

**Royaume du Maroc**  
**Université Mohammed Premier - Oujda**  
**École Nationale des Sciences Appliquées - Oujda**

**Speciality:** Information Security & Cyber Security

## Personal Security Project Report

Under the theme:

# Windows Endpoint Security Monitoring: Implementing Sysmon and Wazuh

**Realized by:**

AMAHROUK Asmae

**-2025-**

## Table of Contents

Table of Figures.....	2
Summary .....	3
1. Benefits and Outcomes: .....	3
2. Future Enhancements: .....	3
Introduction.....	4
1. Project Scope.....	4
2. Basic Concepts .....	4
a. EDR / XDR: .....	4
b. Endpoint Security Monitoring .....	5
3. Tools Utilized: .....	6
a. Sysmon (System Monitor): .....	6
b. Wazuh:.....	7
c. Elastic Stack (Elasticsearch, Logstash, Kibana): .....	7
4. Architecture .....	7
Chapter 1: Sysmon Installation.....	8
1. Introduction .....	8
2. Sysmon Installation on Windows .....	8
Chapter 2: Wazuh Installation .....	11
1. Introduction .....	11
2. Wazuh Manager Installation on Kali Linux.....	11
3. Wazuh Agent Installation on Windows.....	13
4. Connect Wazuh Agent with Wazuh Manager .....	14
Chapter 3: Integrate Sysmon with Wazuh.....	16
1. Wazuh Agent Configuration .....	16
2. Wazuh Manager Configuration .....	17
3. Results .....	18
Conclusion .....	20
Webography .....	21

## Table of Figures

Figure 1 : Wazuh & Sysmon Implementation Architecture .....	7
Figure 2 : Sysmon Installer.....	8
Figure 3 : Sysmon installer unzipped .....	9
Figure 4 : Install Sysmon configuration file .....	9
Figure 5 : Sysmon Installation .....	9
Figure 6 : Sysmon Successful installation message .....	10
Figure 7 : Sysmon functioning properly.....	10
Figure 8 : Wazuh Manager Installation.....	12
Figure 9 : Wazuh Manager Installed Successfully .....	12
Figure 10 : Wazuh Log In Web Interface .....	12
Figure 11 : Wazuh Web Interface.....	13
Figure 12 : Wazuh Agent Setup.....	13
Figure 13 : Wazuh Agent Setup 2 .....	14
Figure 14 : Wazuh Agent Configuration.....	14
Figure 15 : Wazuh Agent Configuration 2 .....	15
Figure 16 : Wazuh agent connectivity test on Wazuh Dashboard .....	15
Figure 17 : Modifying ossec.conf file .....	16
Figure 18 : Restart the Wazuh Agent on Windows .....	16
Figure 19 : Add new rules file in Wazuh.....	17
Figure 20 : Add Sysmon Alerts Rules in Wazuh.....	17
Figure 21 : Wazuh Manager restarting .....	18
Figure 22 : Sysmon alerts on Wazuh dashboard.....	18
Figure 23 : notepad process creation Sysmon alert on Wazuh Dashboard .....	19

## Summary

The primary goal of this project is to implement a comprehensive and scalable security monitoring solution for Windows endpoint. By leveraging **Sysmon** for advanced system activity logging and **Wazuh** for log aggregation, correlation, and analysis, this project aims to improve threat detection capabilities, support incident response, and enhance the overall security visibility within an organization's IT environment.

### 1. Benefits and Outcomes:

- **Improved Endpoint Visibility:** In-depth insights into endpoint behaviors and anomalies.
- **Real-Time Threat Detection:** Faster detection and response to suspicious activities.
- **Customizable Detection Rules:** Ability to define and update detection logic as threats evolve.
- **Centralized Monitoring:** Unified view of endpoint security events from all Windows systems.
- **Open-Source Cost Efficiency:** Achieved enterprise-grade monitoring using open-source tools without commercial licensing costs.

### 2. Future Enhancements:

- Integrate with Security Information and Event Management (SIEM) or SOAR platforms for automated incident response.
- Continuously update Sysmon configs and Wazuh rules based on threat intelligence feeds.
- Apply machine learning for anomaly detection over time.

# Introduction

In today's threat landscape, endpoint visibility is critical for detecting and responding to cyber threats. This project aims to enhance the security posture of Windows endpoints by implementing **System Monitor (Sysmon)** for detailed system activity logging and **Wazuh** for centralized log analysis, threat detection, and response. The combination offers a powerful and scalable solution for real-time endpoint monitoring and security event correlation.

## 1. Project Scope

- **Deployment of Sysmon** across Windows endpoint to capture detailed event logs including process creation, network connections, file changes, and more.
- **Configuration of Sysmon with a tailored configuration file** to reduce noise and focus on relevant security events.
- **Installation and integration of Wazuh agent** on Windows endpoint to collect and forward Sysmon logs.
- **Setup of Wazuh server/manager** on a Kali Linux VM for centralized log management, rule-based alerting, and dashboard visualization (via Kibana).
- **Implementation of custom detection rules and decoders** to enhance threat visibility based on organizational requirements.
- **Dashboard and report generation** for real-time monitoring and historical analysis.
- **Testing and validation of the system** to ensure accurate detection of suspicious behavior and response effectiveness.

## 2. Basic Concepts

### a. EDR / XDR:

- **Endpoint Detection and Response (EDR)** is a cybersecurity technology that monitors endpoint events and collects telemetry data. EDR solutions provide real-time analysis of user and device

activity, enabling security teams to detect malicious activity, investigate suspicious incidents, and respond to threats quickly.

- **Extended Detection and Response (XDR)** is a more recent security solution that extends the capabilities of EDR. It collects and automatically correlates data across multiple security layers – endpoints, network, email, servers, and cloud workloads – not just endpoints. By taking a more holistic approach, XDR provides a more comprehensive view of the threat landscape, allowing for faster detection and response.

Both EDR and XDR offer features that can significantly enhance an organization's security posture.

EDR tools typically feature:

- Threat hunting,
- Behavioral analysis, and
- Vulnerability assessment capabilities.

On the other hand, XDR not only incorporates these features but also adds:

- Network traffic analysis,
- Security information and event management (SIEM), and
- Cloud security capabilities.

In conclusion, both EDR and XDR offer robust security capabilities. While EDR focuses on endpoint security, XDR provides a more comprehensive security overview by integrating data from various sources.

#### b. Endpoint Security Monitoring

**Endpoint security monitoring** deals with the constant observation and analysis of devices connected to any organization's network, which includes computers, servers, and mobile devices. It aims to prevent, detect, and respond to potential cybersecurity threats before they might compromise the network.

The endpoint monitoring software provides an organization the ability to identify the users' behaviour, the system's performance, and all anomalies occurring in normal activities, hence further enhancing their cybersecurity.

Endpoint security monitoring is not something that businesses can afford to take lightly, as it plays a major role in many of the important functions an organization has, among them we mention:

- **Data Protection:** Since data is almost considered liquid gold in meaning for organizations, its security thereof automatically becomes very important.
- **Threat Detection and Response:** Endpoint security monitoring provides an organization with the relevant arsenal of early threat detection.
- **Compliance Assurance:** Continuous observation of endpoint activities makes endpoint security monitoring ensure compliance, confirming whether sensitive data has been managed appropriately.
- **Improved Control and Visibility:** Endpoint security monitoring allows the organization to extend its view and control of all the different devices connected to the network.

### 3. Tools Utilized:

#### a. Sysmon (System Monitor):



A Windows system service and driver from Microsoft Sysinternals that logs detailed system activity such as process creation, network connections, and file integrity events.

b. Wazuh:



An open-source security monitoring platform that integrates with Elastic Stack to provide log collection, threat detection, vulnerability detection, file integrity monitoring, and incident response capabilities.

c. Elastic Stack (Elasticsearch, Logstash, Kibana):



Used for indexing, searching, visualizing, and analyzing collected logs in real-time.

