SOC Concepts – Beginner Friendly Guide

Designed for SOC Analysts, Interviews, and Real-World Understanding

1. Alert vs Incident

Alert
An alert is a notification generated by a security tool (SIEM, EDR, IDS, Firewall, Cloud logs) indicating that something suspicious might be happening. Alerts are not confirmed threats.

Examples of Alerts:

- Multiple failed login attempts from one IP
- Malware hash detected but not executed
- Login from a new country

Incident
An incident is a confirmed security event that has impact or potential impact on the organization. An incident always starts as an alert but is validated through investigation.

Examples of Incidents:

- Failed logins followed by a successful login
- Malware executed on endpoint
- Phishing email where user clicked and entered credentials

2. False Positive vs True Positive

False Positive
A false positive occurs when an alert is triggered but there is no actual security threat. These are common and expected in SOC environments.

- User traveling and logging in from another country
- Admin running PowerShell scripts
- Vulnerability scanner triggering IDS alerts

True Positive
A true positive means the alert represents real malicious activity and requires action.

- Password spray attack with successful login
- Malware communicating with command-and-control server
- MFA fatigue attack accepted by user

3. Severity Levels in SOC

- **Low**: Informational, no impact (example: single failed login). Action: document and close.
- **Medium**: Suspicious activity (example: multiple failed logins). Action: investigate.
- **High**: Confirmed threat with limited impact (example: malware quarantined). Action: escalate.
- **Critical**: Active breach (example: ransomware, data exfiltration). Action: immediate response.

4. SOC Analyst Responsibilities

Tier 1 SOC Analyst

- Monitor security alerts
- Triage alerts and identify false positives
- Validate incidents and escalate when required
- Document findings clearly

Tier 2 SOC Analyst

- Deep investigation and correlation
- Malware and phishing analysis
- Threat hunting and detection improvement

Tier 3 / Incident Response

- Containment and remediation
- Forensics and root cause analysis
- Post-incident lessons learned

Interview Quick Tips

- Alert is potential, incident is confirmed.
- Severity is based on impact, not number of alerts.
- SOC goal is fast detection and accurate response.