

Implementation of a Security Operations Center (SOC) Using Wazuh Tool

This repository contains the implementation details, configurations, and documentation for building a functional Security Operations Center (SOC) using open-source tools. The project integrates **Wazuh (SIEM)**, **AbuseIPDB (Threat Intelligence Platform)**, and **IRIS (Ticketing System)** to provide a comprehensive framework for detecting, analyzing, and responding to security incidents.

Features

- **Comprehensive SOC Setup:** Fully functional Security Operations Center utilizing open-source tools.
 - **SIEM Integration:** Wazuh tool for security event management and log analysis.
 - **Threat Intelligence:** AbuseIPDB integration for enriched threat data and automated incident handling.
 - **Incident Management:** IRIS configuration for case management and response automation.
 - **Active Response Mechanisms:** Automated responses to common security threats like brute force attacks and malware detection.
-

Project Structure

Goal

The objective of this project is to enhance the capabilities of detecting, analyzing, and responding to security incidents using a combination of open-source tools and automated workflows.

Key Tasks and Contributions

- **Infrastructure Setup:** Environment setup and Wazuh configuration.
 - **Threat Intelligence:** Integration with AbuseIPDB for enriching security data.
 - **Incident Automation:** Automated workflows and responses for detected incidents.
 - **Case Management:** IRIS setup for incident ticketing and tracking.
 - **Testing & Documentation:** Simulated attacks and consolidated reporting.
-

Tools and Technologies Used

1. **Wazuh:** Security Information and Event Management (SIEM) platform for monitoring, alerting, and responding to threats.
 2. **AbuseIPDB:** A threat intelligence platform for identifying malicious IP addresses.
 3. **IRIS:** Ticketing system for managing security incidents.
 4. **Docker:** For deploying IRIS and other services in a containerized environment.
 5. **Linux Systems:** Ubuntu 22.04 and 20.04 for hosting and configuring tools.
-

Repository Contents

- **Documentation:**
 - Detailed setup and configuration instructions.
 - Integration processes for Wazuh, AbuseIPDB, and IRIS.
 - Troubleshooting steps and challenges faced during the implementation.
 - **Scripts:**
 - Python and configuration scripts for AbuseIPDB and IRIS integration.
 - Automation workflows and active response setups.
 - **Testing:**
 - Scenarios for brute force attack simulation and response validation.
 - Logs and screenshots demonstrating successful implementation.
 - **Report:**
 - [Project Analysis Report](#).
-

Getting Started

Prerequisites

- Virtual machines or Docker setup.
- Linux-based operating system (Ubuntu 20.04/22.04).
- Access to AbuseIPDB API and IRIS configuration.

Installation

1. Wazuh Setup:

Follow the [official installation guide](#).

2. AbuseIPDB Integration:

Refer to the [AbuseIPDB Integration](#).

3. IRIS Setup:

Install and configure IRIS using Docker. See the [IRIS integration section](#).

Usage

Detection and Alerting

- Configure Wazuh to monitor security events.
- Use AbuseIPDB for threat intelligence enrichment.
- Trigger alerts for incidents like brute force attacks or malware detection.

Automated Response

- Enable Wazuh's active response mechanisms (e.g., IP blocking, account disabling).
 - Automatically log incidents into IRIS for tracking and escalation.
-

Challenges and Insights

- Resolved issues with API compatibility during tool integration.
 - Overcame networking and configuration challenges in a multi-tool environment.
 - Gained hands-on experience with incident response automation and SOC tools.
-

Future Improvements

- Expand the SOC with additional tools like MISP for advanced threat intelligence.
 - Optimize active response mechanisms for faster incident handling.
 - Enhance documentation and scripts for seamless integration.
-

Contributing

Contributions are welcome! Please fork the repository, create a feature branch, and submit a pull request for review.

License

This project is licensed under the [MIT License](#).

For detailed steps and implementation, refer to the [Project Documentation](#). For any queries, please contact the contributors listed in the documentation.