IBM Innovation Centre for Education

PHEMESOFT Software That Matters

YENEPOYA (DEEMED TO BE UNIVERSITY)

YENEPOYA INSTITUTE OF ARTS, SCIENCE, COMMERCE AND MANAGEMENT
(A constituent unit of Yenepoya Deemed to be University)

SECURATRIX

PROJECT SYNOPSIS

Security Operations Center (SOC)
Implementing SIEM for small Businesses

BACHELOR OF COMPUTER APPLICATION
(IoT, Ethical Hacking, Cyber Security and Digital Forensics)

SUBMITTED BY: **Team-040: Securatrix**

Name	REG NO.	Email ID
Kiran Singh	**22BCIECS048**	**21071@yenepoya.edu.in**
Mohammed Fairooz S	22BCIECS088	21114@yenepoya.edu.in
Sabareesh M S	22BCIECS109	21108@yenepoya.edu.in
Sayanth V P	22BCIECS112	22690@yenepoya.edu.in
Muhammed Ansar T	22BCIECS081	21062@yenepoya.edu.in

GUIDED BY:
Mr. Shashank – IBM SME

INDEX

INTRODUCTION:

The increasing complexity and volume of cyber threats necessitate the automation of Security Operations Centers (SOCs). Traditional SOCs rely heavily on manual processes, which can be time-consuming and prone to human error. As cyber threats evolve, the need for rapid detection and response becomes critical. Automation in SOCs aims to address these challenges by leveraging advanced tools and technologies to streamline operations.

Wazuh, an open-source security monitoring platform, offers comprehensive capabilities for threat detection, compliance management, and incident response. By integrating Wazuh into SOC operations, organizations can automate routine tasks, enhance threat visibility, and improve response times. This project focuses on developing automation tools using Wazuh to enhance the efficiency and effectiveness of SOC operations. The primary goal is to streamline incident detection, analysis, and response processes, thereby reducing the time to detect and respond to security incidents.

Automation in SOCs not only improves operational efficiency but also allows security analysts to focus on more strategic tasks. By reducing the burden of manual processes, SOCs can better manage the increasing volume of security alerts and incidents. This project will explore the practical implementation of Wazuh for SOC automation, providing detailed methodologies and use cases to demonstrate its effectiveness.

LITERATURE SURVEY:

The automation of Security Operations Centers (SOCs) has become a critical focus in cybersecurity due to the increasing volume and sophistication of cyber threats. This section reviews key studies and data on SOC automation, with a particular emphasis on the use of Wazuh.

SOC Automation Overview

SOC automation involves the use of advanced tools and technologies to streamline and enhance the processes of threat detection, analysis, and response. Automation aims to reduce the manual workload on SOC analysts, improve response times, and minimize human error. According to a report by Gartner, by 2025, 50% of organizations will have integrated security orchestration, automation, and response (SOAR) capabilities into their SOCs, up from less than 10% in 2020[1].

Wazuh in SOC Automation

Wazuh is an open-source security monitoring platform that provides comprehensive capabilities for threat detection, compliance management, and incident response. It integrates with various tools to automate SOC workflows effectively. Key features of Wazuh include:

- **Real-time Threat Detection**: Wazuh can monitor and analyze security events in real-time, providing immediate alerts for suspicious activities[2].
- **Compliance Management**: Wazuh helps organizations comply with regulatory requirements by continuously monitoring and reporting on compliance status[3].
- **Incident Response**: Wazuh supports automated incident response actions, reducing the time to mitigate threats[4].
-

Case Studies and Practical Implementations

1. **Automated Threat Detection and Response**:
    - **Scenario**: A suspicious login attempt is detected outside of normal business hours.
    - **Implementation**: Wazuh detects the anomaly and triggers an alert. An automated script in Shuffle (a SOAR tool) isolates the affected system and notifies the SOC team for further investigation.
2. **Compliance Monitoring**:
    - **Scenario**: Ensuring compliance with GDPR by monitoring data access and usage.
    - **Implementation**: Wazuh continuously monitors file access logs and generates alerts for any unauthorized access. Automated workflows ensure that compliance reports are generated and reviewed regularly.
3. **Incident Response Automation**:
    - **Scenario**: A malware infection is detected on a workstation.
    - **Implementation**: Wazuh identifies the malware signature and triggers an automated response. The Hive (a case management tool) logs the incident, and Shuffle executes predefined scripts to quarantine the system and initiate malware removal procedures.
4. **Security Configuration Assessment**:
    - **Scenario**: Regularly assessing the security configurations of all endpoints.
    - **Implementation**: Wazuh performs scheduled scans to check for compliance with security policies. Non-compliant configurations trigger alerts and automated remediation actions.