#### 4. Architecture

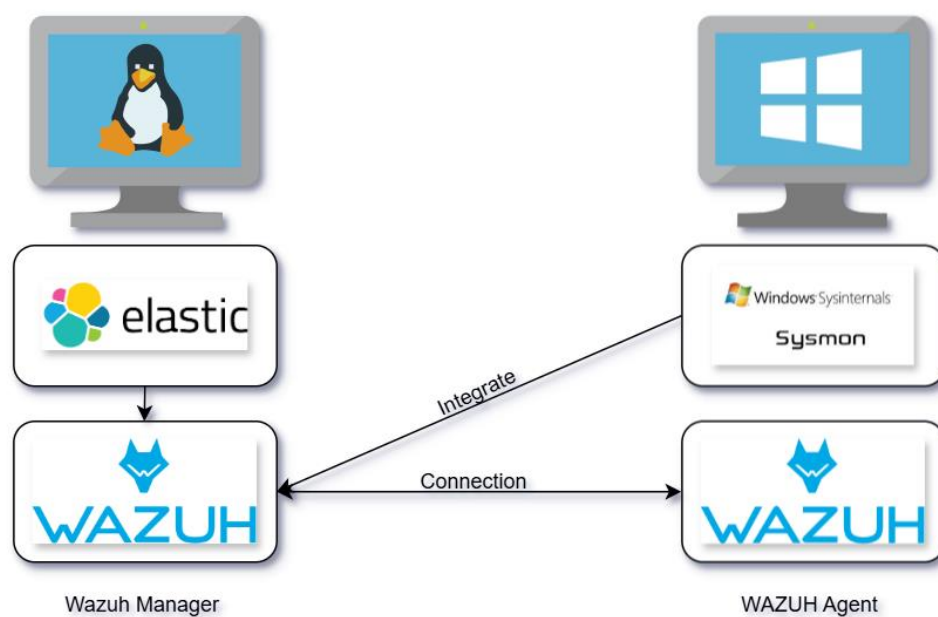


Figure 1 : Wazuh & Sysmon Implementation Architecture



# Chapter 1: Sysmon Installation

## 1. Introduction

**System Monitor (Sysmon)** is a Windows system service and device driver that, once installed on a system, remains resident across system reboots to monitor and log system activity to the Windows event log.

It provides detailed information about process creations, network connections, and changes to file creation time.

By collecting the events it generates using Windows Event Collection or SIEM agents and subsequently analyzing them, you can identify malicious or anomalous activity and understand how intruders and malware operate on your network.

## 2. Sysmon Installation on Windows

First of all, we have to download the **Sysmon installer** file from the [Microsoft Official Documentation](#), then unzip it.

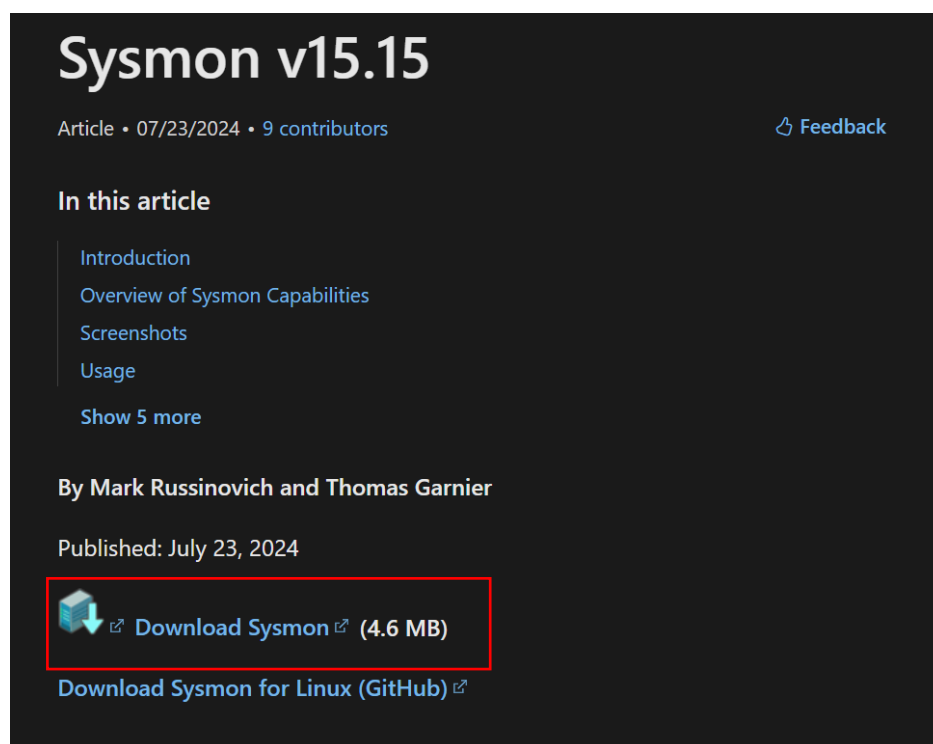


Figure 2 : Sysmon Installer

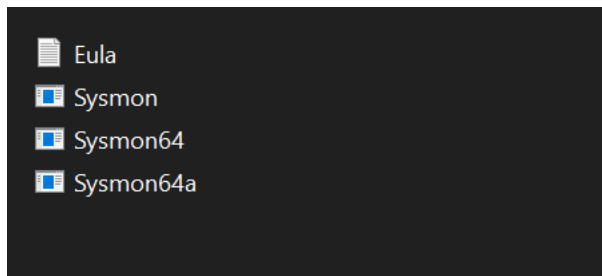


Figure 3 : Sysmon installer unzipped

Then, we have to download the **configuration file** which tells Sysmon which logs to collect, For this project I used this [configuration file](#).

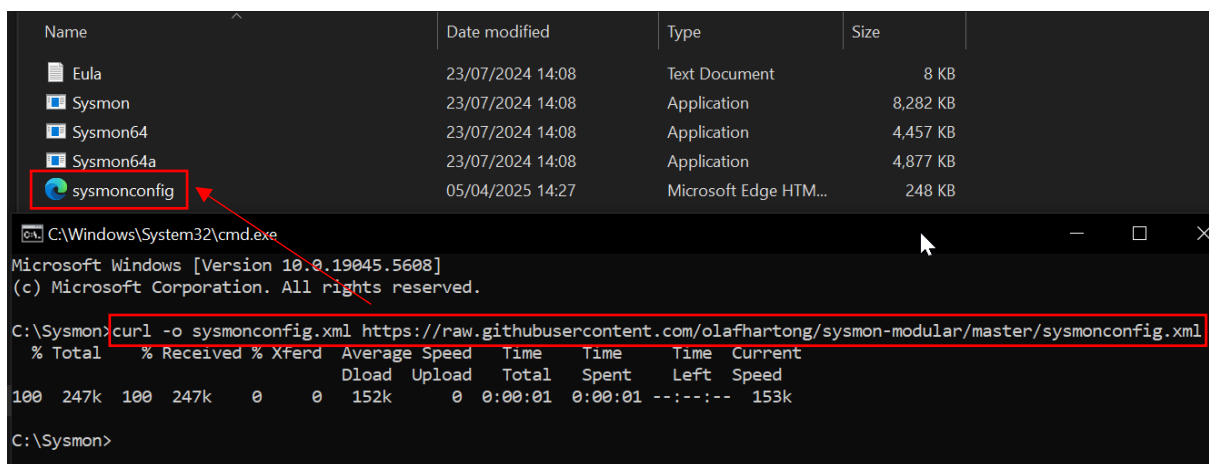


Figure 4 : Install Sysmon configuration file

Now, we have to run the **cmd.exe** as an Administrator in the directory where we have **Sysmon**, and execute the following command:

