National College of Ireland

# Configuration Manual

MSc Research Project
MSc Cybersecurity


## Parth Madhukar Shinde
Student ID: x23266571

School of Computing
National College of Ireland


Supervisor: Kamil Mahajan

**National College of Ireland**
**Project Submission Sheet**
**School of Computing**

| | |
|---|---|
| **Student Name:** | Parth Madhukar Shinde |
| **Student ID:** | x23266571 |
| **Programme:** | MSc Cybersecurity |
| **Year:** | 2024-25 |
| **Module:** | MSc Research Project |
| **Supervisor:** | Kamil Mahajan |
| **Submission Due Date:** | 31/08/2025 |
| **Project Title:** | Evaluating SIEM Solutions for Small and Medium Enterprises: A metric-focused Performance Study Identification |
| **Word Count:** | 987 |
| **Page Count:** | 8 |

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.

**ALL** internet material must be referenced in the bibliography section. Students are required to use the Referencing Standard specified in the report template. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action.

| | |
|---|---|
| **Signature:** | Parth Madhukar Shinde |
| **Date:** | 24th August 2025 |

## PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST:

| | |
|---|---|
| Attach a completed copy of this sheet to each project (including multiple copies). | ☐ |
| **Attach a Moodle submission receipt of the online project submission**, to each project (including multiple copies). | ☐ |
| **You must ensure that you retain a HARD COPY of the project**, both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer. | ☐ |

Assignments that are submitted to the Programme Coordinator office must be placed into the assignment box located outside the office.

| **Office Use Only** | |
|---|---|
| Signature: | |
| Date: | |
| Penalty Applied (if applicable): | |

# Configuration Manual

Parth Madhukar Shinde
x23266571

# 1 Introduction

The configuration manual completely documents the setup and implementation of four SIEM solutions, Wazuh, ELK, Huntress and LimaCharlie across Windows or Ubuntu. The aim of this manual is to provide the steps for replicating the environment used for performance evaluation of our research. Among the selected tools, Wazuh was deployed offline as a self-hosted instance, while Huntress, LimaCharlie and ELK were accessed from cloud-based portals. This guide includes installation, system configuration, data verification for each solution.

# 2 System Configuration

## 2.1 VirtualBox

*VirtualBox* (2025) VirtualBox was used to simulate both Windows and Linux systems in isolated environments. It was ensured that enough memory and resources were allocated to the systems for operations.

## 2.2 Internet access on VMs

Internet connectivity was required for downloading and updating agents and for communication with SIEM solutions hosted on cloud.

## 2.3 Windows 11 and Ubuntu ISO images

Fresh installation of Windows 11 Pro and Ubuntu 22.04 was configured. No additional applications were installed and snapshots of VMs were taken to restore after testing each SIEM, to maintain consistency across tests.

### 2.4 Virtual machine configurations

| Parameter | Windows System | Ubuntu System |
|---|---|---|
| OS Version | Windows 11 Pro | Ubuntu 22.04 LTS |
| RAM | 4 GB | 4 GB |
| CPU | 2 vCPU | 2 vCPU |
| Disk | 80 GB SSD | 60 GB SSD |
| Network | NAT + Host Adapter | NAT + Host Adapter |

Table 1: System Configuration for Virtual Machines

## 3 Tool Setup Overview

| Tool | Deployment Type | Tested OS | Test Types(*eicar.*; 2025) |
|---|---|---|---|
| Wazuh | Offline (self-hosted) | Windows and Ubuntu | EICAR anti-malware file |
| ELK Stack | Cloud hosted | Windows and Ubuntu | EICAR anti-malware file |
| Huntress | Cloud hosted | Windows Only | EICAR and Login brute-force |
| LimaCharlie | Cloud hosted | Windows and Ubuntu | EICAR anti-malware file |

Table 2: SIEM Tool Setup Summary

## 4 Configuration Steps

### 4.1 Wazuh (Offline - Self-hosted)(Wazuh; 2025)

#### 4.1.1 Environment

- Installed Wazuh on ubuntu virtual machine using ova file.
- Windows and Ubuntu endpoints were configured by installing Wazuh agents.

