Wazuh in

SIEM

**Group** **1**

Contents

### 01 02

##### Introduction In depth

Overview about Wazuh

and SIEM

### 03

##### Demo

Performing attack, monitor and alert

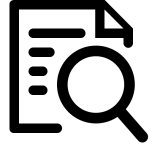
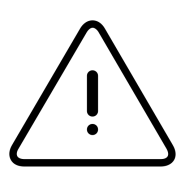
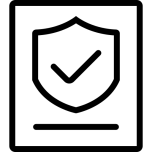
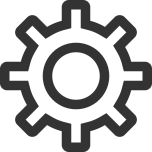
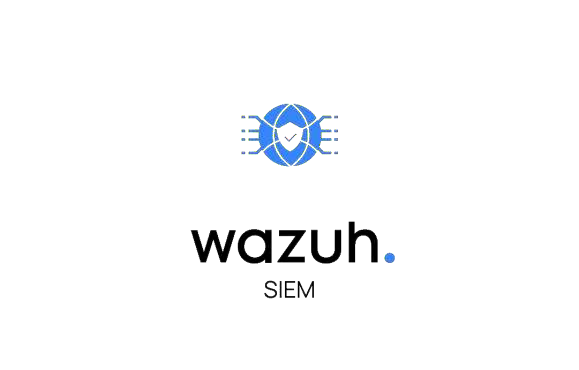
Wazuh architecture

# 01

## Introduction

Overview about Wazuh

#### Introduction

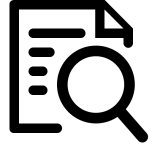
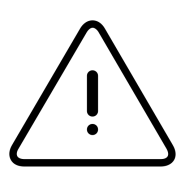
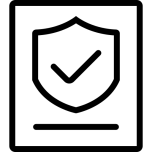
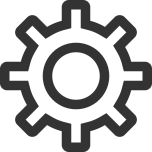
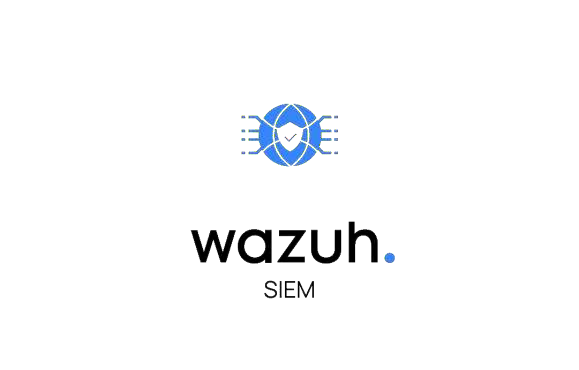


###### SIEM (Security Information and Event Management)

📫 Centralized platform

📫 Help organizations detect, analyze and respond to security threats before they harm business operations

#### Introduction



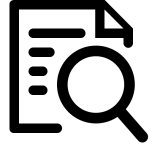
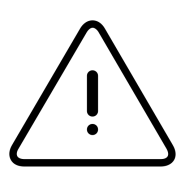
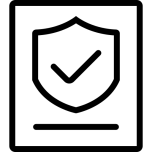
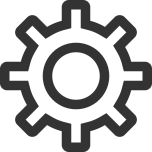
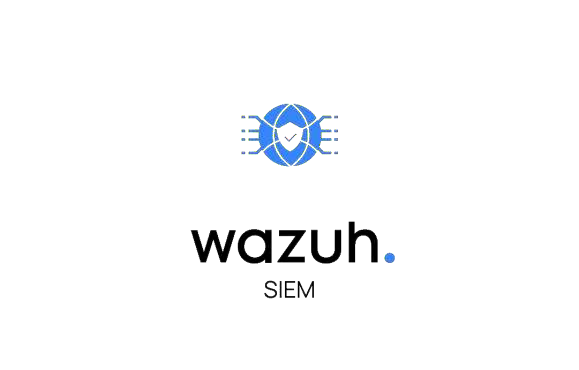
###### Capabilities & Features

SIEM systems vary in their capabilities but

generally offer these core functions:

* Log management
* Event correlation
* Incident monitoring and response

#### Introduction



###### Wazuh

📫 Open-source and free platform providing

ability of XDR and SIEM.

📫 Helps organizations and individuals to protect their data assets against security threats.