**sysmon64.exe -i sysmonconfig.xml**

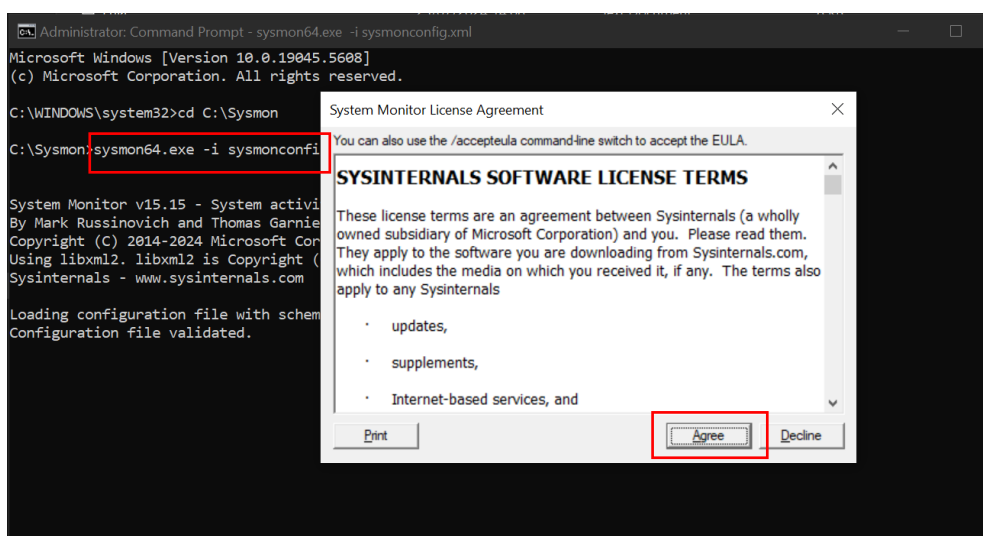


Figure 5 : Sysmon Installation

We should now get a Successful installation message.

```
C:\Sysmon>sysmon64.exe -i sysmonconfig.xml

System Monitor v15.15 - System activity monitor
By Mark Russinovich and Thomas Garnier
Copyright (C) 2014-2024 Microsoft Corporation
Using libxml2. libxml2 is Copyright (C) 1998-2012 Daniel Veillard. All Rights Reserved.
Sysinternals - www.sysinternals.com

Loading configuration file with schema version 4.90
Configuration file validated.
Sysmon64 installed.
SysmonDrv installed.
Starting SysmonDrv.
SysmonDrv started.
Starting Sysmon64..
Sysmon64 started.
```

Figure 6 : Sysmon Successful installation message

Now, to check that **Sysmon** is started and functioning, we will open the Event Viewer, navigate to **Application and Services** → **Microsoft** → **Windows**, we should find **Sysmon** → **Operational** under it.

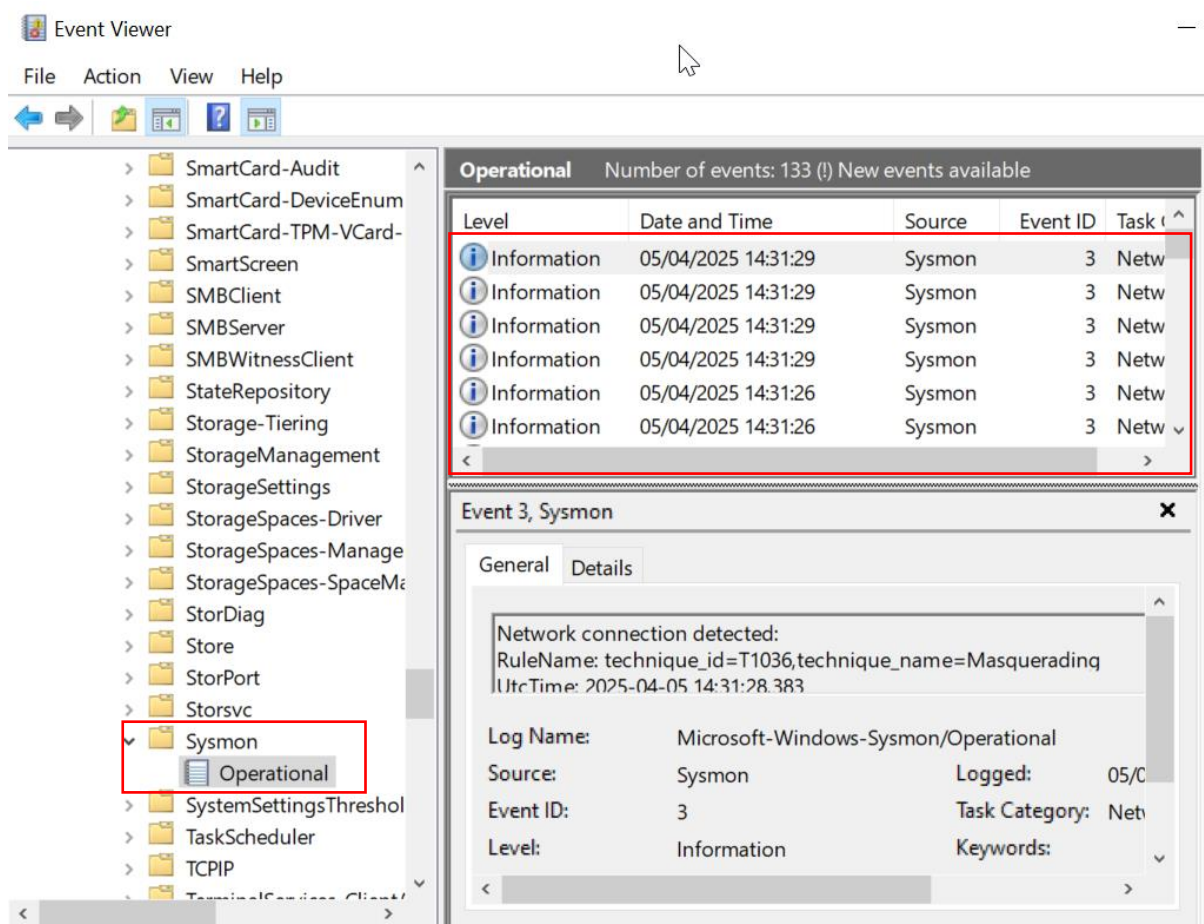


Figure 7 : Sysmon functioning properly

## Chapter 2: Wazuh Installation

### 1. Introduction

**The Wazuh platform** provides XDR and SIEM features to protect your cloud, container, and server workloads. These include log data analysis, intrusion and malware detection, file integrity monitoring, configuration assessment, vulnerability detection, and support for regulatory compliance.

The Wazuh solution is based on the **Wazuh agent**, which is deployed on the monitored endpoints, and on three central components: the **Wazuh server**, the **Wazuh indexer**, and the **Wazuh dashboard**.

- **Wazuh indexer:** This central component indexes and stores alerts generated by the Wazuh server.
- **Wazuh server:** analyzes data received from the agents. It processes it through decoders and rules, using threat intelligence to look for well-known indicators of compromise (IOCs).
- **Wazuh dashboard:** is the web user interface for data visualization and analysis.
- **Wazuh agents:** are installed on endpoints such as laptops, desktops, servers, cloud instances, or virtual machines. They provide threat prevention, detection, and response capabilities.

