



1. Introduction

This project was based on the use of Security Incident and Event Management (SIEM) tools and evaluating how useful they are in protecting networks.

SIEM tools allow the collection of logs from a variety of systems to be sent to the tool to be used/analysed in various ways.

These tools can support cloud systems alongside on-premise systems to provide security that fits everything.

Organisations still slack on security and SIEM tools should be a resource to invest in to protect their networks.

2. Aim & Objectives

- Evaluate how useful SIEM tools are.
- Test the impact of simulated attacks against systems supported by SIEM tools.
- Discuss the different configuration possibilities.
- Provide Recommendations for SIEM tool configurations.

3. Design

What will be needed?

- Host PC
- Virtualisation Software
- SIEM tool of choice
- Malware to simulate attacks

A host PC will be needed to run the virtualisation software needed to create a virtualised environment which allows simulated attacks to be performed without risking the outside network being affected.

The default settings in VirtualBox was used except for an increase in resource allocation to make the virtual machine run smoother.

Splunk Enterprise was the SIEM tool chosen and took a few attempts to set up. The tool is quite complex, which made configuration quite difficult.

Malware was chosen at random from "The-Malware-Repo" on GitHub, made by the user "Da2dalus". This malware was tested 5 times to ensure that the results are reliable and repeatable.

4. Results

The results show numerous things. Firstly, SIEM tools are incredible for intaking thousands of logs from a large number of systems and allowing to filter them down to a small number to pinpoint suspicious activity.

Next was the result of the simulated attacks. Splunk was able to detect each of the malware tested on every test. The addition of "Add-ons" within Splunk would allow for extreme depth of customisation to allow tailored SIEM configurations to fit an organisations needs.

The screenshot shows the Splunk search interface. The top bar indicates 3,916 events for the time range 3/16/24 10:00:00.000 PM to 3/17/24 10:57:57.000 PM. Below the search bar, there are tabs for Events (3,916), Patterns, Statistics, and Visualization. The search results show a single event with the source "WinEventLog:Security" and EventCode=4648. Below this, there is a table with 5 tests and 3 columns: AgentTesla, Whiter.A, and NoStart.

	AgentTesla	Whiter.A	NoStart
1st Test	Yes	Yes	Yes
2nd Test	Yes	Yes	Yes
3rd Test	Yes	Yes	Yes
4th Test	Yes	Yes	Yes
5th Test	Yes	Yes	Yes