Project One Pager: SOAR Detection & Response for LaZagne Malware

Actual Idea:
Implement an automated Security Orchestration, Automation, and Response (SOAR) workflow to detect, report, and respond to LaZagne malware, a credential-stealing tool, by combining LimaCharlie EDR detection with Tines.com automation. The solution integrates endpoint monitoring, automated alerting, and controlled incident response to minimize the impact of malware on enterprise networks.

Project Summary:

- **Detection:** LimaCharlie continuously monitors endpoints for LaZagne execution using sophisticated rules that check file paths, command lines, and file hashes. This ensures rapid identification of credential-stealing attempts.
- **Notification:** Detected events are forwarded to Tines, which automates real-time alert delivery to Slack channels and email distribution lists, providing immediate situational awareness to SOC teams.
- **Manual Decision:** SOC analysts access Tines' manual approval interface to review detection details and determine whether endpoint isolation is required, allowing human oversight for critical decisions.
- **Action:** Upon analyst approval, Tines executes the `isolate_sensor` action via LimaCharlie API, isolating affected endpoints from the network and sending confirmation alerts to ensure traceability.
- **Audit and Reporting:** All detection events, analyst decisions, and automated actions are logged for compliance, reporting, and future forensic analysis.

What Has Been Done & Working:

- Detection rules for LaZagne malware successfully deployed and validated in LimaCharlie.
- Tines automation workflow fully operational for event reception, alerting, and manual isolation approvals.
- End-to-end testing completed: alerts successfully sent to Slack/email, manual isolation interface functional, endpoint isolation executed without errors.
- Integration with notification systems and APIs verified, ensuring seamless automation across platforms.

Benefits:

- Rapid and accurate malware detection with minimal false positives.
- Automated alerting reduces Security Operations Center response time and improves situational awareness.
- Controlled, analyst-approved response prevents unnecessary disruption while ensuring security.
- Complete audit trail supports compliance, forensic analysis, and continuous improvement.
- Scalable solution adaptable to various enterprise environments and additional malware types.

Conclusion:
The project demonstrates an effective and practical SOAR workflow for malware detection and response. By combining automated detection, real-time notifications, manual decision-making, and endpoint isolation, it provides a robust, scalable, and secure approach to mitigating credential-stealing malware threats. The system enhances SOC efficiency, ensures timely threat containment, and maintains human oversight for critical security decisions, providing a comprehensive enterprise-grade solution.