### 2. Wazuh Manager Installation on Kali Linux

We need to execute this command:

```
curl -sO https://packages.wazuh.com/4.11/wazuh-install.sh && sudo  
bash ./wazuh-install.sh -a
```

Which will install:

- Wazuh Manager (SIEM engine)
- Wazuh API
- Filebeat (for ELK integration)
- Kibana & Elasticsearch (for dashboards)

```
(kali@kali)~$ curl -sO https://packages.wazuh.com/4.11/wazuh-install.sh && sudo bash ./wazuh-install.sh -a
[sudo] password for kali:
05/04/2025 11:30:35 INFO: Starting Wazuh installation assistant. Wazuh version: 4.11.2 (x86_64/AMD64)
05/04/2025 11:30:35 INFO: Verbose logging redirected to /var/log/wazuh-install.log
05/04/2025 11:30:35 INFO: The recommended systems are: Red Hat Enterprise Linux 7, 8, 9; CentOS 7, 8;
05/04/2025 11:30:35 WARNING: The current system does not match with the list of recommended systems. T
05/04/2025 11:30:57 INFO: Verifying that your system meets the recommended minimum hardware requiremen
05/04/2025 11:30:57 INFO: Wazuh web interface port will be 443.
```

Figure 8 : Wazuh Manager Installation

Once the assistant finishes the installation, the output shows the access credentials and a message that confirms that the installation was successful.

```
05/04/2025 11:43:24 INFO: — Summary —
05/04/2025 11:43:24 INFO: You can access the web interface https://<wazuh-dashboard-ip>:443
    User: admin
    Password:
05/04/2025 11:43:24 INFO: Installation finished.
```

Figure 9 : Wazuh Manager Installed Successfully

Now we can access **Wazuh Dabsboard** and Use the credentials afforded to log in!

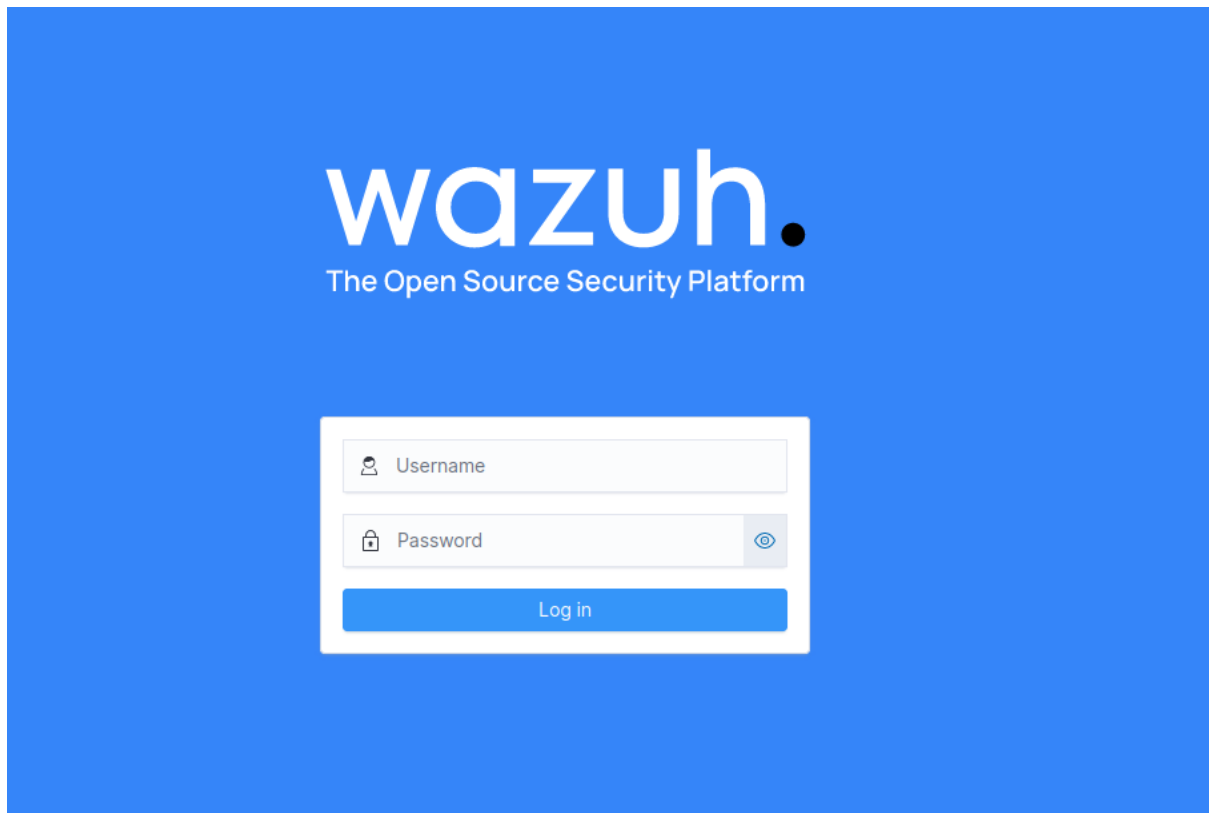


Figure 10 : Wazuh Log In Web Interface

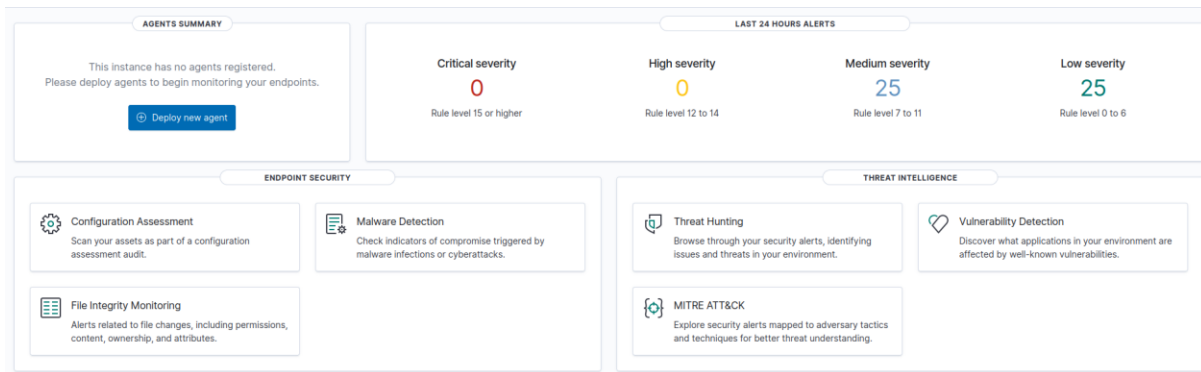


Figure 11 : Wazuh Web Interface

Now we need to add an agent so that we can monitor its state on **Wazuh DASHBOARD**.

### 3. Wazuh Agent Installation on Windows

Now we need to install the Wazuh Agent on the endpoint that we want to monitor, in our case it's our Windows endpoint.

To do so, we have to install firstly the windows installer from [this link](#), then execute it and follow the steps in the installation wizard.