Benefits of SOC Automation with Wazuh

- **Efficiency**: Automation reduces the time required for threat detection and response, allowing SOC analysts to focus on more strategic tasks.
- **Accuracy**: Automated processes minimize human error, ensuring consistent and reliable security operations.
- **Scalability**: SOC automation can handle increasing volumes of security events without a proportional increase in manual effort.

METHODOLOGY (Phrases):

The methodology for automating a Security Operations Center (SOC) using Wazuh involves several key phases:

1. **Requirement Analysis**:
    - Identify the specific needs and challenges of the SOC.
    - Define the scope and objectives of the automation project.
    - Gather input from SOC analysts and stakeholders to understand their pain points and requirements.
2. **Tool Selection and Configuration**:
    - Select Wazuh as the primary tool for security monitoring and automation.
    - Configure Wazuh to integrate with existing SOC tools and infrastructure.
    - Set up data collection agents on endpoints and servers to gather security event data.
3. **Automation Development**:
    - Develop scripts and workflows to automate routine SOC tasks such as threat detection, alerting, and incident response.
    - Use Wazuh's API and integration capabilities to create seamless workflows.
    - Implement automated playbooks for common security incidents.

4. **Testing and Validation**:
    - Conduct thorough testing of the automation scripts and workflows in a controlled environment.
    - Validate the accuracy and effectiveness of the automation tools.
    - Refine and optimize the automation processes based on feedback and test results.
5. **Deployment and Monitoring**:
    - Deploy the automation tools in the live SOC environment.
    - Continuously monitor the performance and effectiveness of the automation tools.
    - Make adjustments and improvements as needed to ensure optimal performance.
6. **Training and Documentation**:
    - Provide training for SOC analysts on the use of the new automation tools.
    - Develop comprehensive documentation for the automation processes and workflows.
    - Ensure that all team members are familiar with the new tools and procedures.
7. **Continuous Improvement**:
    - Regularly review and update the automation tools and processes.
    - Stay informed about new threats and advancements in SOC automation technology.

Incorporate feedback from SOC analysts to continuously improve the automation system

FACILITIES REQUIRED:

To successfully implement SOC automation using Wazuh, the following facilities are required:

1. **Hardware**:
    - **Servers**: High-performance servers to host Wazuh and other SOC tools.
    - **Workstations**: Computers for SOC analysts to monitor and respond to security incidents.
    - **Storage**: Sufficient storage capacity for logs, alerts, and other security data.
2. **Software**:
    - **Wazuh**: The primary security monitoring and automation platform.
    - **SIEM Systems**: Security Information and Event Management systems for centralized log management and analysis.
    - **SOAR Tools**: Security Orchestration, Automation, and Response tools like Shuffle for automating workflows.
    - **Case Management Tools**: Tools like The Hive for managing and tracking security incidents.
    - **Endpoint Agents**: Software agents installed on endpoints to collect and send security data to Wazuh.
3. **Network Infrastructure**:
    - **Secure Network Connections**: Reliable and secure network connections for data transmission between endpoints, servers, and SOC tools.
    - **Firewalls and IDS/IPS**: Network security devices to protect against unauthorized access and detect intrusions.
4. **Human Resources**:
    - **SOC Analysts**: Skilled personnel to monitor security alerts, analyze incidents, and respond to threats.
    - **Automation Developers**: Experts in scripting and automation to develop and maintain automated workflows.
    - **System Administrators**: Personnel to manage and maintain the hardware and software infrastructure.

5. **Training and Documentation**:
    - **Training Programs**: Comprehensive training for SOC analysts and automation developers on the use of Wazuh and other SOC tools.
    - **Documentation**: Detailed documentation of the automation processes, workflows, and tools to ensure smooth operation and maintenance.
6. **Security Policies and Procedures**:
    - **Incident Response Plans**: Well-defined procedures for responding to security incidents.
    - **Compliance Policies**: Policies to ensure adherence to regulatory requirements and industry standards.
    - **Continuous Improvement Processes**: Mechanisms for regularly reviewing and updating security policies and automation workflows.

REFERENCES:

1. **GitHub - uruc/SOC-Automation-Lab**. (2024). This repository provides practical examples and scripts for automating SOC operations using Wazuh. Retrieved from GitHub

2. **Certbar - TheHive & Wazuh: Streamlined Incident Management**. (2024). This article discusses the integration of TheHive and Wazuh for efficient incident management and response. Retrieved from Certbar

3. **Wazuh Documentation - Use Cases**. (2024). The official Wazuh documentation provides detailed use cases and implementation guides for various security scenarios. Retrieved from Wazuh Documentation

4. **GitHub - ibtesam5d/wazuh**. (2024). This repository includes configurations and scripts for deploying and managing Wazuh in a SOC environment. Retrieved from GitHub