SOC Automation Project Report- Navjot Singh

SOC Environment Design Report - Emphasis on Mimikatz Detection

Executive Summary:

This report extends the design of the Security Operations Center (SOC) environment to include Security Orchestration, Automation, and Response (SOAR) capabilities with Shuffle. The primary focus remains on detecting Mimikatz, utilizing Wazuh for SIEM, Windows 10 agents, TheHive for case management, and now incorporating Shuffle with SOAR workflows. The objective is to automate incident response processes and enrich alert details through integration with Virustotal.

Introduction:

In line with the primary goal of enhancing the organization's ability to detect and respond to Mimikatz incidents, SOAR capabilities through Shuffle are introduced. This includes automated workflows that leverage Wazuh alerts, Virustotal reputation checks, and integration with TheHive for streamlined incident response.

Components of the SOC Environment:

Wazuh Manager with Dashboard:

- Customized configurations in Wazuh for specialized Mimikatz detection.
- Real-time alerting and correlation capabilities for identifying potential Mimikatz activity.
- Integration with Windows 10 agents for enhanced endpoint visibility.

Windows 10 Agent:

- Configured to monitor and detect Mimikatz-related activities.
- Continuous monitoring of memory, processes, and system events.
- Integration with Wazuh for centralized alerting and response.

TheHive for Case Management:

- Utilization of TheHive for centralized case management.
- Automatic case creation upon detection of Mimikatz activity by Wazuh.
- Seamless integration with Wazuh for coordinated incident response.

Shuffle for SOAR Workflow:

- Introduction of SOAR capabilities through Shuffle.
- Workflow:

- Mimikatz alert generated by Wazuh triggers Shuffle.
- Shuffle extracts SHA-256 hash from the Wazuh alert.
- Virustotal is queried to check the reputation score of the hash.
- Details from Wazuh alert and Virustotal are sent to TheHive to open a new case and insert all relevant information.
- Shuffle sends an email to SOC analysts, alerting them and requesting a response to potentially block based on the event ID.

Implementation Details:

- Wazuh is configured with custom rules for specialized Mimikatz detection.
- Windows 10 agents deployed and configured for Mimikatz-related events reporting to Wazuh.
- TheHive is configured for automatic case creation upon detection of Mimikatz incidents.
- Shuffle integrated into the workflow for SOAR capabilities, including Virustotal integration and email alerts.

Advantages and Disadvantages:

Advantages

Early Detection and Swift Response:

- SOAR capabilities through Shuffle enable early detection of Mimikatz incidents, automating workflows for a swift and proactive response.

Enriched Alert Details:

- Virustotal integration enhances alert details by automatically extracting and checking the SHA-256 hash, providing analysts with informed insights.

Streamlined Incident Management:

- Shuffle's integration with 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 prompt 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:

- Introducing SOAR capabilities adds complexity to the SOC environment, requiring careful implementation and ongoing management.

Resource Intensive:

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

Dependency on External Services:

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

False Positives:

- Automated workflows may generate false positives without finely tuned rules, leading to unnecessary alerts and potential misallocation of resources.

Training and Familiarization:

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

Conclusion:

This SOC Automation Project has been an exciting and enlightening journey into the intricacies of security incident detection and response. Through careful design, meticulous setup, and hands-on configurations, I've explored the capabilities of tools like Wazuh Manager, TheHive, and Shuffle, gaining valuable insights into SOC workflows.

As I reflect on this project, I've not only honed my technical skills but also developed a deeper understanding of the importance of systematic approaches in cybersecurity. The integration of Mimikatz detection, SOAR capabilities with Shuffle, and the utilization of various tools have contributed to a robust and comprehensive security framework.

This guide serves as a testament to the learning and growth experienced throughout the project. If you embark on a similar journey, I hope this guide provides you with insights and practical steps to enhance your understanding of SOC automation.

Remember, the ever-evolving landscape of cybersecurity requires continuous learning and adaptation. Stay curious, stay vigilant, and keep exploring the exciting realm of security operations.

If you have any questions or seek further clarification on specific aspects of the guide, feel free to reach out. Happy automating and securing!