Project Title: Security Orchestration, Automation, and Response (SOAR) Framework

1. Introduction

In the current cybersecurity landscape, Security Operations Centers (SOC) face significant challenges due to the overwhelming volume of security alerts, often leading to "alert fatigue." Traditional manual incident response is no longer sufficient against sophisticated and automated cyber threats.

Security Orchestration, Automation, and Response (SOAR) is an advanced technology framework designed to streamline security operations. It enables organizations to collect data about security threats from multiple sources and respond to low-level security events without human intervention. The goal of this project is to create a cohesive environment where disparate security tools work in unison to provide a rapid, standardized, and effective defense mechanism.

---

2. System Architecture Description

The architecture of the proposed SOAR framework is organized into a modular four-tier structure to ensure scalability and seamless integration:

- **Data Ingestion Layer (Security Sources):** This layer consists of various security tools like **SIEM** (Security Information and Event Management), **Next-Gen Firewalls**, and **Endpoint Detection & Response (EDR)** systems. These tools act as sensors, generating alerts and logs based on network activity.
- **Orchestration & Integration Layer:** The core of the system where **API-based connectors** link the SOAR platform with third-party security tools. This layer enables "Orchestration," allowing different products to share context and execute coordinated actions across the infrastructure.
- **Automation & Intelligence Layer:** This layer hosts the **Automation Playbooks** and **Threat Intelligence** feeds. It automates repetitive tasks such as IP reputation checks, file sandboxing, and domain lookup by correlating internal alerts with external databases (e.g., VirusTotal, AbuseIPDB).
- **Management & Response Layer:** The final layer provides a **Centralized Case Management Dashboard**. It allows security analysts to monitor incident lifecycles, review automated actions, and generate compliance reports for auditing purposes.

---

3. Objectives of the Study

The primary objective of this laboratory project is to design and implement a framework that enhances the efficiency of Security Operations Centers (SOC). The specific objectives are as follows:

- **Integration and Orchestration:** To integrate disparate security tools (such as SIEM, Firewalls, and Endpoint Protection) into a unified interface using APIs and ensure coordinated defense.
- **Automation of Incident Response:** To deploy Automated Playbooks for high-volume, low-complexity threats (Phishing, Brute-force) to reduce the **Mean Time to Respond (MTTR)**.
- **Standardization of Workflows:** To establish **Standard Operating Procedures (SOPs)** to minimize human error and ensure consistency in incident handling.
- **Threat Intelligence Integration:** To automate the ingestion of external threat feeds for real-time context and correlation with internal logs.
- **Centralized Case Management & Reporting:** To implement a dashboard for tracking incident lifecycles and generating data-driven performance reports.

---

4. Expected Outcome

By the end of this lab, the project aims to demonstrate:

1. A significant reduction in the manual workload of security analysts.
2. Faster containment and remediation of common security threats.
3. An improved overall security posture through standardized, logic-driven response mechanisms.