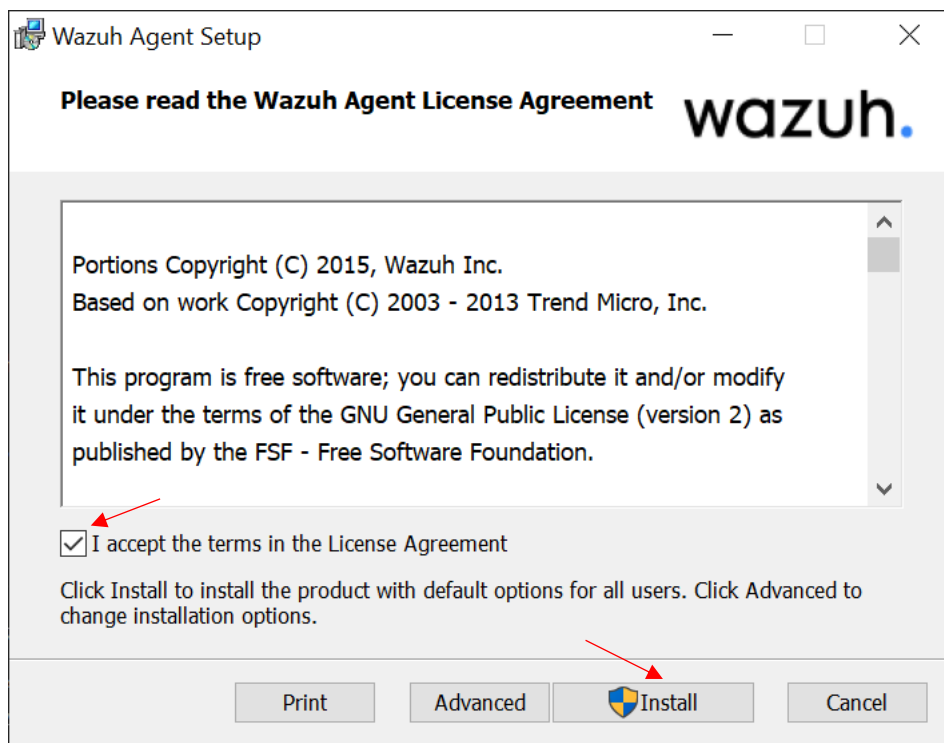


Figure 12 : Wazuh Agent Setup

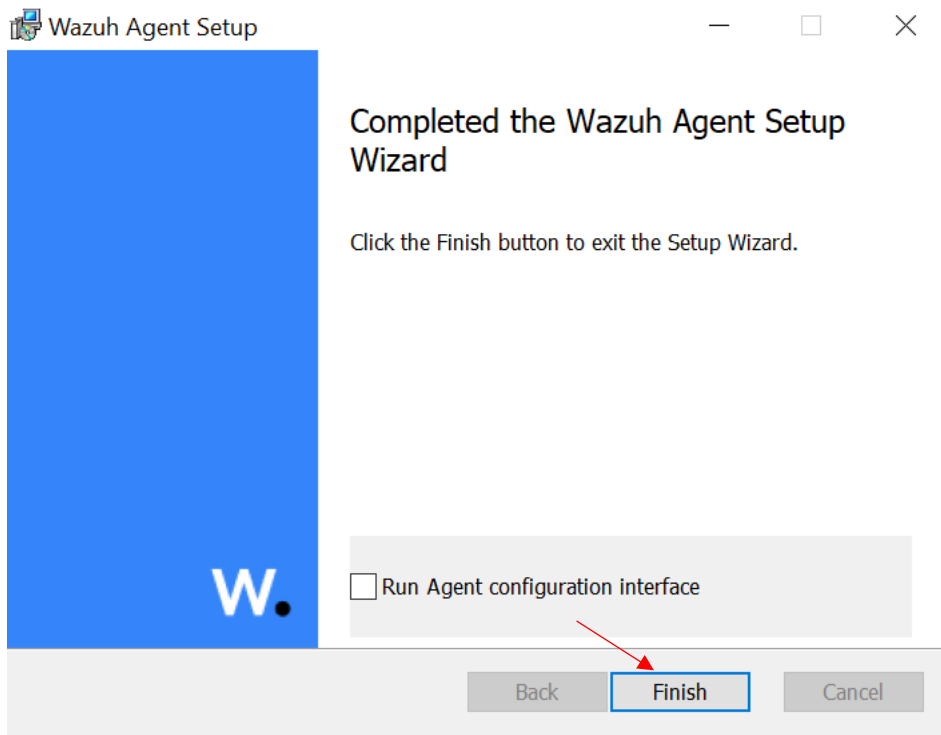


Figure 13 : Wazuh Agent Setup 2

#### 4. Connect Wazuh Agent with Wazuh Manager

Once installed, the agent uses a GUI for configuration.

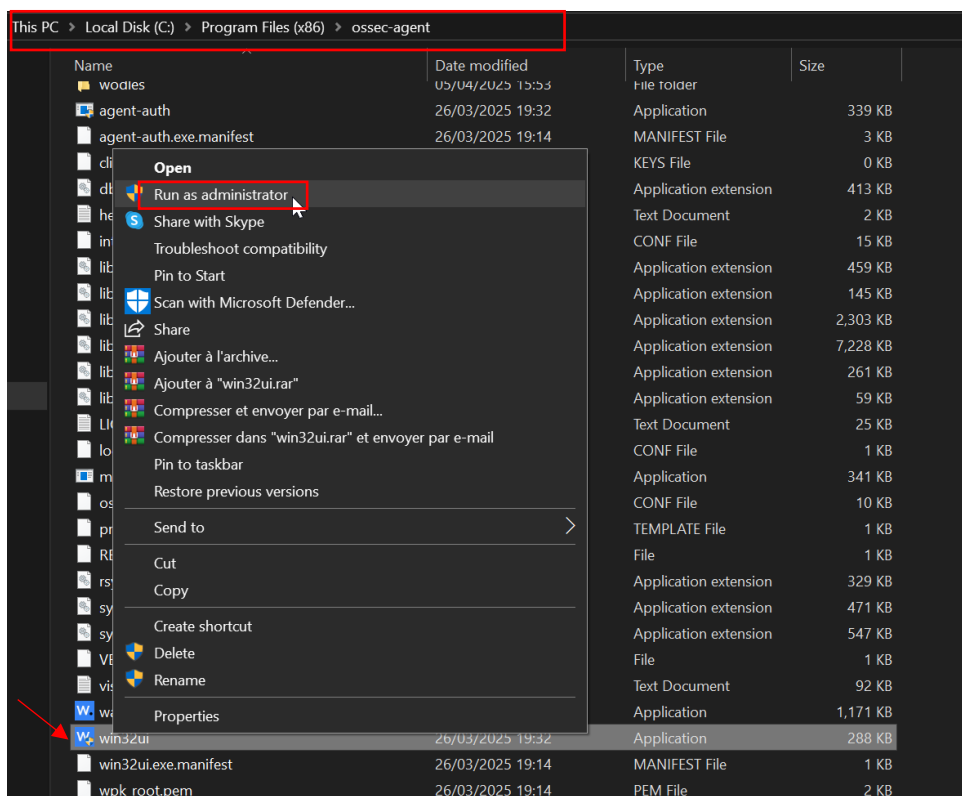
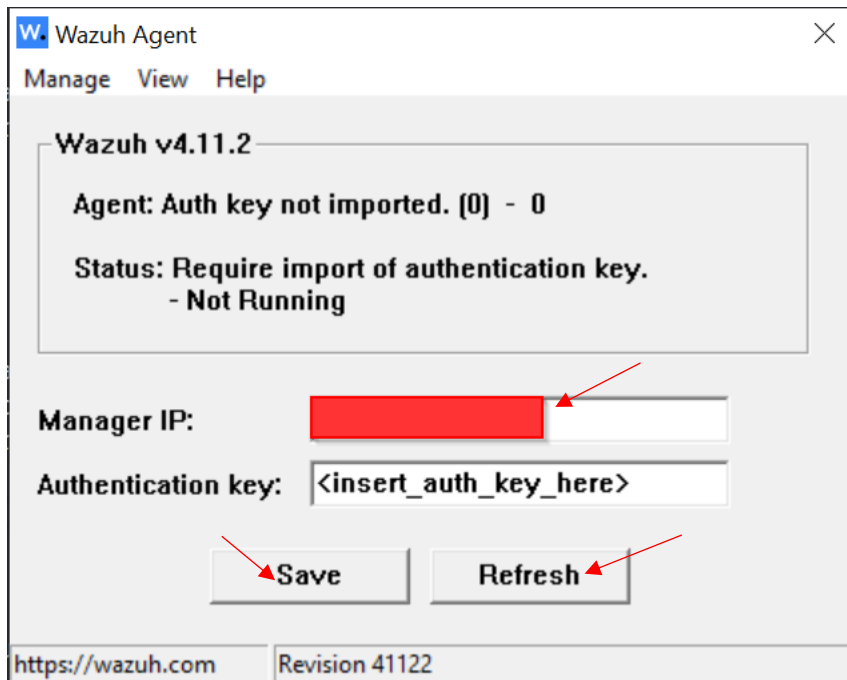


Figure 14 : Wazuh Agent Configuration

Now, we have to add **Wazuh Manager IP**, which is the IP address of the machine where **Wazuh Manager** is running, then **Save** and **Refresh**.