#### 4.1.2 Steps

- Installed Wazuh Manager, Server and Indexer using Ova file on Ubuntu server virtual machine.
- Configured the ossec.conf file for file integrity monitoring and virustotal integration.
- Installed agents using scripts on Windows and Ubuntu.
- Triggered the alert by downloading malicious EICAR file.

#### 4.1.3 Verification

- Wazuh detected eicar file download, which was visible on the wazuh dashboard.
- The MTTD and MTTR metrics noted


Figure 1: The image shows the detection of EICAR malware file on Ubuntu machine. This alert is categorized as File Integrity Monitoring, and included metadata such as file path and file hash. This verified the ability of Wazuh to monitor the endpoint's file systems in real-time

## 4.2 ELK Stack (*elastic*; 2025)

### 4.2.1 Environment

- Elastic Cloud (Free Tier Trial)

### 4.2.2 Steps

- Registered and deployed ELK Stack through Elastic cloud portal.
- Installed EDR Agent on Windows and Ubuntu through scripts.

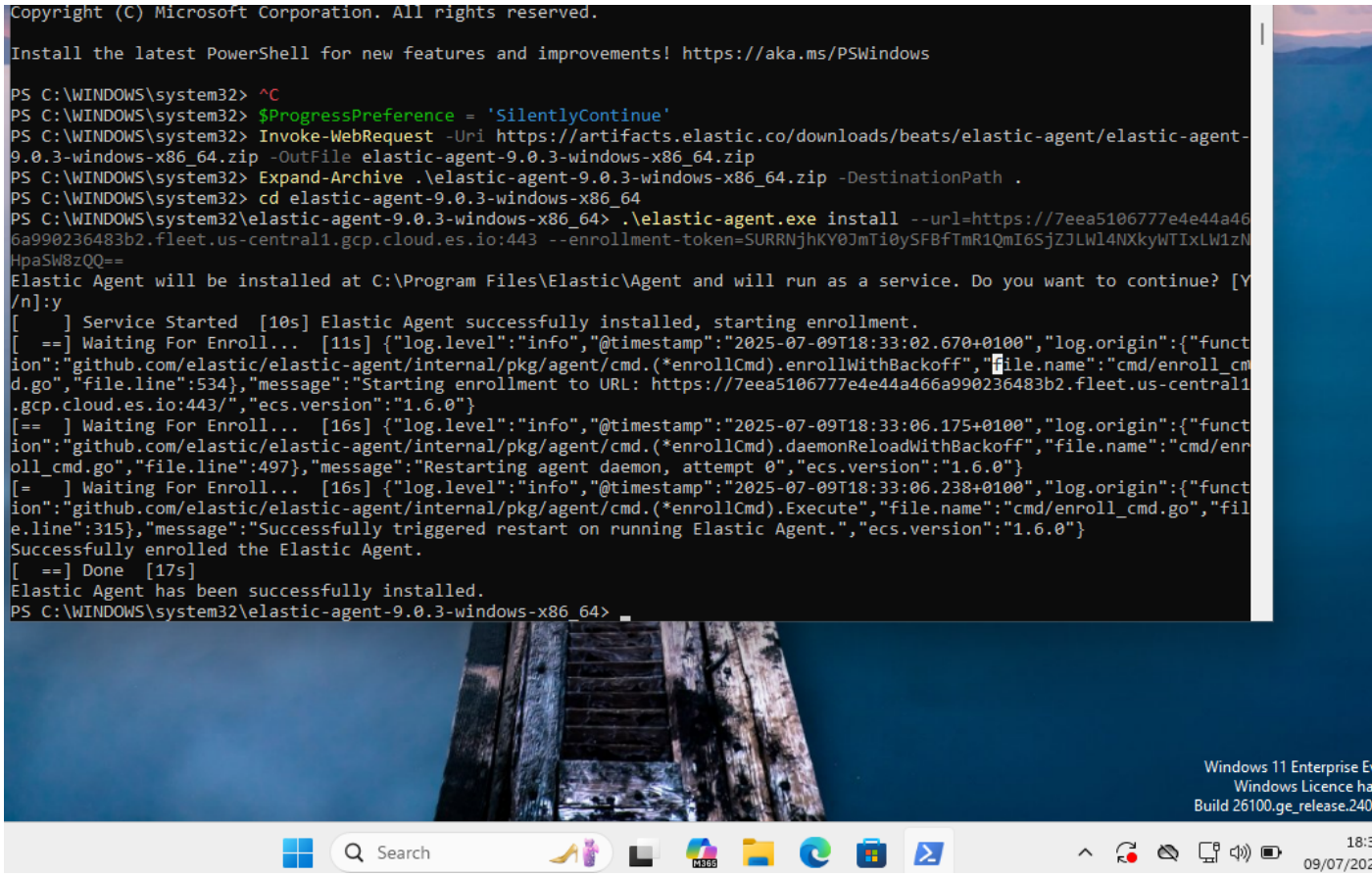


Figure 2: The image shows displays the Elastic Agent being downloaded and installed through powershell script on Windows machine. This involves the enrollment token and fleet server for secure registration. It is crucial when integrating Windows with ELK for monitoring.

- Connected the agents into fleet models by using enrollment tokens.

- Downloaded the EICAR test file, which triggered the EDR agent.

#### 4.2.3 Verification

- The alerts were triggered on Elastic EDR dashboard.
- The "Malware Prevention Alert" was observed on screen.

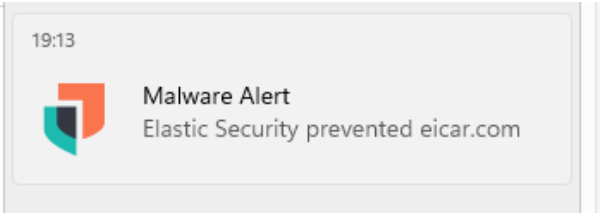


Figure 3: The Elastic EDR generated a "Malware Alert" on the endpoint. This detection reflected ELK's integration with Elastic agent for the policies. This triggered the alert which was correlated with file hash, process and file behaviour

