Security Operations Center Alert Handling

Alert Triage

SOC monitors security alerts 24/7. Alerts triaged by severity: Critical (immediate threat), High (potential threat), Medium (suspicious), Low (informational).

Triage within: Critical - 15 minutes, High - 1 hour, Medium - 4 hours, Low - next business day.

Alert Sources

Alerts from: SIEM, IDS/IPS, endpoint protection, firewall, email security, cloud security, threat intelligence feeds.

Automated correlation reduces false positives. Machine learning identifies anomalous patterns.

Initial Assessment

Analyst reviews alert details: Source, destination, user, time, indicators of compromise (IOCs).

Check if alert is false positive based on known patterns. Verify if activity is authorized or expected.

Investigation Procedures

Gather additional context: User activity, system logs, network traffic, related alerts.

Check threat intelligence for known malicious IPs, domains, or file hashes. Determine if incident or false positive.

Escalation Criteria

Escalate to senior analyst if: Confirmed malicious activity, data exfiltration suspected, multiple systems affected, advanced persistent threat (APT) indicators.

Critical incidents escalated to incident commander and CISO. Stakeholders notified per communication plan.

Containment Actions

Isolate affected systems from network if active threat. Disable compromised accounts. Block malicious IPs/domains at firewall.

Preserve evidence for forensic analysis. Don't alert attacker that they've been detected if ongoing investigation.

Documentation Requirements

Document all investigation steps, findings, and actions taken. Use standardized incident ticket format.

Include: Timeline, affected systems, IOCs, root cause, containment actions, remediation steps. Attach relevant logs and screenshots.

False Positive Handling

Document reason for false positive determination. Tune detection rules to reduce future false positives.

Track false positive rate by alert type. High false positive rates indicate need for rule refinement.

Threat Hunting

Proactive searching for threats not detected by automated tools. Use threat intelligence and attack patterns.

Hunt for: Lateral movement, privilege escalation, persistence mechanisms, data staging. Document findings and improve detections.

Alert Metrics

Track: Alert volume, false positive rate, mean time to detect (MTTD), mean time to respond (MTTR), escalation rate.

Review metrics weekly. Identify trends and improvement opportunities. Report to management monthly.

Shift Handoff

Handoff between shifts includes: Active incidents, ongoing investigations, system issues, upcoming maintenance.

Use standardized handoff template. Incoming shift reviews handoff notes and asks clarifying questions.

Continuous Improvement

Post-incident reviews identify lessons learned. Update runbooks and procedures. Improve detection rules.

Share knowledge across team. Training on new threats and techniques. Participate in threat intelligence community.