Capstone SOC Project

Capstone-SOC/ │ ├── README.md ├── logs/ │ ├── windows_event_logs.csv │ ├── linux_sys_logs.csv │ ├── firewall_logs.csv │ └── application_logs.csv │ ├── detections/ │ ├── malware_detection.kql │ ├── privilege_escalation.kql │ ├── ransomware_behavior.kql │ └── unauthorized_access.kql │ ├── reports/ │ ├── incident_report_template.docx │ ├── incident_report_ransomware.pdf │ ├── incident_report_privilege_escalation.pdf │ └── threat_hunt_report.pdf │ ├── scripts/ │ ├── parse_logs.py │ ├── extract_iocs.py │ ├── generate_alerts.py │ └── dashboard_generator.py │ └── visuals/ ├── capstone_soc_workflow.png └── sentinel_dashboard_screenshot.png

README.md Sample Content:

-
  ```
  # Capstone SOC Project – Advanced Monitoring & Incident
  Response

  ## Overview
  Capstone SOC project demonstrating advanced log analysis,
  threat detection, alert correlation, and incident response
  workflows for multiple systems.

  ## Objective
  Showcase practical, end-to-end SOC skills and incident
  handling capabilities suitable for recruiter evaluation and
  portfolio display.

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

  ## Project Structure
  - logs/: Windows, Linux, firewall, and application logs with
  multiple attack scenarios
  - detections/: KQL detection rules for malware, ransomware,
  ```

```
privilege escalation, and unauthorized access
- 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. Execute `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 across systems |
| Privilege Escalation | Abuse Elevation Control | T1548 |
Medium | Unexpected privilege escalation detected |
| Defense Evasion | Obfuscation | T1027 | Medium | Suspicious
script or process obfuscation |
| Impact | Data Encrypted for Impact | T1486 | High |
Simulated ransomware activity detected |
| Initial Access | Unauthorized Access | T1078 | High |
Credential misuse detected |

## Learning Outcomes / Skills Demonstrated
- Multi-system SIEM monitoring and alert correlation
- Log parsing and IOC extraction using Python
- Threat detection and mapping to MITRE ATT&CK
- Incident reporting and mitigation recommendations
- Dashboard visualization and SOC workflow illustration

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

Enhancements in Logs:

- Multiple systems: Windows, Linux, Firewall, Applications

- Realistic attack scenarios: ransomware, privilege escalation, unauthorized access, malware

Enhancements in Scripts:

- Enhanced alert correlation between multiple log sources
- Dashboard generator producing cross-platform visual summaries
- Automated PDF and CSV export of alerts and incidents

Reports:

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

Visuals:

- SOC workflow diagram illustrating multi-system monitoring and alert correlation
- Dashboard screenshot demonstrating alerts and response