





# Essential Functions of a Modern SOC Analyst

## 1: Log Ingestion & Centralization

Log ingestion is the backbone of SOC operations. It involves gathering logs from:

-  Firewalls, Routers, IDS/IPS
-  Servers (Web, File, DB)
-  Endpoints (Laptops, Workstations)
-  Applications (Cloud & Internal)

Logs contain vital events (e.g., login attempts, file access) and are continuously collected using agents or collectors.

Without logs, **detection is impossible**.




---

## 2: Security Reporting & Visualization

This function turns raw data into meaningful insights through:


-  Dashboards
-  Weekly/Monthly Reports
-  Compliance Logs
-  Incident Reports



Useful for:

-  Management → Risk Awareness
  -  Security Teams → Performance Review
  -  Auditors/Regulators → Compliance Verification
- 

## 3: Cybersecurity R&D (Research & Detection) Key

for proactive defense, including:

-  Studying new exploits (e.g., zero-days)


-  Writing custom SIEM rules
-  Building automation scripts
- ☐ Testing new tools in lab environments

Continuous R&D keeps the SOC ahead of threats.

---

#### 4: Threat Intelligence Integration

Enriches detection with:





- ☐ IOCs (malicious IPs, domains, hashes)
- ☐ TTPs from MITRE ATT&CK
-  Threat Feeds (OSINT, commercial, gov)

This enables **faster detection** and **predictive defense**.

---

#### 5: SOC Knowledge Base

The SOC's internal memory:




-  Past incidents + resolutions
-  Playbooks for specific threats (e.g., phishing)
-  Checklists for investigations
- ☐  Training docs for analysts

Ensures consistency, faster response, and smoother onboarding.

---

#### 6: Incident Ticketing System

Using tools like **JIRA**, **ServiceNow**, or **RTIR** to:

-  Auto-generate tickets from alerts
- ☐ Assign analysts with priorities
-  Document every action
-  Enable collaboration




-  Maintain audit trail

Ensures structured and traceable response workflows.

---

## 7: SIEM Technology Backbone

SIEM (e.g., **Splunk**, **QRadar**, **Sentinel**) powers the SOC by:



-  Ingesting diverse log sources
-  Normalizing + correlating data
-  Triggering alerts from anomalies

SIEM offers **centralized visibility** and **real-time detection**.

---

## 8: Data Aggregation & Correlation

Links scattered events into meaningful alerts:

-  Suspicious login from abroad + data exfil → Attack Chain
-  Repeated login failures → Brute-force Attempt

Reduces noise and detects **multi-stage attacks**.