# 🛡️ Exploring Security Operations Center (SOC): Log Collection in Cyber Defense

Welcome to this documentation repository focused on **Log Collection** — a fundamental capability within any **Security Operations Center (SOC)**. This guide reflects my learning journey and hands-on exploration in cybersecurity operations.

### 🚀 Why Log Collection Matters

Logs are the heartbeat of a SOC. They provide the **raw telemetry** needed for:

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

### 🔍 Key Focus Areas

#### 1️⃣ System Logs

Capture logs from:

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

#### 2️⃣ Application Logs

Track:

- Web applications (access logs, error logs)
- Authentication systems (login attempts)
- Database queries and transactions
- API calls and responses

### 3️⃣ Security Devices

Collect alerts and detections from:

- Antivirus / EDR solutions
- Firewalls and UTM
- IDS/IPS systems (Snort, Suricata)

### 4️⃣ Log Normalization

Convert logs into a **standard format** (e.g., via regex or parsing rules) to make them analyzable across platforms and tools like SIEM.

### 5️⃣ Log Transport & Forwarding

Use agents and protocols to forward logs securely:

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

### 6️⃣ Storage & Retention

Store logs efficiently:

- Locally (short-term)
- Cloud (long-term, archival)
- Meet compliance (e.g., retain 1 year for PCI-DSS)

### 7️⃣ Log Integrity

Ensure logs are **tamper-proof**:

- Use cryptographic checksums
- Log file permissions and access control
- Immutable storage (WORM)

### 8️⃣ Real-Time Ingestion

Push logs immediately for:

- Alerting and correlation

- Live dashboards
- Threat hunting and behavioral analysis

## 🛠 Tools Used

- 🟠 **Splunk Enterprise & Universal Forwarder**
- ⚙️ **Syslog / 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 aimed at SOC enthusiasts, blue teamers, and cybersecurity students diving into the log collection side of cyber defense. Contributions and feedback are welcome!