

Introduction

In the current age, businesses of all sizes are being targeted and attacked using different techniques.[1] This has forced business to invest in proper cyber defence solutions, but not every company has the budget for these tools.

This project aimed to evaluate an Open-Source solution to determine its effectiveness for small businesses.

Aims and Objectives

The aim for this project was to implement a SIEM, Wazuh, and determine its effectiveness at detecting cyber-attacks.

The following objectives include:

- Configure and deploy an Open-Source solution in a virtual environment
- Simulate a range of common cyber-attacks on the network and virtual devices
- Analyse the collected data to determine the systems effectiveness

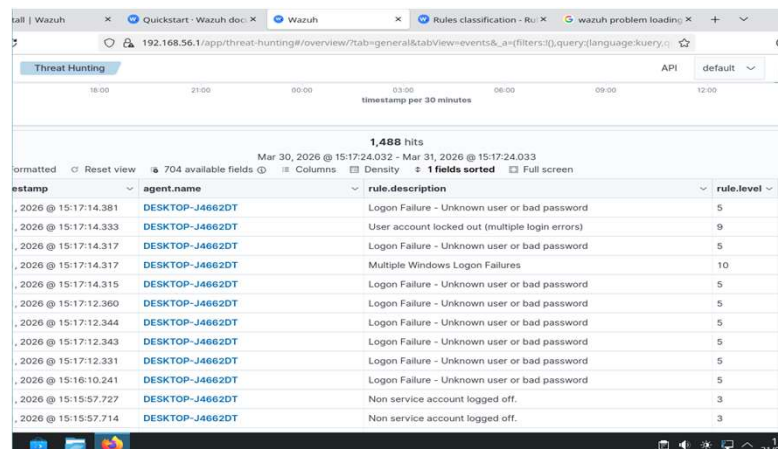
Methods

For this project, a positivist approach was employed using a deductive approach. This included using an experimental testing strategy to help effectively measure the strengths and weaknesses of the SIEM system chosen, Wazuh.

Design and Implementation

To effectively test Wazuh, a virtual environment was created using the platform VirtualBox to help simulate a virtual environment. This process including setting up several devices in an isolated network and doing basic configurations to ensure that attacks do not leave the environment.

The SIEM system itself was then setup on a server with the log collecting “agents” deployed on the rest of the devices. From there, several cyber attacks were introduced and the responses from the system were monitored.



timestamp	agent.name	rule.description	rule.level	ru
2026 @ 15:17:14.381	DESKTOP-J4662DT	Login Failure - Unknown user or bad password	5	66
2026 @ 15:17:14.333	DESKTOP-J4662DT	User account locked out (multiple login errors)	9	66
2026 @ 15:17:14.317	DESKTOP-J4662DT	Login Failure - Unknown user or bad password	5	66
2026 @ 15:17:14.317	DESKTOP-J4662DT	Multiple Windows Login Failures	10	66
2026 @ 15:17:14.315	DESKTOP-J4662DT	Login Failure - Unknown user or bad password	5	66
2026 @ 15:17:12.360	DESKTOP-J4662DT	Login Failure - Unknown user or bad password	5	66
2026 @ 15:17:12.344	DESKTOP-J4662DT	Login Failure - Unknown user or bad password	5	66
2026 @ 15:17:12.343	DESKTOP-J4662DT	Login Failure - Unknown user or bad password	5	66
2026 @ 15:17:12.331	DESKTOP-J4662DT	Login Failure - Unknown user or bad password	5	66
2026 @ 15:16:10.241	DESKTOP-J4662DT	Login Failure - Unknown user or bad password	5	66
2026 @ 15:15:57.727	DESKTOP-J4662DT	Non service account logged off.	3	67
2026 @ 15:15:57.714	DESKTOP-J4662DT	Non service account logged off.	3	67

Figure 1: Example of SIEM response to repeated authentication attempts

Results and Conclusions

The key findings from testing was that the SIEM was very effective at detecting any kind of system-level changes, including authentication-based attacks, file changes such as additions or deletion and potentially harmful account creation. Unfortunately, the base installation of Wazuh could not detect network-based attacks and relies on 3rd party integration for that ability.

The conclusions gathered from testing show that Wazuh is a great base system for detecting system changes, however coverage of network attacks requires integration with other tools like Suricata [2], which may not be suitable for certain small environments with limited resources to run and deploy these tools.

References

- [1] <https://www.gov.uk/government/statistics/cyber-security-breaches-survey-20252026/cyber-security-breaches-survey-20252026>
- [2] <https://wazuh.com/blog/responding-to-network-attacks-with-suricata-and-wazuh-xdr/>