

Introduction to Security Operations and Management

Introduction to Security Operations and Management
Key concepts, roles, processes, and best-practice frameworks

1. What Is Security Operations (SecOps)?

Aspect	Description
Purpose	Detect, analyze, respond to, and mitigate security threats in real time.
Scope	Network traffic, endpoints, cloud services, applications, and physical assets.
Outcome	Maintain confidentiality, integrity, and availability (CIA) of organizational assets while minimizing risk exposure.
Core Activities	Monitoring, threat hunting, incident response, vulnerability management, and security automation.

2. Security Operations Center (SOC)

Component	Function
People	Analysts (Tier1–3), engineers, threat hunters, incident responders, SOC manager.
Process	Standard Operating Procedures (SOPs), playbooks, escalation matrices, post-incident reviews.
Technology	SIEM, EDR/XDR, IDS/IPS, threat intelligence platforms, SOAR, log collectors, dashboards.
Metrics	MTTR (Mean Time to Respond), MTTA (Mean Time to Acknowledge), false-positive rate, detection coverage.

Typical SOC Tier Structure

Tier	Role	Main Tasks
Tier1	Alert triage	Validate alerts, gather context, assign severity, forward to Tier2.
Tier2	Investigation	Deep dive on alerts, perform forensic analysis, determine root cause.

Introduction to Security Operations and Management

Tier	Role	Main Tasks
Tier 3	Incident response & remediation	Investigate, analyze, contain, eradicate, recover; develop and refine detection rules.

3. Security Management Fundamentals

1. Risk Management

- Identify assets ? assess threats & vulnerabilities ? calculate risk (impact × likelihood).
- Prioritize mitigation based on risk appetite.

2. Policy & Governance

- Develop security policies, standards, and procedures aligned with regulations (e.g., GDPR, HIPAA, PCI?DSS).
- Enforce through controls, audits, and continuous improvement.

3. Compliance & Auditing

- Map controls to frameworks (NIST CSF, ISO?27001, CIS Controls).
- Conduct internal/external audits, track remediation.

4. Asset Management

- Maintain an up-to-date inventory of hardware, software, cloud resources, and data flows.
- Tag assets for criticality and apply appropriate security baselines.

5. Change & Configuration Management

- Use CMDB and change-control processes to avoid unintended security gaps.
 - Automate baseline configuration checks (e.g., CIS Benchmarks).
-

4. Core Security Operations Processes

4.1 Monitoring & Detection

Introduction to Security Operations and Management

- **Log Collection** – Centralize logs from firewalls, servers, applications, cloud services.
- **SIEM Correlation** – Apply rule sets, statistical models, and user behavior analytics (UEBA).
- **Threat Intelligence Integration** – Enrich alerts with IOCs, TTPs, and reputation data.

4.2 Threat Hunting

- **Hypothesis-Driven** – Form a hypothesis (e.g., “Lateral movement via SMB”) and test with data queries.
- **Tools** – Elastic Stack, Splunk, Carbon Black, custom scripts.
- **Outcome** – Discover hidden threats, improve detection rules, and update threat models.

4.3 Incident Response (IR)

1. **Preparation** – Playbooks, communication plans, forensics kits.