Developing an Automated Incident Detection and Response System Using Open-Source Tool

**Slide 1: Title Slide**

* **Project Title:** Developing an Automated Incident Detection and Response System Using Open-Source SIEM Tools
* **Presented By:** [Student's Group]
* **Date:** [Date of Presentation]

**Slide 2: Introduction**

* **Overview:**
  + Importance of real-time incident detection and response in modern cybersecurity.
  + Role of SIEM (Security Information and Event Management) tools in automating incident detection and response.
* **Focus Tool:** **Wazuh** - an open-source SIEM tool for threat detection, integrity monitoring, incident response, and compliance.
* **Project Aim:** To create an automated system that can detect, analyze, and respond to security incidents using Wazuh in real-time.

**Slide 3: Project Objectives**

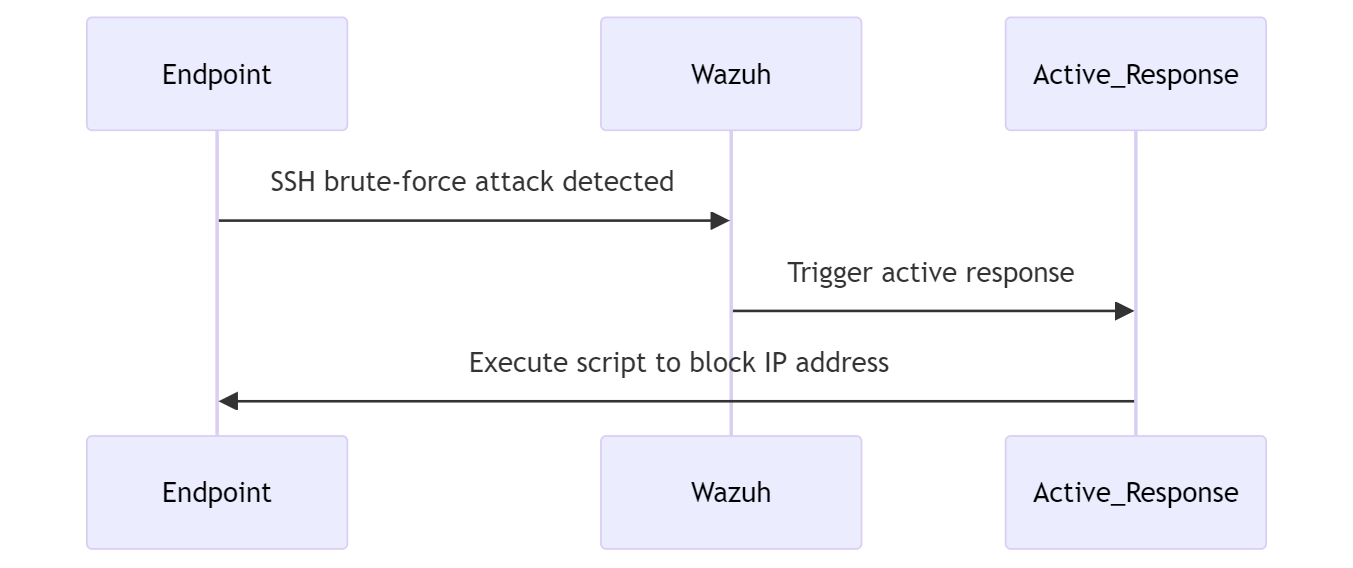
1. **Understand Wazuh Architecture:** Gain in-depth knowledge of how Wazuh collects, processes, and analyzes security data.
2. **Set Up Wazuh SIEM Environment:** Deploy Wazuh and integrate it with key data sources (e.g., system logs, network traffic)
3. **Automate Incident Detection:** Develop rules for detecting suspicious activities like unauthorized access, malware infections, and data exfiltration.
4. **Automate Incident Response:** Implement automated actions like isolating compromised endpoints, blocking malicious IPs, and generating alerts.
5. **Testing and Validation:** Simulate attack scenarios to test the effectiveness of the automated detection and response system.
6. **Documentation and Reporting:** Create a comprehensive report and playbook detailing system setup, incident scenarios, and response actions.