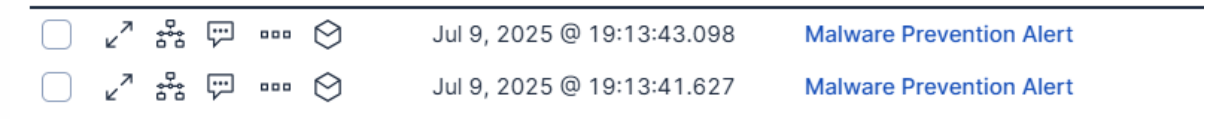


Figure 4: The log output captured the timing of event, including exact timestamps for when the EICAR file was detected. This helped to calculate MTTD and MTTR for ELK. These logs help further in real-world forensic analysis

### 4.3 Huntress (*huntress*; 2025)

#### 4.3.1 Environment

- Huntress Cloud portal via free subscription

#### 4.3.2 Steps

- Registered on the Huntress portal
- Installed Huntress agents on Window machine.
- Windows default antivirus was integrated.
- Alert was triggered through:
  1. Brute force login attempts
  2. EICAR file download.
- Logs viewed in dashboard.

### 4.3.3 Verification

- The alerts were triggered on Elastic EDR dashboard.
- The "Malware Prevention Alert" was observed on screen.

## 4.4 Huntress

### 4.4.1 Environment

- Huntress Cloud portal via free subscription

### 4.4.2 Steps

- Registered on the Huntress portal
- Installed Huntress agents on Window machine.
- Windows default antivirus was integrated.
- Alert was triggered through:
  1. Brute force login attempts
  2. EICAR file download.
- Logs viewed in dashboard.

### 4.4.3 Verification

- Login attempts and download of EICAR file was detected.
- The timestamps confirmed the significant delay in detection.

## 4.5 LimaCharlie (*limacharlie*; 2025)

### 4.5.1 Environment

- LimaCharlie Web UI

### 4.5.2 Steps

- Registered for LimaCharlie Free Trial
- Created sensors for Windows and Ubuntu with tag lc-system.
- Installed agents on Windows and Ubuntu system with a unique key for enrolment.
- Setup file monitoring rule on agents for "Downloads directory".

