CYSA+ STUDY SHEET · DOMAIN 3.0

Incident Response and Management

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

24% of the exam · 3 exam objectives · CS0-004

Incident Response and Management is how an analyst understands and handles an attack: describing it with the Cyber Kill Chain, the Diamond Model and MITRE ATT&CK, following the incident response process from preparation to post-incident review, and applying the techniques that make a response work, from plans, playbooks and exercises to log analysis, triage, evidence handling, isolation, restoration and root cause analysis.

You should be able to: Malware is beaconing from a workstation and the company expects legal action. Which Cyber Kill Chain phase is the beaconing, what should the team do to contain it while keeping evidence, and what proves later that the disk image is unchanged?

Every exam objective: the key point and the trap

3.1 Summarize concepts related to attack methodology frameworks.

Attack methodology frameworks give analysts a shared way to describe, detect and disrupt intrusions. The three to know are the Cyber Kill Chain, the Diamond Model of Intrusion Analysis and MITRE ATT&CK.

Trap: Mixing the frameworks' vocabulary: Weaponization is a kill chain phase, not an ATT&CK tactic, and Phishing is an ATT&CK technique, not a tactic. In ATT&CK, the tactic is always the goal.

3.2 Summarize the incident response process.

The incident response process runs in this order: Preparation, Detection, Analysis, Containment, Eradication, Recovery and Post-incident. Lessons from the last phase feed back into preparation.

Trap: Jumping from detection straight to reimaging. Restoring before containment and eradication destroys evidence and, if the cause is still present, lets the attacker straight back in.

3.3 Given a scenario, implement incident response techniques.

Plans and preparation: the incident response plan sets authority, roles, phases and reporting; the communication plan sets who tells whom, when and through which channels, including approved media spokespeople. Playbooks give step-by-step handling for one incident type, and defined roles say who leads, investigates, communicates and approves.

Trap: Treating a write blocker or a chain of custody form as proof that the data is unchanged. Matching hashes are what prove integrity; the other controls prevent change and document handling.

Key terms

CSIRT: Cybersecurity Incident Response Team

CERT: Computer Emergency Response Team

TTPs: Tactics, Techniques, and Procedures

IoC: Indicator of Compromise

APT: Advanced Persistent Threat

SIEM: Security Information and Event Management

SOAR: Security Orchestration, Automation, and Response

EDR: Endpoint Detection and Response

GeoIP: Geolocation by IP

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.