Asagba Jeremiah's SOC Automation Project Report

Executive Summary:
Over the course of seven days, I embarked on a journey to develop and document my SOC Automation Project. Through meticulous planning, hands-on implementation, and collaboration with the cybersecurity community, I successfully built a dynamic and efficient Security Operations Center (SOC) environment. This report provides a comprehensive overview of the project, detailing the objectives, challenges, solutions, and key learnings encountered along the way.

Project Overview:
The SOC Automation Project aimed to create a robust and automated SOC environment capable of effectively detecting, analyzing, and responding to security incidents. Key components of the project included:

Components of the Project:
Wazuh Manager, Complete with Dashboard:

- Customized settings within Wazuh aimed at targeted Mimikatz detection.
- Real-time alerting and correlation functionalities to pinpoint potential Mimikatz activity.
- Integration with Windows 10 agents to enhance visibility at the endpoint.

Windows 10 Agent:

- Set up to monitor and identify Mimikatz-related actions.
- Continuous monitoring of system memory, processes, and events.
- Linked with Wazuh for consolidated alerting and response mechanisms.

TheHive for Comprehensive Case Management:

- Employed TheHive for centralized management of cases.
- Automatic initiation of cases when Mimikatz activity is detected by Wazuh.
- Smooth integration with Wazuh to coordinate responses to incidents.

Shuffle for SOAR :

- Introduction of SOAR functionalities through Shuffle.

Workflow:

- Wazuh-generated Mimikatz alert triggers Shuffle.
- Shuffle extracts SHA-256 hash from the Wazuh alert.
- Query to Virustotal to assess the reputation score of the hash.
- Transmission of details from Wazuh alert and Virustotal to TheHive to open a new case and input all relevant information.
- Dispatch of an email to SOC analysts, alerting them and requesting action based on the event ID.

Advantages and Disadvantages:

Advantages:

Early Detection and Swift Response:

- Utilizing SOAR capabilities via Shuffle enables the prompt detection of Mimikatz incidents, automating workflows for swift and proactive responses.

Enriched Alert Details:

- Integration with Virustotal enriches alert details by automatically extracting and verifying the SHA-256 hash, equipping analysts with informed insights.

Streamlined Incident Management:

- The integration between Shuffle and TheHive centralizes and streamlines incident management, automating case creation and ensuring a structured response.

Efficient Communication:

- Email alerts generated by Shuffle to SOC analysts facilitate efficient communication, ensuring timely notification and response to Mimikatz incidents.

Proactive Threat Mitigation:

- Automated workflows and enriched details empower SOC analysts to proactively mitigate potential threats, contributing to a proactive security posture.

Disadvantages:

Complex Implementation:

- Incorporating SOAR capabilities introduces complexity to the SOC environment, necessitating careful implementation and ongoing management.

Resource Intensive:

- SOAR workflows may consume additional system resources, potentially impacting performance if not adequately provisioned.

Dependency on External Services:

- Integration with external services introduces dependencies, rendering the SOC environment vulnerable to disruptions or changes in these services.

False Positives:

- Automated workflows may produce false positives without finely tuned rules, resulting in unnecessary alerts and potential misallocation of resources.

Training and Familiarization:

- Comprehensive training for SOC analysts is essential to effectively leverage the new SOAR workflows, ensuring optimal utilization and preventing misconfigurations.

Key Learnings:

- The importance of networking and community support in navigating challenges.
- The significance of attention to detail in configuration and troubleshooting processes.
- The value of continuous learning and adaptability in the field of cybersecurity.

Conclusion:
In conclusion, the SOC Automation Project has been a rewarding and enlightening experience, enabling me to deepen my understanding of SOC operations, automation, and incident response. I am grateful for the opportunity to document and share my journey with the cybersecurity community, and I look forward to applying the knowledge gained to future endeavors.

Thank you to everyone who has followed along and provided support throughout this project. If you have any questions or seek further clarification on specific aspects of the guide, feel free to reach out. Happy automating and securing