### 4.5.3 Verification

- The log showed "Action:Modified" for EICAR file download due to FIM.
- Process hash along with Process ID was captured for the activity.

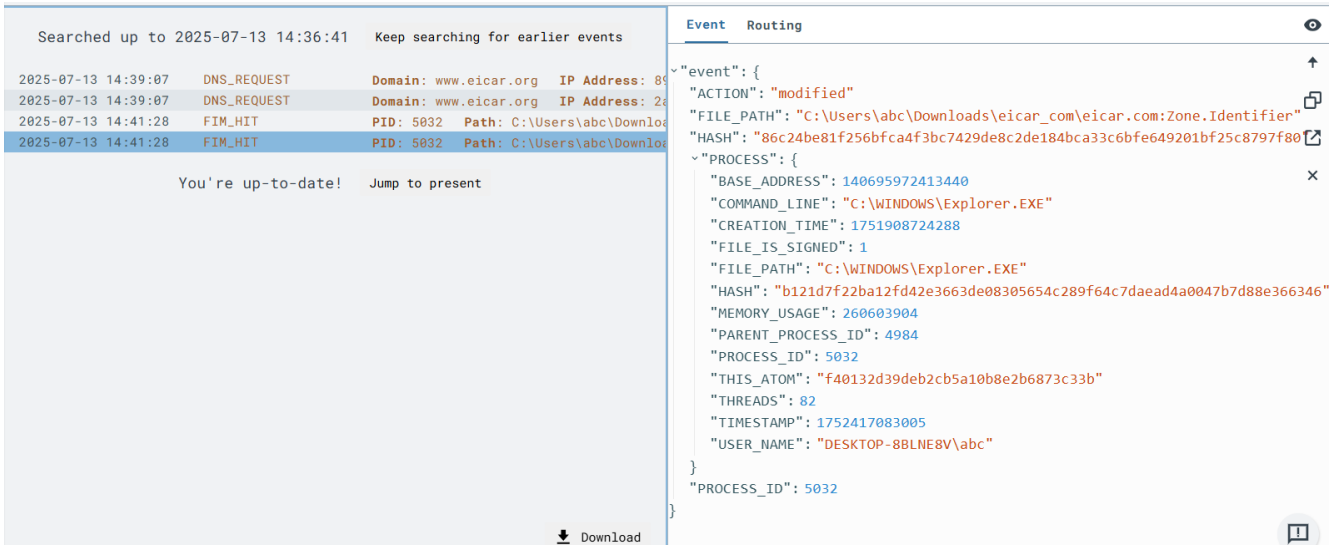


Figure 5: LimaCharlie detected the malware file on Windows. This detection included the file hash value, path and rule. This confirmed tool's usage for FIM


Figure 6: LimaCharlie detected the malware file on Linux machine. This detection included the file path, process id and rule. This confirmed tool's usage for FIM


Figure 7: This log shows the event generated when the EICAR file was downloaded on the machine. This data includes timestamp and path which helps to evaluate the MTTD and MTTR. This log can be used for SOC investigations

