Reporting and Communication

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

16% of the exam · 2 exam objectives · CS0-004

Reporting and Communication is how analysts turn security work into decisions and action: vulnerability reports, scorecards and action plans matched to their readers, the inhibitors that delay fixes and the metrics that track them, and, for incidents, declaration and escalation, communication plans, post-incident reporting, handovers and the SOC's key performance indicators.

You should be able to: A critical patch cannot be applied because it needs an outage on a system that runs all day, and the same week a confirmed intrusion reaches the corporate email system. Which inhibitor is delaying the patch, and how should the incident team communicate?

Every exam objective: the key point and the trap

4.1 Explain the importance of vulnerability management reporting and communication.

Vulnerability scan reports are the detailed, technical view: each host, the vulnerability identifier, its severity such as a CVSS base score, the evidence and the fix. They are written for the administrators and developers who remediate.

Trap: Sending the detailed scan report to executives, or a risk scorecard to administrators. Match the report to its reader: technical detail for those who fix, business-level ratings and trends for those who decide.

4.2 Explain the importance of security operations and incident response reporting and communication.

Incident declaration and escalation: when an event meets the incident response plan's criteria, it is formally declared an incident and escalated to the people the plan names, so the response has an owner and the authority to act.

Trap: Mixing up the time metrics. Mean time to detect ends at detection; mean time to respond starts there and ends when the response begins (some organizations measure it to containment; either way it ends before remediation); mean time to remediate ends only when the underlying weakness is fixed.

Key terms

KPI: Key Performance Indicator

SLA: Service-level Agreement

SLO: Service-level Objective

CVSS: Common Vulnerability Scoring System

CSIRT: Cybersecurity Incident Response Team

PII: Personally Identifiable Information

PCI DSS: Payment Card Industry Data Security Standard

SIEM: Security Information and Event Management

SOAR: Security Orchestration, Automation, and Response

TTPs: Tactics, Techniques, and Procedures

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.