**Slide 4: Wazuh Overview**

* **What is Wazuh?**
  + Open-source security platform for threat detection, monitoring, and incident response.
  + Includes features like log analysis, file integrity monitoring (FIM), vulnerability detection, and security analytics.
* **Key Components:**
  + **Wazuh Agent:** Installed on monitored endpoints to collect logs and data.
  + **Wazuh Manager:** Processes data, applies detection rules, and generates alerts.
  + **Wazuh Dashboard:** Web interface for visualizing alerts and managing configurations.
* **Integration Capabilities:** Works with Elasticsearch and Kibana for enhanced search and data visualization.

**Slide 5: System Architecture**

* **Architecture Diagram:** Visual representation of the Wazuh deployment.
  + **Wazuh Agents** on endpoints (e.g., servers, workstations).
  + **Wazuh Manager** for data processing.
  + **Elasticsearch** for storing event data.
  + **Kibana Dashboard** for visualizing alerts and trends.
* **Data Flow:**
  + Agents collect security events → Data sent to Manager → Indexed in Elasticsearch → Analyzed and visualized in Kibana on Wazuh



**Slide 6: Setting Up the Environment**

* **Step-by-Step Process:**

1. **Deploy Wazuh Manager and Agents:** Installation and configuration.
2. **Integrate with Data Sources:** System logs, application logs.
3. **Enable Security Modules:** e.g vulnerability detection, and log analysis.

**Slide 7: Automated Incident Detection**

* **Custom Detection Rules:** Developing and implementing rules to detect:
  + Unusual login attempts.
  + **Brute force attacks.**
  + Malware signatures in logs.
  + Changes to critical system files.
* **Correlation with External Threat Feeds:** Using threat intelligence to enrich data and correlate with known indicators of compromise (IOCs).

**Slide 8: Automated Incident Response**

* **Predefined Response Actions:** Configuring automated actions like:
  + Isolating compromised endpoints.
  + **Blocking IP addresses associated with threats.**
  + Sending alerts via email or messaging platforms like Slack.
* **Using Wazuh's Active Response Module:** Automating the execution of scripts to mitigate threats.

**Slide 9: Testing and Validation**

* **Simulating SSH Attack Scenarios:** Simulate SSH attacks to test the system’s detection capabilities.
* **Monitoring Detection Accuracy:** Analyze how well Wazuh detects these incidents.
* **Response Evaluation:** Measure the speed and effectiveness of automated responses.

**Slide 10: Results & Analysis**

* **Key Findings of the Active Response. E.g Wazuh logs showing Blocked SSH Attempts**

**Slide 11: Lessons Learned**

* **Technical Skills Developed:** SIEM configuration, log analysis, rule development, and automation scripting.
* **Best Practices:** Importance of regular rule updates, testing in different environments, and continuously refining the system.

**Slide 12: Conclusion**

* **Summary of Project:** Recap of key achievements in building an automated incident detection and response system using Wazuh.
* **Key Takeaway:** Demonstrated how open-source tools can provide robust security solutions for real-time incident response.

**Slide 14: Q&A**

* **Questions and Discussion:** Open the floor for any questions from the audience.

Resources

* Blocking SSH brute-force attack with active response

<https://documentation.wazuh.com/current/user-manual/capabilities/active-response/ar-use-cases/blocking-ssh-brute-force.html>

* Threat Detection & Active Response With Wazuh

<https://www.youtube.com/watch?v=vJZAVZOIpfA>

* Blocking SSH brute-force attack with active response

<https://documentation.wazuh.com/current/user-manual/capabilities/active-response/ar-use-cases/blocking-ssh-brute-force.html>

* Auto Block Malicious IPs With Wazuh’s Active Response

<https://opensecure.medium.com/auto-block-malicious-ips-with-wazuhs-active-response-21603e653673>