# 5 Logging Path and File Monitoring

## 5.1 Windows path for EICAR testing

- `C:\Users\abc\Downloads`

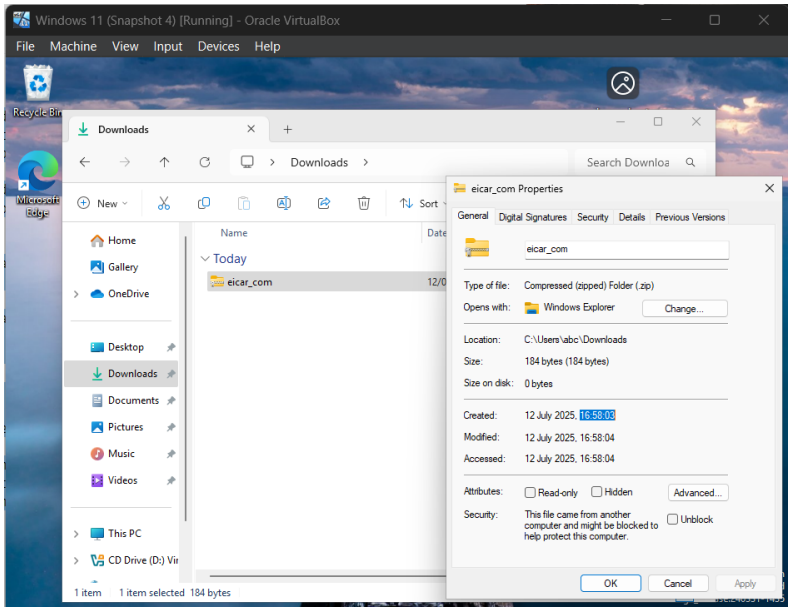


Figure 8: The screenshot shows the EICAR file being downloaded in Windows machine. This posed as a trigger after being unzipped for ELK, where for others the presence was detected and alerted. This file was used consistently to ensure standardization.

## 5.2 Linux path for EICAR testing

- `home/root1404/Downloads`

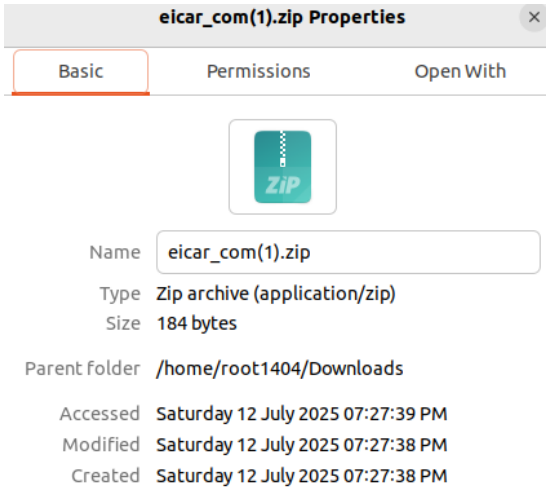


Figure 9: The image shows EICAR file being in the Downloads folder of Ubuntu machine. This process was repeated across all SIEM solutions to maintain uniformity

# 6 Tool Results

## 6.1 MTTD and MTTR Metrics

| Tool | OS | Test Type | MTTD (sec) | MTTR (sec) |
|---|---|---|---|---|
| Wazuh | Windows | EICAR | 4 | 177 |
| | Ubuntu | EICAR | 1 | 82 |
| ELK | Windows | EICAR | 46 | 115 |
| | Ubuntu | EICAR | 54 | 104 |
| Huntress | Windows | EICAR | 219 | 337 |
| | Windows | Login | 361 | 481 |
| LimaCharlie | Windows | EICAR | 122 | 122 |
| | Ubuntu | EICAR | 10 | 70 |

Table 3: Mean Time to Detect and Respond across SIEM Tools

## 6.2 Resource Utilization Comparison

| Tool | OS | CPU Usage | Memory Usage | Agent Disk Size |
|---|---|---|---|---|
| Wazuh | Windows | 8% | 14.2 MB | 55.2 MB |
| | Ubuntu | 0.5% | 62.7 MB | 26 MB |
| ELK | Windows | 6% | 450 MB | 661 MB |
| | Ubuntu | 0.5% | 315 MB | 830 MB |
| Huntress | Windows | 10% | 24 MB | 34.2 MB |
| LimaCharlie | Windows | 3% | 1.5 MB | 1.8 MB |
| | Ubuntu | 2% | 1.2 MB | 1.6 MB |

Table 4: Agent Resource Utilization for Each Tool

# References


*eicar.* (2025). `https://www.eicar.org/download-anti-malware-testfile/`. [Accessed 06-2025].

*elastic* (2025). `https://www.elastic.co/elastic-stack`. [Accessed 06-2025].

*huntress* (2025). `https://www.huntress.com/`. [Accessed 06-2025].

*limacharlie* (2025). `https://limacharlie.io/`. [Accessed 06-2025].

*VirtualBox* (2025). `https://www.virtualbox.org/`. [Accessed 05-2025].

Wazuh (2025). Wazuh, `https://documentation.wazuh.com/current/user-manual/capabilities/file-integrity/index.html`. [Accessed 02-08-2025].