The image shows a 'Wazuh Agent' configuration window. At the top, it says 'Wazuh v4.11.2'. Below that, a message box states: 'Agent: Auth key not imported. [0] - 0' and 'Status: Require import of authentication key. - Not Running'. There are two input fields: 'Manager IP:' with a redacted IP address, and 'Authentication key:' with the placeholder '<insert\_auth\_key\_here>'. Below these fields are two buttons: 'Save' and 'Refresh'. Red arrows point to the 'Manager IP' field, the 'Save' button, and the 'Refresh' button. At the bottom, there is a footer with 'https://wazuh.com' and 'Revision 41122'.

Figure 15 : Wazuh Agent Configuration 2

Now to finalize the process, we have to start **Wazuh service** on the Windows machine by executing the following command:

***net start wazuhsvc***

After that, the agent (which is our Windows machine) should be active on our **Wazuh Dashboard**.

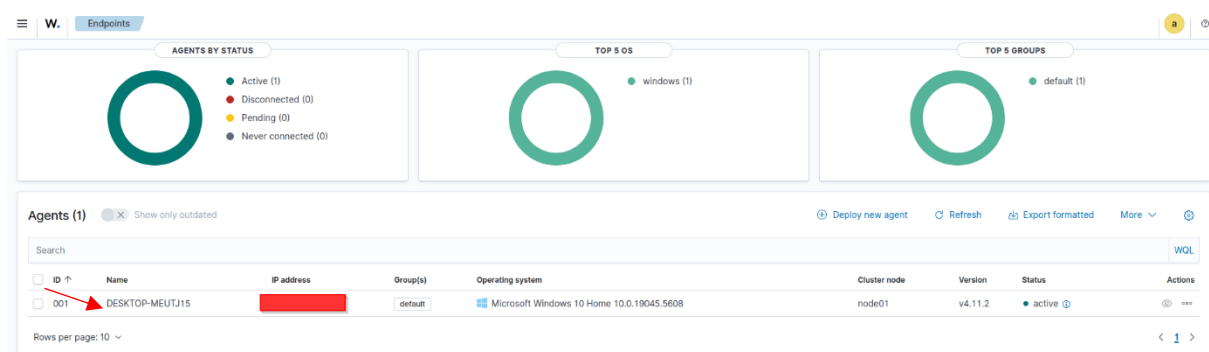


Figure 16 : Wazuh agent connectivity test on Wazuh Dashboard



## Chapter 3: Integrate Sysmon with Wazuh

Now after setting up both of **Sysmon** on Windows, **Wazuh Agent** on Windows and **Wazuh Manager** on Kali Linux, we have to integrate them so that **Wazuh** could monitor **Sysmon alerts** on its dashboard.

### 1. Wazuh Agent Configuration

It is necessary to tell this agent that we want to monitor **Sysmon events**. For that, we need to include this code as part of the configuration of the agent by modifying **ossec.conf** accordingly:

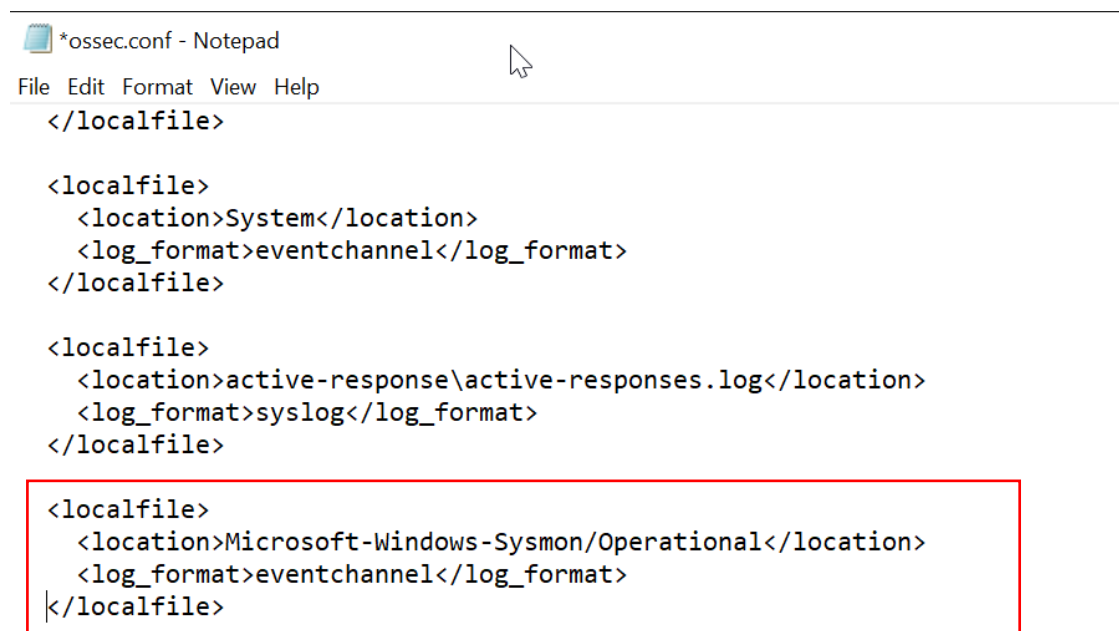


Figure 17: Modifying ossec.conf file

Save the changes, then restart the agent to apply the changes.

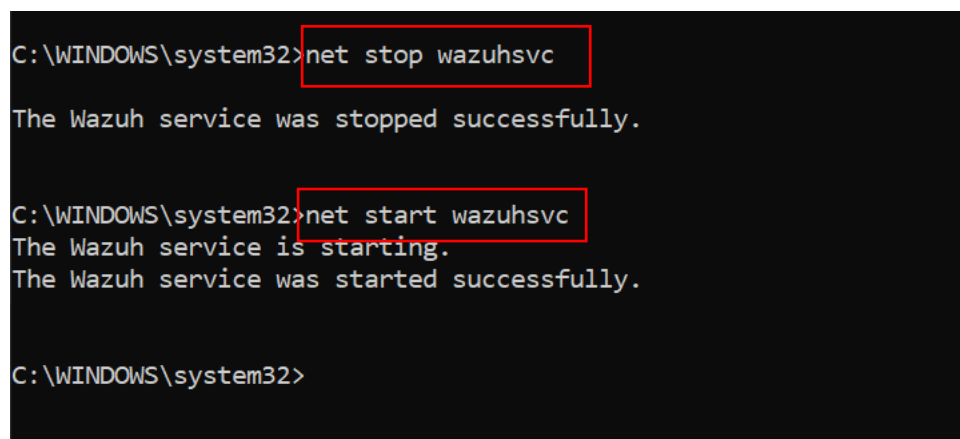
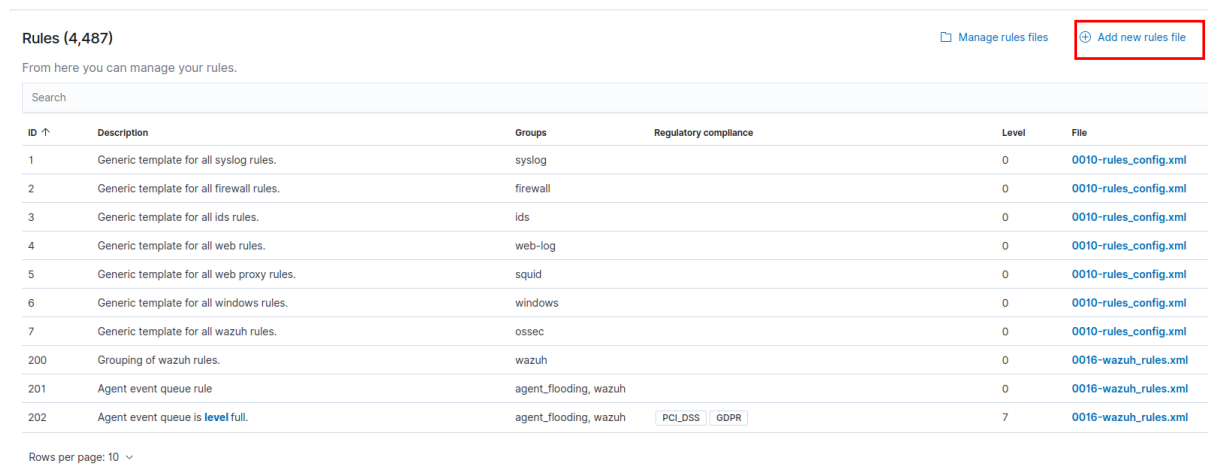


