SOAR Project: Automated Threat Response System Isolation System

Summary:

This document provides a detailed overview of an implemented Security Orchestration, Automation, and Response (SOAR) project. The initiative was designed to address the challenges of manual alert fatigue and delayed incident response within a simulated security environment. By integrating industry-standard tools—an Endpoint Detection and Response (EDR) platform, a SOAR engine, and a team communication channel—this project established a robust, event-driven automation pipeline for detecting and containing a credential-stealing attack with minimal human intervention.

The Challenge: From Manual Chaos to Automated Control

In a modern security operations center, the sheer volume of alerts can overwhelm even the most skilled analysts. The repetitive, time-consuming tasks of initial triage, data enrichment, and containment actions often lead to human error and critical delays. This project was born from the need to transform this reactive and inefficient process into a proactive and automated system. The goal was to build a cohesive solution that could rapidly identify a specific threat—credential theft—and automatically coordinate a definitive, effective response.

Technology used:

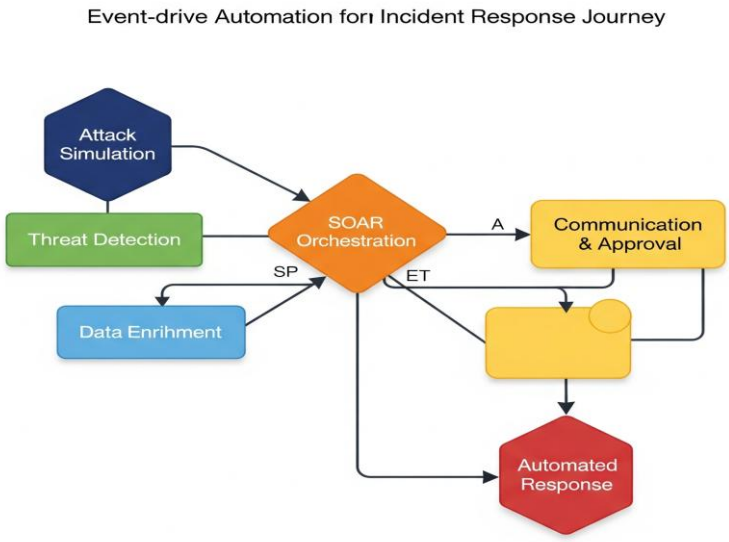
The success of this project was dependent on the strategic integration of a diverse set of security applications and platforms, each fulfilling a critical role in the automated workflow.

- **Tines:** As the central intelligence and orchestration hub, Tines was responsible for designing and executing the entire automated workflow. Its no-code platform was leveraged to build complex, conditional logic that connects and manages all other tools in the pipeline.
- **LimaCharlie:** This powerful EDR platform was deployed on the virtual machine to serve as the project's primary detection mechanism. It was configured to monitor for suspicious processes and file activities, generating the initial security alerts that would trigger the automation.
- **Windows VM:** The project's operational environment was a Windows Virtual Machine. This isolated and controlled space was essential for safely simulating the attack and providing a realistic host for the EDR agent.
- **Lazagne:** A credential recovery tool, Lazagne was intentionally used to simulate the malicious activity of a real-world attacker. Its execution served as the test case, allowing for a realistic demonstration of the detection capabilities and automated response.
- **Slack:** Integrated as the communication and human-in-the-loop component, Slack received real-time, actionable notifications from the SOAR platform. It provided a simple, interactive interface for a security analyst to approve or deny containment actions.

Workflow: A Step-by-Step Response:

The project's core is an event-driven automation that provides a seamless, end-to-end incident response journey. The process unfolds as follows:

1. **Attack Simulation:** The journey begins with the simulated execution of the Lazagne tool on the Windows VM, mimicking a real-world credential-stealing attempt through the Windows VM.
2. **Threat Detection:** LimaCharlie's EDR agent immediately detects this activity as suspicious, based on predefined rules, and generates a security alert. This alert serves as the trigger for the entire SOAR workflow.
3. **SOAR Orchestration:** The LimaCharlie alert is automatically ingested by Tines. Tines, acting as the master conductor, instantly initiates the pre-built automation.
4. **Data Enrichment:** The workflow's first action is to enrich the raw alert data. Tines automatically extracts critical context, such as the compromised host's name and user account information, by querying LimaCharlie's API for further details on the process that triggered the alert.
5. **Communication & Approval:** Tines then sends a carefully formatted message to a designated Slack channel. This message contains the enriched alert details and, crucially, an interactive button. This "human-in-the-loop" step allows an analyst to provide a go-or-no-go decision on the next action.
6. **Automated Response:** Upon receiving approval from Slack, Tines sends an API call directly back to LimaCharlie. This final, decisive action commands LimaCharlie to automatically isolate the host from the network, containing the threat and preventing any further lateral movement.



Key Skills and Project Outcomes

This project is a tangible demonstration of several critical cybersecurity and automation skills. It moves beyond theoretical knowledge to showcase practical, hands-on experience in building and managing a complex security pipeline.

- **SOAR Principles:** The project provides concrete proof of the ability to design and implement a security automation workflow that significantly improves both efficiency and consistency.
- **Tool Integration:** It highlights hands-on experience in connecting disparate security platforms—an EDR tool, a SOAR platform, and a communication application—using APIs and webhooks.
- **Threat Simulation:** The successful simulation of a realistic attack demonstrates a practical understanding of attack vectors and the capability to safely test defensive controls.
- **Automation Logic:** It showcases proficiency in building logical, conditional workflows that enable automated decision-making based on real-time data.
- **Problem-Solving:** The project itself serves as a testament to the ability to identify a real-world security challenge and leverage a combination of application-based tools to solve it effectively.

Future Outlook: Continuous Improvement

While this project successfully demonstrates a core SOAR capability, the pipeline is designed for continuous enhancement. Potential future expansions include:

- **Ticketing System Integration:** Automating the creation of a ticket in a platform like Jira or ServiceNow to provide a single source of truth for tracking the incident.
- **Threat Intelligence Enrichment:** Integrating with a threat intelligence platform (e.g., VirusTotal or AlienVault OTX) to automatically check for known malicious hashes or IP addresses during the enrichment phase.
- **Advanced Response Actions:** Expanding the automated response capabilities to include more granular actions, such as terminating a malicious process or deleting a file, based on the severity of the threat.