SIEM-Home-Lab/

│── README.md # Main project guide

│── architecture/ # Diagrams

│ └── siem-architecture.png

│── setup-guides/ # Setup documentation

│ ├── siem-installation.md

│ ├── windows-log-collection.md

│ ├── linux-log-collection.md

│ └── firewall-integration.md

│── detections/ # Detection rules (queries/correlation)

│ ├── brute-force-detection.spl

│ ├── ransomware-detection.spl

│ ├── suspicious-dns.spl

│ └── privilege-escalation.spl

│── dashboards/ # Dashboard JSON/exports

│ ├── overview.json

│ ├── incident-response.json

│ └── threat-hunting.json

│── playbooks/ # IR & hunting guides

│ ├── incident-response.md

│ ├── threat-hunting.md

│ └── malware-investigation.md

│── logs-samples/ # Sample anonymized logs

│ ├── windows-event-logs.txt

│ ├── linux-syslog.txt

│ └── firewall-logs.txt

│── LICENSE

└── .gitignore

📝 Example README.md

markdown

Copy code

# 🔐 SIEM Home Lab Project

This project is a \*\*Security Information and Event Management (SIEM) lab\*\* built to simulate a \*\*real SOC environment\*\*.

It demonstrates \*\*log collection, detection rules, dashboards, and incident workflows\*\* using open-source tools or Splunk/ELK/Wazuh.

---

## 🎯 Objectives

- Build a working \*\*SIEM platform\*\*

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

- Write \*\*detection rules for common attacks\*\*

- Create \*\*SOC dashboards\*\* for monitoring

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

- Align use cases with \*\*MITRE ATT&CK framework\*\*

---

## 🧩 Tools & Stack

Choose one SIEM solution (based on preference):

- \*\*Splunk\*\* (SIEM & dashboards)

- \*\*ELK Stack (Elasticsearch, Logstash, Kibana)\*\*

- \*\*Wazuh SIEM\*\* (open-source alternative)

---

## 💻 Lab Requirements

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

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

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

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

---

## ⚡ Setup Workflow

1. Install \*\*SIEM platform\*\* (Splunk / ELK / Wazuh)

2. Deploy agents for \*\*Windows/Linux/Firewall log collection\*\*

3. Configure log forwarding (\*\*Syslog, Winlogbeat, Filebeat\*\*)

4. Create \*\*dashboards\*\* for SOC visibility

5. Develop \*\*detection rules\*\* for Brute Force, Ransomware, Suspicious DNS, Privilege Escalation

6. Document \*\*Incident Response playbooks\*\*

---

## 📂 Project Structure

- `setup-guides/` → Installation & configuration steps

- `detections/` → SIEM queries/correlation rules

- `dashboards/` → JSON exports of dashboards

- `playbooks/` → Incident Response & Threat Hunting guides

- `logs-samples/` → Example log files

---

## 📷 Architecture Diagram

![SIEM Architecture](architecture/siem-architecture.png)

---

## 📌 Roadmap

- [x] Setup SIEM platform

- [x] Collect logs from Windows & Linux

- [ ] Add Firewall & Cloud log ingestion

- [ ] Add Threat Intelligence integration

- [ ] Expand detections with MITRE ATT&CK use cases

- [ ] Automate alerts with SOAR integration

---

## 🤝 Contribution

Contributions are welcome – feel free to submit pull requests or share detection rules!