Figure 18: Restart the Wazuh Agent on Windows

## 2. Wazuh Manager Configuration

Go to

**‘Wazuh/Management/Rules/Manage\_rule\_files/custom\_rules/Add\_new\_rule\_file’**



Rules (4,487) Manage rules files Add new rules file

From here you can manage your rules.

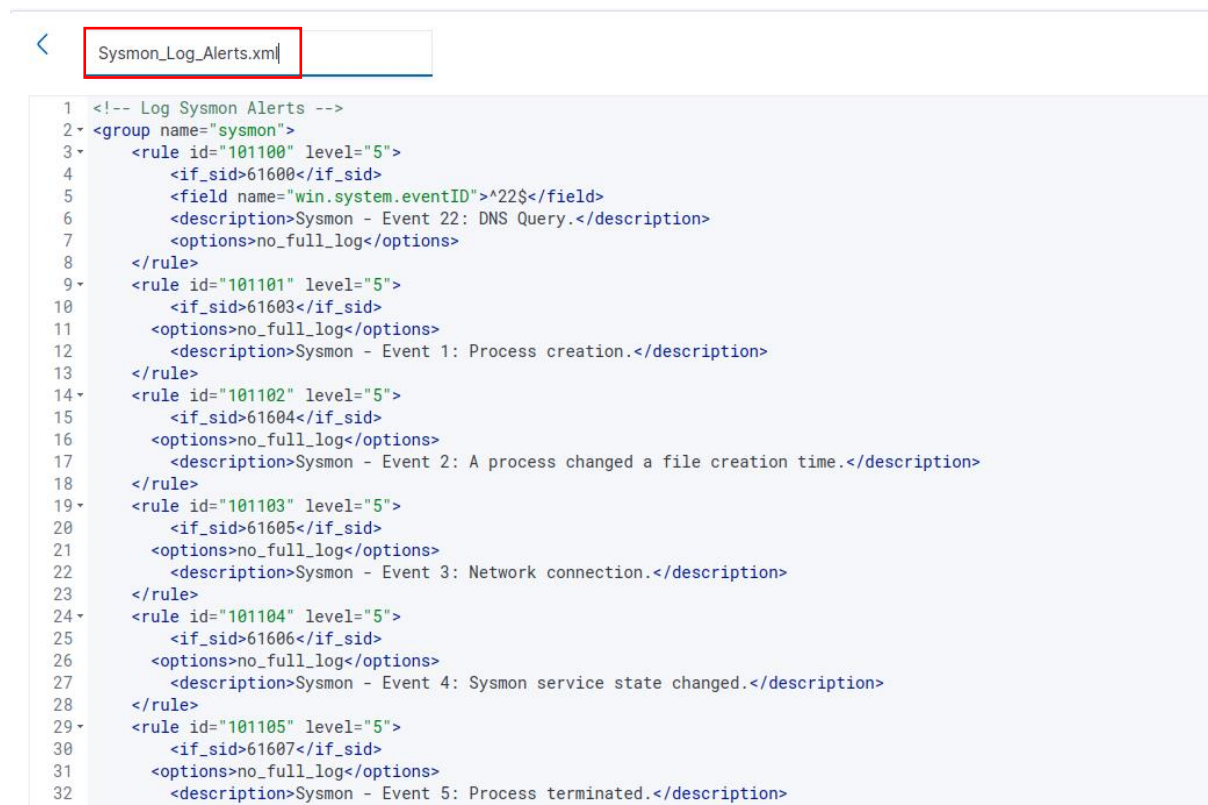
ID ↑	Description	Groups	Regulatory compliance	Level	File
1	Generic template for all syslog rules.	syslog		0	0010-rules_config.xml
2	Generic template for all firewall rules.	firewall		0	0010-rules_config.xml
3	Generic template for all ids rules.	ids		0	0010-rules_config.xml
4	Generic template for all web rules.	web-log		0	0010-rules_config.xml
5	Generic template for all web proxy rules.	squid		0	0010-rules_config.xml
6	Generic template for all windows rules.	windows		0	0010-rules_config.xml
7	Generic template for all wazuh rules.	ossec		0	0010-rules_config.xml
200	Grouping of wazuh rules.	wazuh		0	0016-wazuh_rules.xml
201	Agent event queue rule	agent_flooding, wazuh		0	0016-wazuh_rules.xml
202	Agent event queue is <b>level</b> full.	agent_flooding, wazuh	PCI_DSS   GDPR	7	0016-wazuh_rules.xml

Rows per page: 10

Figure 19 : Add new rules file in Wazuh

And then put your custom rules for Sysmon alerts, I used [this rules](#).

Put the rules in the **Wazuh file** and save it as an **XML** file as shown in the below images.



< Sysmon\_Log\_Alerts.xml

```
1 <!-- Log Sysmon Alerts -->
2 <group name="sysmon">
3   <rule id="101100" level="5">
4     <if_sid>61600</if_sid>
5     <field name="win.system.eventID">^22$</field>
6     <description>Sysmon - Event 22: DNS Query.</description>
7     <options>no_full_log</options>
8   </rule>
9   <rule id="101101" level="5">
10    <if_sid>61603</if_sid>
11    <options>no_full_log</options>
12    <description>Sysmon - Event 1: Process creation.</description>
13  </rule>
14  <rule id="101102" level="5">
15    <if_sid>61604</if_sid>
16    <options>no_full_log</options>
17    <description>Sysmon - Event 2: A process changed a file creation time.</description>
18  </rule>
19  <rule id="101103" level="5">
20    <if_sid>61605</if_sid>
21    <options>no_full_log</options>
22    <description>Sysmon - Event 3: Network connection.</description>
23  </rule>
24  <rule id="101104" level="5">
25    <if_sid>61606</if_sid>
26    <options>no_full_log</options>
27    <description>Sysmon - Event 4: Sysmon service state changed.</description>
28  </rule>
29  <rule id="101105" level="5">
30    <if_sid>61607</if_sid>
31    <options>no_full_log</options>
32    <description>Sysmon - Event 5: Process terminated.</description>
```

Figure 20 : Add Sysmon Alerts Rules in Wazuh

Now we need to restart the **Wazuh manager** to apply changer.

