Cybersecurity Operations Management – Cheat Sheet

01. SecOps Overview

- Manages network, infrastructure, data & user security - Protection at rest, in transit, in use - Key models: 3LD (Controls, Risk & Audit) - Frameworks: ISO, NIST, TOGAF, MITRE - Security Architecture + Operating Model - Course setup: lectures, labs, Moodle, CompTIA

02. Cyber Functions

- Core Areas: Network, Application, Data, User, Cloud - TVM, Monitoring, IR, IAM, Governance - RACI: Responsible, Accountable, Consulted, Informed - All functions have audit, SIEM, vendor, and governance integration

03. Core Functions

- Strategy & Architecture alignment - Security Engineering: hardening, firewall, EDR, DLP, PKI - Org chart: CISO, Ops Lead, Monitoring, IR, IAM, Strategy - Challenges: Tech change, evolving threats, regulation

04. Operational Monitoring

- SIEM, alert triage (3 analyst levels) - Use Case Lifecycle: ID > Create > Tune > Report - Maturity: from basic alerts to automated threat hunting - Frameworks: NIST (Detect), ISO A12/A16, MITRE mappings

05. TVM (Vulnerability Management)

- Scan, Qualify, Remediate, Report - Standards define schedule, classification, testing - Compliance dashboards, vendor intel, threat hunting - Maturity: from perimeter scanning to full lifecycle integration

06. IAM (Identity & Access Management)

- General, Privileged, Service Accounts - JML Process (Joiner, Mover, Leaver) - IAM = EIAM, CIAM, PAM - Federation, MFA, recertification, automation - Aligns to ISO A9, NIST Protect, MITRE (Priv Escalation)

07. Threat Management

- 4 Pillars: Threat Intel, Threat Modelling, Threat Hunting, Advanced Threat Mgt - Modelling: STRIDE, Attack Trees, Kill Chain - Hunting: Structured, Unstructured, Situational - Tools: SIEM, XDR, Honeypots - Frameworks: NIST ID/DE/RS, ISO A12/A14/A16, MITRE ATT&CK