SOC-Simulation Project

SOC-Simulation/ │ ├── README.md ├── logs/ │ ├── windows_security_logs.csv │ ├── linux_auth_logs.csv │ └── web_server_access.log │ ├── detections/ │ ├── brute_force_detection.kql │ ├── suspicious_logins.kql │ ├── privilege_escalation.kql │ └── malware_alerts.kql │ ├── reports/ │ ├── incident_report_template.docx │ ├── incident_report_bruteforce.pdf │ ├── incident_report_malware.pdf │ └── threat_hunt_report.pdf │ ├── scripts/ │ ├── parse_logs.py │ ├── extract_iocs.py │ ├── generate_alerts.py │ └── dashboard_generator.py │ └── visuals/ ├── soc_workflow_diagram.png └── sentinel_dashboard_screenshot.png

README.md Sample Content:

```
# SOC Simulation – Microsoft Sentinel & MITRE ATT&CK

## Overview
Professional SOC Simulation demonstrating log analysis,
detection, alert triage, threat hunting, and incident
reporting with realistic scenarios and visual dashboards.

## Objective
Showcase practical SOC Level 1 skills to recruiters and hiring
managers, including detection, incident handling, and threat
mapping.

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

## Project Structure
- logs/: Realistic Windows, Linux, and Web Server logs with
multiple attack scenarios
- detections/: KQL detection rules for brute force, privilege
```

```
escalation, suspicious logins, and malware
- scripts/: Python automation scripts and dashboard generator
- reports/: Polished incident and threat hunt reports
- visuals/: SOC workflow diagram 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 generated alerts, dashboards, and reports in
`reports/` and `visuals/`.

## MITRE ATT&CK Mapping
| Tactic | Technique | ID | Severity | Description |
|--------|-----------|----|---------|-------------|
| Credential Access | Brute Force | T1110 | High | Multiple
failed login attempts detected |
| Privilege Escalation | Abuse Elevation Control | T1548 |
Medium | Admin privileges accessed unexpectedly |
| Defense Evasion | Obfuscation | T1027 | Medium | Suspicious
process or script obfuscation |
| Execution | Malware Execution | T1059 | High | Detected
malware running in logs |

## Learning Outcomes / Skills Demonstrated
- SIEM monitoring and alert triage
- Log parsing and IOC extraction using Python
- Threat detection aligned with MITRE ATT&CK
- Incident documentation and reporting
- Visualization of SOC workflow and dashboards

## Visuals
![SOC Workflow](visuals/soc_workflow_diagram.png)
![Sentinel
Dashboard](visuals/sentinel_dashboard_screenshot.png)
```

Enhancements in Logs:

- Larger datasets with hundreds of events
- Multiple attack scenarios (brute force, malware, suspicious logins, privilege escalation)

Enhancements in Scripts:

- `dashboard_generator.py` produces visual summaries of alerts and incidents
- Enhanced alert generation with automated PDF and CSV exports
- Cross-platform log correlation

Reports:

- Completed incident reports for each attack scenario
- Threat hunting summary with mitigation recommendations
- Professional template for recruiter showcase

Visuals:

- Workflow diagram: log ingestion → detection → alert → incident report
- Dashboard screenshot from Sentinel or Splunk