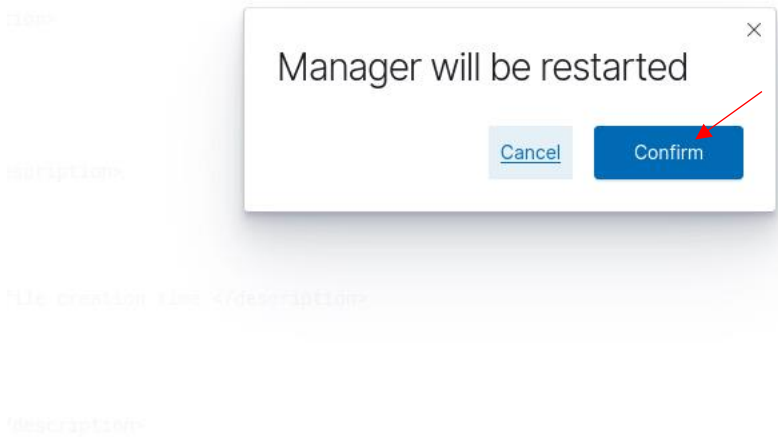


Figure 21 : Wazuh Manager restarting

Now, everything is setup and **Wazuh** can receive **Sysmon** alerts to monitor Windows endpoint security state.

### 3. Results

In the Wazuh Dashboard, after searching on Sysmon, we get Sysmon alerts from the Windows endpoint.

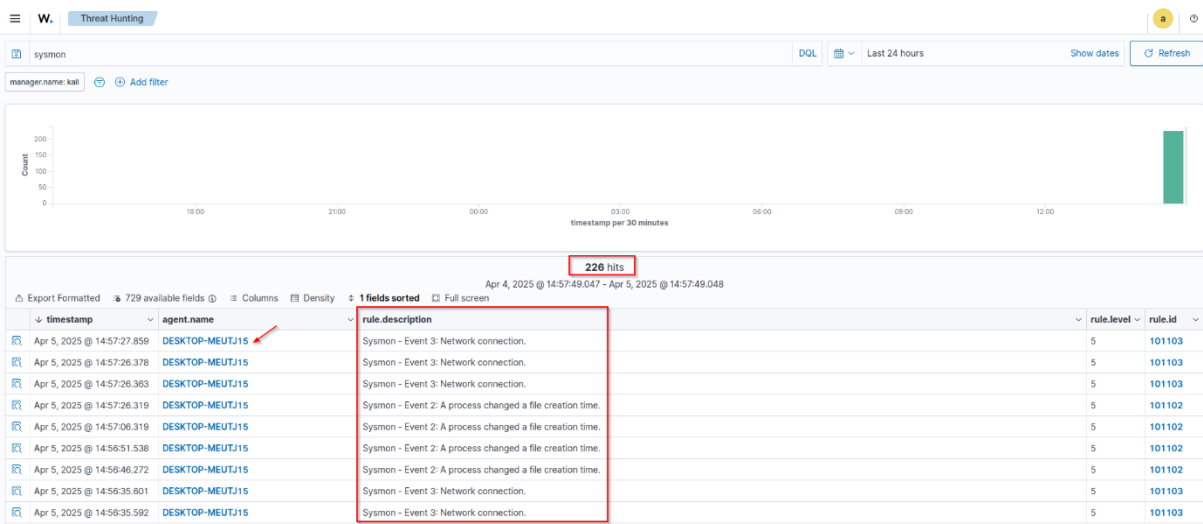


Figure 22 : Sysmon alerts on Wazuh dashboard

We will open **notepad.exe** on Windows to see if the alert will be captured by **Sysmon** and sent to **Wazuh manager** to be listed on **Wazuh Dashboard**.

And as results we have:

Table	JSON
† _index	wazuh-alerts-4.x-2025.04.05
† agent.id	001
† agent.ip	[REDACTED]
† agent.name	DESKTOP-MEUTJ15
† data.win.eventdata.commandLine	"C:\\WINDOWS\\system32\\notepad.exe" ←
† data.win.eventdata.company	Microsoft Corporation
† data.win.eventdata.currentDirectory	C:\\Users\\asmae\\
† data.win.eventdata.description	Notepad
† data.win.eventdata.fileVersion	10.0.19041.5553 (WinBuild.160101.0800)
† data.win.eventdata.hashes	[REDACTED]
† data.win.eventdata.image	C:\\Windows\\System32\\notepad.exe
† data.win.eventdata.integrityLevel	Medium
† data.win.eventdata.logonGuid	{b23d2b99-6bd2-67f0-8e0f-260c00000000}
† data.win.eventdata.logonId	0xc260f8e
† data.win.eventdata.originalFileName	NOTEPAD.EXE
† data.win.eventdata.parentCommandLine	C:\\WINDOWS\\Explorer.EXE

Figure 23 : notepad process creation Sysmon alert on Wazuh Dashboard

## Conclusion

This project, titled “**Windows Security Monitoring: Implementing Sysmon and Wazuh,**” set out to enhance the visibility and detection capabilities of a Windows-based system using open-source tools. The primary objective was to leverage Sysmon for detailed, host-level event logging and integrate it with the Wazuh EDR platform for centralized analysis and alerting. The outcome of this integration was a lightweight yet powerful monitoring solution that enables real-time security insights into endpoint activity.

During the course of the project, Sysmon was successfully deployed on a Windows system using a robust configuration designed to capture critical events such as process creation, network connections, file modifications, and registry changes. On the other side, Wazuh Manager, accompanied by the necessary ELK components—Elasticsearch, Logstash/Filebeat, and Kibana—was installed on a Linux machine to serve as the central analysis and visualization hub. The Wazuh agent was configured on the Windows host, enabling secure communication with the manager and continuous forwarding of Sysmon logs.

Special attention was given to configuring the Wazuh agent on Windows to collect logs directly from the Event Channel used by Sysmon, ensuring that all relevant security events were captured and parsed correctly.

Overall, the project successfully demonstrated how a free and open-source stack can be used to build a real-time Windows monitoring solution with high visibility into endpoint events. It lays a strong foundation for more advanced detection and response capabilities, and it serves as a model that can be adopted and scaled across enterprise environments.

In conclusion, this project proves the effectiveness of Sysmon and Wazuh as a reliable, open-source monitoring stack for Windows environments. It equips security practitioners with a strong foundation for detecting, analyzing, and responding to threats, and offers numerous opportunities for future growth—ranging from automation and machine learning integration to cloud and hybrid deployment. With further refinement, this solution can evolve into a full-featured Endpoint Detection and Response (EDR) platform tailored to a wide range of operational and research environments.

## Webography

- What is Security Monitoring? <https://www.redzonetech.net/blog-posts/security-monitoring#:~:text=Security%20monitoring%20helps%20organizations%20identify,significantly%20reduce%20their%20security%20vulnerabilities.>
- Endpoint Security Monitoring: <https://www.sentinelone.com/cybersecurity-101/endpoint-security/endpoint-security-monitoring/>
- EDR vs XDR: <https://www.ninjaone.com/it-hub/endpoint-management/edr-vs-xdr-whats-the-difference/>
- Wazuh Components: <https://documentation.wazuh.com/current/getting-started/components/index.html>
- Sysmon Official Documentation: <https://learn.microsoft.com/en-us/sysinternals/downloads/sysmon>
- Sysmon Configuration File : <https://raw.githubusercontent.com/olafhartong/sysmon-modular/master/sysmonconfig.xml>
- Wazuh Official Documentation : <https://documentation.wazuh.com/current/quickstart.html>
- Wazuh Agent Installation Guide : <https://documentation.wazuh.com/current/installation-guide/wazuh-agent/wazuh-agent-package-windows.html>
- Wazuh Installation Guide : <https://medium.com/btech-engineering/getting-started-with-wazuh-installation-and-configuration-guide-7caac7d73e42>
- Using Wazuh to monitor Sysmon events: <https://wazuh.com/blog/using-wazuh-to-monitor-sysmon-events/>
- Wazuh | Host Integration & Log Collection: <https://aliahmeddarhere.medium.com/wazuh-host-integration-log-collection-a8b1175ae1f4>
- Sysmon Integration with WAZUH: <https://systemweakness.com/sysmon-integration-with-wazuh-1742cf3805b7>
- Wazuh Sysmon rules file: <https://github.com/OpenSecureCo/Wazuh/blob/main/sysmon.xml>