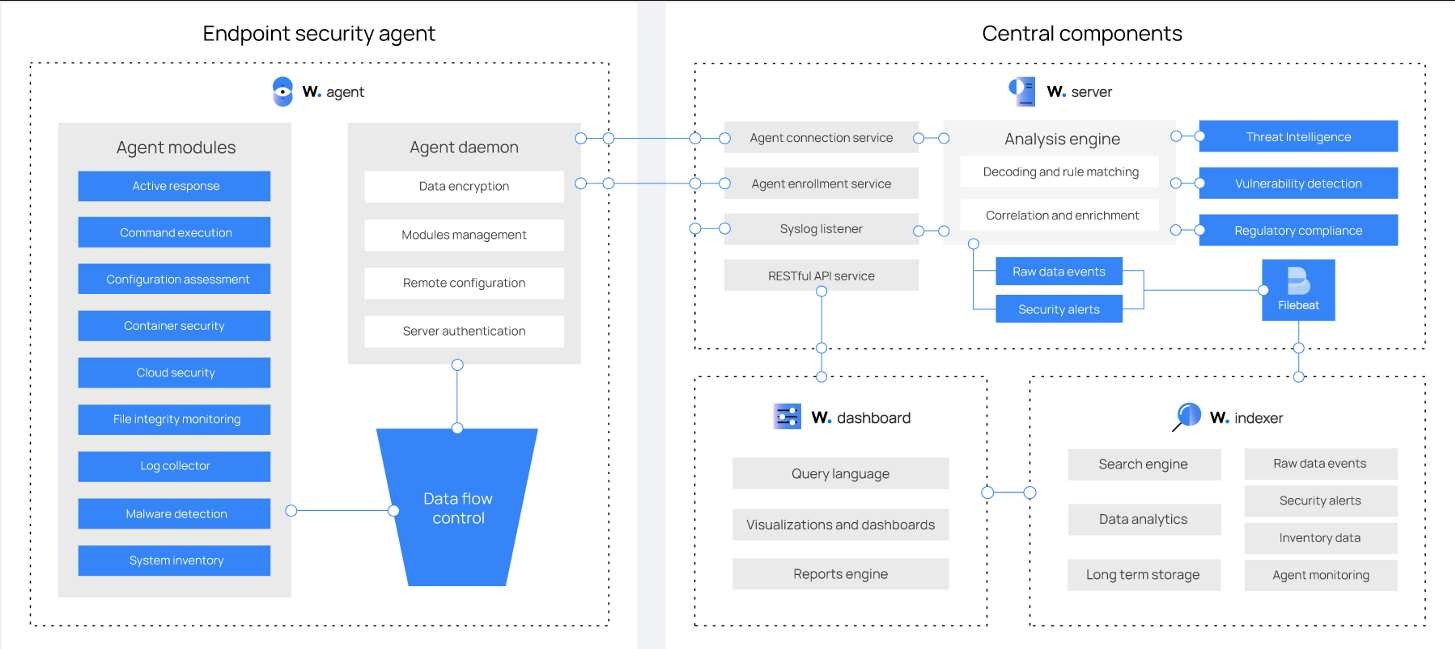
📫 It is widely used by thousands of organizations worldwide, from small businesses to large enterprises.

# 02

## In depth

Wazuh Architecture

#### In depth



Wazuh’s components

Wazuh solution is an agent-based platform, which is deployed on the monitored endpoints, and on three central components: Wazuh server; Wazuh indexer and Wazuh dashboard.

* **The** **Wazuh** **indexer** is a highly scalable, full-text search and analytics engine. This central

component indexes and stores alerts generated by the Wazuh server.

* **The** **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). A single server can analyze data from hundreds or thousands of agents, and scale horizontally when set up as a cluster. This central component is also used to manage the agents, configuring and upgrading them remotely when necessary.

#### Wazuh’s components

Wazuh solution is an agent-based platform, which is deployed on the monitored endpoints, and on

three central components: Wazuh server; Wazuh indexer and Wazuh dashboard.

* **The** **Wazuh** **dashboard** is the web user interface for data visualization and analysis. It includes out-of-the-box dashboards for threat hunting, regulatory compliance (e.g., PCI DSS, GDPR, CIS,

HIPAA, NIST 800-53), detected vulnerable applications, file integrity monitoring data, configuration assessment results, cloud infrastructure monitoring events, and others. It is also used to manage Wazuh configuration and to monitor its status.

