Draft Project Proposal

Student Name: Ahmed Reda Ismail

Project Title: SIREN – Smart Incident Response & Event Notifier

---

Initial Description of the Problem

In modern organizations, the number of cybersecurity incidents is growing rapidly due to the increasing complexity of networks and the evolving sophistication of attacks. Security teams (SOC Analysts) often struggle to detect, analyze, and respond to incidents in real-time, leading to data breaches, downtime, and financial losses.

Most existing monitoring tools are either too complex, too expensive, or lack automated response mechanisms. Manual handling of incidents results in slower reaction times, inconsistent responses, and incomplete investigations significantly increasing the risk of prolonged compromise.Therefore, there is a critical need for a system that can **automate the detection and response process** to ensure faster containment and minimize human error.

Initial Description of the Suggested Solution

The proposed solution, **SIREN (Smart Incident Response & Event Notifier)**, is an intelligent and semi-automated incident response platform designed to enhance the efficiency and accuracy of cybersecurity teams. It aims to automate key stages of the **Incident Handling Process** Preparation, Detection, Containment, and Post-Incident Activity.

The system will be composed of the following major components:

- **Frontend (React/Tailwind + Framer Motion):** A responsive, modern dashboard interface for monitoring hosts, processes, and incidents in real-time.
- **Backend Middleware (Node.js):** A lightweight API layer that bridges the user interface and the local Python agent.
- **Python Agent (Windows-based):** Responsible for interacting directly with the system scanning files, monitoring processes, and executing automated containment actions.

The goal of SIREN is to simulate an automated **Security Operations Center (SOC)** that can quickly identify, analyze, and mitigate security incidents with minimal human intervention.

Key Features

1. **Host Scan & Baseline Integrity Checker** – Detects unauthorized or malicious changes in system files and configurations.
2. **Behavioral Monitoring** – Continuously observes process behavior and detects anomalies in real-time.
3. **IOC Hunting** – Searches for known Indicators of Compromise (hashes, IPs, domains) across connected hosts.
4. **Auto-Containment Playbooks** – Automates response actions such as isolating hosts, killing suspicious processes, and notifying administrators.
5. **Cyber Kill Chain Visualization** – Maps the progress of an attack across stages (Reconnaissance, Exploit, C2, Action).
6. **Incident Reporting & Lessons Learned** – Automatically generates post-incident summaries with recommendations to improve defenses.

Expected Outcome

By integrating automation with the incident response lifecycle, **SIREN** will:

- Reduce human response time to security incidents.
- Increase accuracy and consistency in threat containment.
- Provide clear visibility into host and process activity.
- Support analysts through actionable alerts and auto-generated reports.

Conclusion

SIREN bridges the gap between traditional manual SOC operations and modern automated cyber defense. It combines responsive UI design, real-time backend communication, and intelligent automation to create a comprehensive incident response and monitoring environment suitable for both learning and real-world simulation.