealthy long-term access to reach a strategic goal such as espionage. An insider threat is a current or former employee, contractor or partner who misuses legitimate access, on purpose or by accident.

Trap: Treating a list of IP addresses or hashes as the strongest intelligence. They sit at the bottom of the Pyramid of Pain and lose value fast; TTPs are the hardest for an adversary to change.

1.5 Explain the importance of efficiency and process improvement in security operations.

Standardizing processes makes the SOC consistent: playbooks document the standard response to a type of incident, with its steps, decision points and roles, and runbooks give the detailed steps for a specific task. Both help team coordination, training and shift handovers.

Trap: Disabling a noisy rule, or hiding its alerts on a dashboard, instead of tuning it. Disabling loses the detection, and hiding leaves the noise in the queue.

1.6 Summarize concepts related to the use of AI in security operations.

Hallucinations: generative AI can state invented facts, such as a CVE number or a log entry that does not exist, with full confidence. Every claim that drives a decision is checked against the original data or an authoritative source.

Trap: Confusing model poisoning with malicious prompts. Poisoning changes what the model learned during training; a malicious prompt manipulates it through input while it runs.

Key terms

SIEM: Security Information and Event Management

SOAR: Security Orchestration, Automation, and Response

EDR: Endpoint Detection and Response

XDR: Extended Detection and Response

ZTNA: Zero Trust Network Access

APT: Advanced Persistent Threat

TTPs: Tactics, Techniques, and Procedures

IoC: Indicator of Compromise

OSINT: Open-Source Intelligence

STRIDE: Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, and Elevation of privilege

ExamDragon, examdragon.com/cysaplus. Independent exam preparation, written in our own words to the CS0-004 exam objectives. CompTIA and CySA+ are trademarks of CompTIA, Inc.