





# Mastering Log Collection in SOC Operations

Welcome to this documentation repository dedicated to **Log Collection** — a foundational capability within any **Security Operations Center (SOC)**. This guide represents my **learning journey and hands-on exploration** into the world of cybersecurity operations, with a particular focus on how logs enable **threat detection, incident response, and infrastructure visibility**.

## Why Log Collection Matters

Logs are the **heartbeat of a SOC**, providing raw telemetry for:

-  Threat Detection & Real-Time Monitoring
  -  Incident Investigation & Digital Forensics
  -  Compliance Auditing (PCI-DSS, HIPAA, ISO)
  -  Infrastructure Visibility & Cyber Resilience
- 

## Key Focus Areas

### System Logs

Capture logs from:

- Linux/Unix servers (`/var/log/syslog`, `auth.log`)
- Network devices (routers, switches)
- Workstations and endpoints

### Application Logs

Track:

- Web application logs (access/error logs)
- Authentication attempts
- Database queries
- API interactions

### Security Devices

Collect alerts from:

- Antivirus, EDR solutions

- Firewalls & UTM
  - IDS/IPS (e.g., Snort, Suricata)
- 

### Log Normalization

Standardize logs using **regex/parsing rules** for compatibility with SIEM tools like Splunk, ELK, QRadar.

---

### Log Transport & Forwarding

Secure log forwarding with tools such as:

- Splunk Universal Forwarder
  - Syslog (rsyslog, syslog-ng)
  - NXLog / Elastic Beats
- 

### Storage & Retention

- Short-term: Local storage
  - Long-term: Cloud or cold storage
  - Compliance: E.g., 1-year retention for PCI-DSS
- 

### Log Integrity

Ensure tamper-proof logs via:

- Cryptographic checksums
  - Permission hardening
  - Immutable (WORM) storage
- 

### Real-Time Ingestion

Enable live analysis:

- Alerting & correlation
- Dashboards
- Threat hunting

---

## Tools Used

- Splunk Enterprise & Universal Forwarder
- Rsyslog / Rsyslog
- NXLog
- SIEM Platforms (Elastic, QRadar, etc.)

### Project Directory

SOC-Log-Collection/

```
├── README.md
├── diagrams/
│   ├── log_flow_architecture.png
│   └── normalization_pipeline.png
├── examples/
│   ├── sample_syslog.log
│   ├── normalized_log.json
│   └── splunk_inputs.conf
├── config/
│   ├── rsyslog.conf
│   ├── nxlog.conf
│   └── splunk_forwarder_outputs.conf
├── scripts/
│   ├── log_rotation.sh
│   └── log_integrity_check.py
└── docs/
```

- | |— 01\_log\_sources.md
- | |— 02\_log\_forwarding.md
- | |— 03\_log\_storage\_retention.md
- | |— 04\_log\_integrity.md
- | |— 05\_real\_time\_ingestion.md
- | — LICENSE

This project is intended for SOC enthusiasts, blue team professionals, and cybersecurity learners exploring the critical role of log collection in cyber defense.