Splunk-SOC-Home-Lab/

│── README.md # Main project guide

│── architecture/ # Diagrams & lab design

│ └── splunk-soc-architecture.png

│── setup-guides/ # Step-by-step Splunk setup docs

│ ├── splunk-install.md

│ ├── universal-forwarder.md

│ ├── windows-log-collection.md

│ ├── linux-log-collection.md

│ └── cloud-integration.md

│── detections/ # Splunk detection rules

│ ├── brute-force-detection.spl

│ ├── powershell-malware.spl

│ └── suspicious-dns-queries.spl

│── dashboards/ # Example dashboards (JSON exports)

│ ├── soc-overview.json

│ └── incident-response.json

│── playbooks/ # SOC use-cases

│ ├── incident-response.md

│ ├── threat-hunting.md

│ └── malware-investigation.md

│── automation/ # Phantom/SOAR playbooks (optional)

│ └── phishing-response.json

│── logs-samples/ # Sample log files

│ ├── windows-event-logs.txt

│ ├── linux-syslog.txt

│ └── firewall-logs.txt

│── LICENSE

└── .gitignore

📝 Example README.md

markdown

Copy code

# 🔐 Splunk SOC Home Lab

A complete \*\*Security Operations Center (SOC) Lab\*\* built using \*\*Splunk Enterprise\*\* and \*\*Splunk Universal Forwarders\*\*.

This project demonstrates \*\*log collection, security monitoring, detection rules, dashboards, and SOC workflows\*\* for practicing \*\*SIEM & Threat Hunting\*\*.

---

## 🎯 Objectives

- Deploy \*\*Splunk-based SOC\*\* environment

- Collect logs from \*\*Windows, Linux, Firewalls, and Cloud services\*\*

- Build \*\*SOC dashboards & correlation searches\*\*

- Detect attacks like \*\*Brute Force, Malware, Suspicious DNS\*\*

- Practice \*\*Incident Response & Threat Hunting\*\*

- (Optional) Integrate \*\*Splunk SOAR (Phantom)\*\* for automation

---

## 🧩 Tools & Stack

- \*\*Splunk Enterprise\*\* → SIEM / Log Management

- \*\*Splunk Universal Forwarders\*\* → Log forwarding agents

- \*\*Windows Event Logs / Linux Syslog\*\* → Data sources

- \*\*Firewall & Proxy Logs\*\* → Network telemetry

- \*\*Splunk Dashboards\*\* → SOC visualization

- \*\*Splunk SOAR (Phantom)\*\* → Incident response automation

---

## 💻 Lab Requirements

- \*\*CPU\*\*: 8+ cores

- \*\*RAM\*\*: 16+ GB

- \*\*Disk\*\*: 100 GB SSD

- \*\*Virtualization\*\*: VMware/VirtualBox/Proxmox/Cloud VM

---

## ⚡ Setup Workflow

1. Install \*\*Splunk Enterprise\*\* on your SOC server

2. Deploy \*\*Splunk Universal Forwarders\*\* on Windows/Linux endpoints

3. Configure \*\*inputs.conf & outputs.conf\*\* for log forwarding

4. Ingest \*\*Windows Event Logs, Syslog, Firewall logs\*\*

5. Build \*\*Dashboards\*\* for Security Monitoring

6. Create \*\*Detection Rules (Splunk SPL searches)\*\*

7. Practice \*\*Incident Response & Threat Hunting\*\*

8. (Optional) Add \*\*Splunk SOAR\*\* for automated playbooks

---

## 📂 Project Structure

- `setup-guides/` → Splunk installation & log collection steps

- `detections/` → Splunk SPL detection rules

- `dashboards/` → JSON dashboard exports

- `playbooks/` → Threat hunting & IR guides

- `automation/` → SOAR playbooks (optional)

- `logs-samples/` → Example log data

---

## 📷 Architecture Diagram

![SOC Architecture](architecture/splunk-soc-architecture.png)

---

## 📌 Roadmap

- [x] Splunk Enterprise installation

- [x] Windows/Linux log collection

- [ ] Firewall & Proxy log ingestion

- [ ] Threat Intelligence feed integration

- [ ] Splunk SOAR automation playbooks

---

## 🤝 Contribution

Pull requests and enhancements are welcome!

---