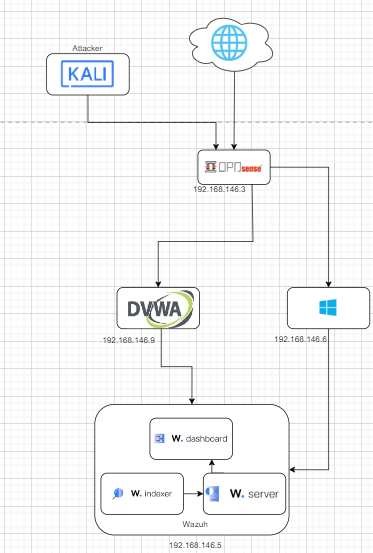
* **The** **Wazuh** **agent** runs on Linux, Windows, MacOS,… The agent helps to protect your system by

providing threat prevention, detection, and response capabilities. It is also used to collect different types of system and application data that it forwards to the Wazuh server through an encrypted and authenticated channel.

# 03

## Demo

Performing attack, monitor and alert



#### Demo

###### Environment

📫 DVWA (Wazuh Agent): Linux Mint 21.3

📫 Client: Windows 10

📫 Attacker: Kali Linux 2024.2

📫 Wazuh (Central components): RHEL 9.0

###### Malware

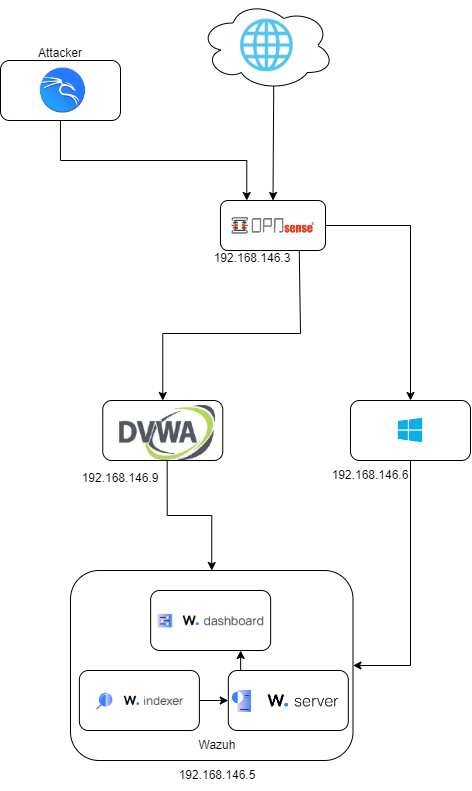
📫 Randsomeware : Kuiper

📫 Trojan: Njrate

📫 Remote access: Sysjoker

📫 Other: Mirai, Lightning Framework

#### Demo



###### Scenario

1. File integrity (1 vid)
2. CDB list (1 vid – Mirai )
3. Virus total integration (1 vid – Sysjoker)
4. Custom rules + Sysmon ( 4 vids – Sysjoker, Yara, Kuiper )

+ Configure rules: 1

5) + Result: 3

6) Yara intergration (3 vids – Njrat, Kuiper )+Configure:

1

7) + Result: 2

1. Audit ( Configure + Result - Yara )
2. Osquery ( 1 vid – Lighting Framework )

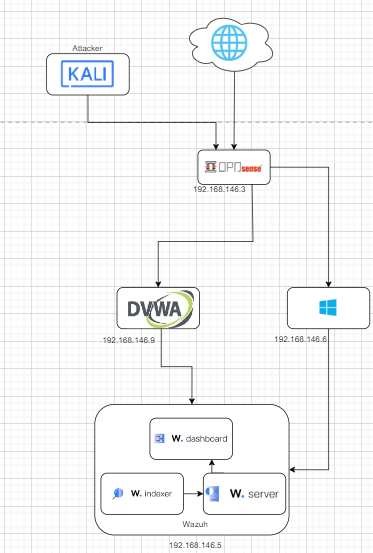
#### Demo

* + **Demo**
  + https://drive.google.com/drive/folders/1i6PIb8AOIhFdUxl-

JAPXjden9fS4cc1M?usp=sharing

Thank you for listening

#### Demo



###### Scenario

1. File integrity (1 vid)
2. CDB list (1 vid – Mirai )
3. Virus total integration (1 vid – Sysjoker)
4. Custom rules + Sysmon ( 4 vids – Sysjoker, Yara, Kuiper )

+ Configure rules: 1

5) + Result: 3

1. Yara intergration (3 vids – Njrat, Kuiper )
   1. Configure: 1
   2. Result: 2
2. Audit ( Configure + Result - Yara )
3. Osquery ( 1 vid – Lighting Framework )