Network Monitoring SOC Project

Network-Monitoring-SOC/ │ ├── README.md ├── logs/ │ ├── network_traffic_logs.csv │ ├── firewall_logs.csv │ ├── dns_logs.csv │ └── web_server_logs.csv │ ├── detections/ │ ├── suspicious_traffic.kql │ ├── ddos_attack.kql │ ├── malware_communication.kql │ └── unauthorized_access.kql │ ├── reports/ │ ├── incident_report_template.docx │ ├── incident_report_ddos.pdf │ ├── incident_report_malware.pdf │ └── threat_hunt_report.pdf │ ├── scripts/ │ ├── parse_logs.py │ ├── extract_iocs.py │ ├── generate_alerts.py │ └── dashboard_generator.py │ └── visuals/ ├── network_monitoring_workflow.png └── sentinel_dashboard_screenshot.png

README.md Sample Content:

```
# Network Monitoring SOC Project – Threat Detection & Alerting

## Overview
Demonstrates SOC-level network monitoring, log analysis, and
alerting for suspicious network activities.

## Objective
Showcase practical network monitoring skills, threat
detection, and incident response for recruiter evaluation.

## Tools Used
- Microsoft Sentinel
- Splunk (trial)
- Python (log parsing, IOC extraction, alert generation,
dashboards)
- Wireshark
- MITRE ATT&CK Framework

## Project Structure
- logs/: Network traffic, firewall, DNS, and web server logs
- detections/: KQL detection rules for suspicious traffic,
DDoS, malware communication, unauthorized access
- scripts/: Python automation scripts and dashboard generator
- reports/: Polished incident and threat hunt reports
- visuals/: Network monitoring workflow and dashboard
```

```
screenshots

## How to Run
1. Clone the repository.
2. Navigate to `scripts/`.
3. Run `parse_logs.py`, `extract_iocs.py`, `generate_alerts.py`, and `dashboard_generator.py`.
4. Review alerts, dashboards, and reports in `reports/` and `visuals/`.

## MITRE ATT&CK Mapping
| Tactic | Technique | ID | Severity | Description |
|--------|-----------|----|---------|-------------|
| Initial Access | Unauthorized Access | T1078 | High | Suspicious network access detected |
| Impact | Data Encrypted for Impact | T1486 | High | Simulated ransomware behavior in network traffic |
| Defense Evasion | Obfuscation | T1027 | Medium | Obfuscated communication patterns |
| Command & Control | C2 Communication | T1071 | High | Malware or attacker communication detected |
| Discovery | Network Service Scanning | T1046 | Medium | Network scanning identified |

## Learning Outcomes / Skills Demonstrated
- Network traffic analysis and monitoring
- Detection of suspicious or malicious network activity
- Log parsing and IOC extraction using Python
- Incident reporting and threat hunt documentation
- Dashboard visualization and workflow illustration

## Visuals
![Network Monitoring Workflow](visuals/network_monitoring_workflow.png)
![Sentinel Dashboard](visuals/sentinel_dashboard_screenshot.png)
```

Enhancements in Logs:

- Realistic network logs with hundreds of events
- Includes DDoS, malware communication, unauthorized access, and suspicious traffic scenarios

Enhancements in Scripts:

- Python scripts for log parsing, IOC extraction, alert generation, and dashboard visualization
- Automated PDF/CSV export of alerts and incidents

Reports:

- Completed incident reports for DDoS, malware, and unauthorized access scenarios
- Threat hunting summary with mitigation recommendations
- Professional templates for recruiter showcase

Visuals:

- Network monitoring workflow diagram
- Dashboard screenshots showing alerts and responses