



En cybersécurité aussi, le savoir n'a de valeur  
que si il est partagé.

In Cybersecurity too, knowledge only  
increases in value once shared.

# SIEM-EDR

## Disclaimer

### Disclaimer

The following demonstration is for educational purposes only.

We do not promote or encourage illegal activities.

Knowing your enemy is a half-won battle

La connaissance n'est réellement profitable que lorsqu'elle est partagée

# SIEM-EDR

## Agenda

1. What is a SIEM?
2. What is an EDR?
3. SIEM vs EDR
4. Example of an open source SIEM-EDR: Wazuh



An abstract network diagram on the left side of the slide, featuring a dense web of interconnected nodes and lines, forming a circular, globe-like structure.

# What is a SIEM?

# SIEM-EDR

## What is a SIEM?

- **Definition:** Overview of SIEM as a solution combining security information management (SIM) and security event management (SEM) to aggregate, analyze, and manage logs.
- **Key Functions:**
  - Real-time event monitoring and alerts.
  - Log aggregation and normalization.
  - Threat detection and incident response.
- **Benefits:** Improved security visibility, regulatory compliance, and rapid threat detection across a network.



# What is an EDR?

# SIEM-EDR

## What is an EDR?

- **Definition:** Overview of EDR, focusing on endpoint monitoring, detection, and response.
- **Core Functions:**
  - Continuous monitoring of endpoint activity.
  - Threat detection on endpoints (e.g., laptops, servers, mobile devices).
  - Rapid containment and response capabilities.
- **Benefits:** Enhanced endpoint security, improved incident response, and prevention of lateral movement in attacks.



# SIEM vs EDR



# SIEM-EDR

## SIEM vs EDR



- **Comparing Approaches:**
  - *SIEM*: Holistic view of network-wide events and logs from multiple sources.
  - *EDR*: Focused on endpoint-specific security and response actions.
- **Complementary Roles:** SIEM and EDR work together to provide comprehensive security coverage.



# Example of an open source SIEM-EDR: Wazuh

# SIEM-EDR

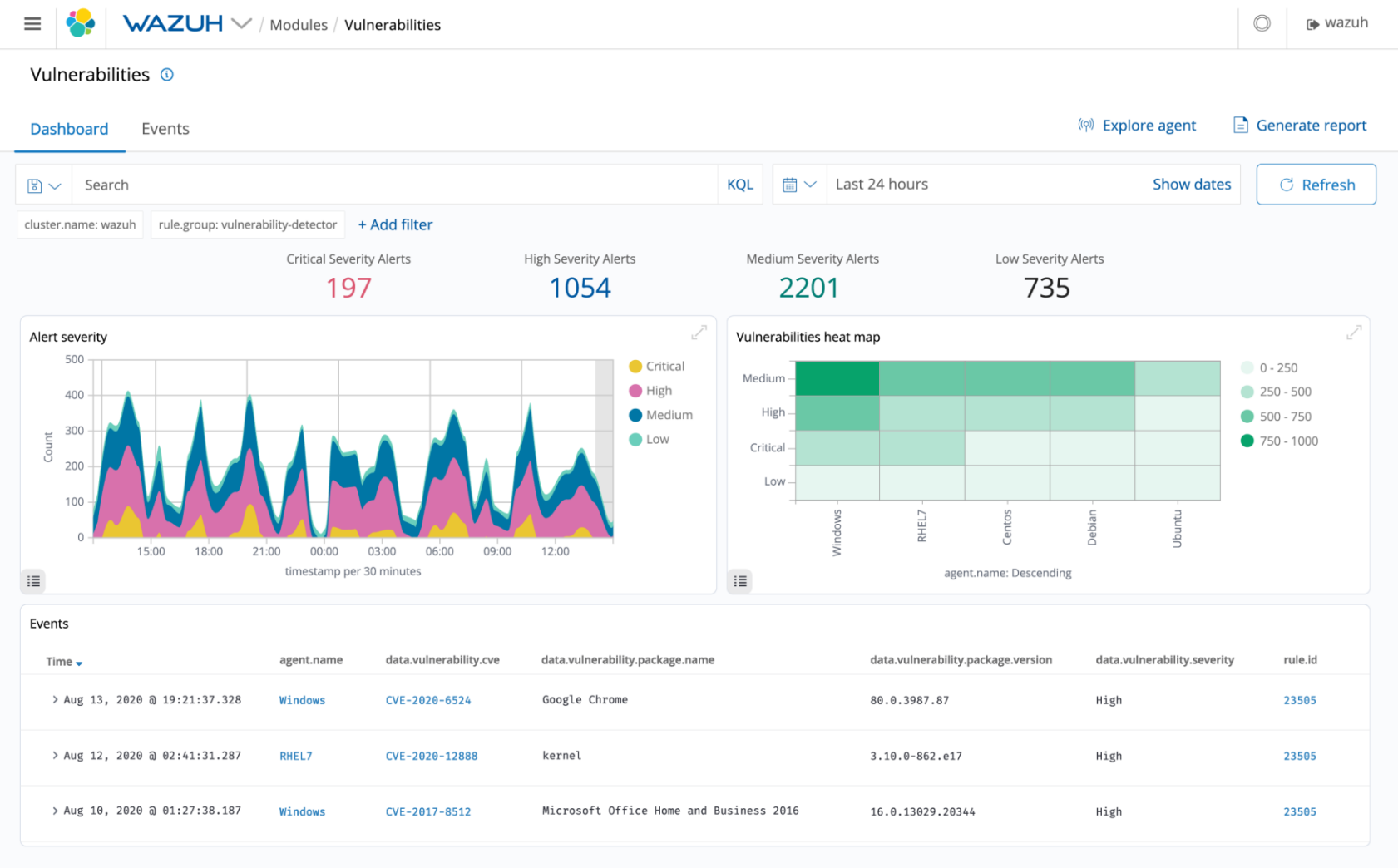
## Wazuh



- **Key Features:**
  - Log data analysis and correlation.
  - Intrusion detection and vulnerability assessment.
  - File integrity monitoring and compliance checks.
  - Endpoint detection and response capabilities.
- **Advantages:**
  - Cost-effective for small businesses and personal use.
  - Flexibility and customization with open-source architecture.

# SIEM-EDR

## Wazuh Alerts



Vulnerabilities ⓘ

Dashboard

Events

🔍

Search

KQL

📅

Last 24 hours

Show dates

🔄 Refresh

cluster.name: wazuh

rule.group: vulnerability-detector

+ Add filter

Critical Severity Alerts

197

High Severity Alerts

1054

Medium Severity Alerts

2201

Low Severity Alerts

735

Alert severity

Alert severity chart showing counts over time (timestamp per 30 minutes). The chart displays four categories: Critical (yellow), High (pink), Medium (blue), and Low (green). The Y-axis represents the count (0 to 500), and the X-axis represents the timestamp per 30 minutes (15:00 to 12:00). The chart shows a significant peak in High severity alerts around 18:00 and 21:00, and a smaller peak in Critical severity alerts around 15:00.

● Critical  
● High  
● Medium  
● Low

Vulnerabilities heat map

Vulnerabilities heat map showing counts across different operating systems (Windows, RHEL7, Centos, Debian, Ubuntu) and severity levels (Medium, High, Critical, Low). The color scale ranges from 0 - 250 (light green) to 750 - 1000 (dark green). The chart shows a high concentration of vulnerabilities in the Windows and RHEL7 agents, particularly in the High and Critical severity levels.

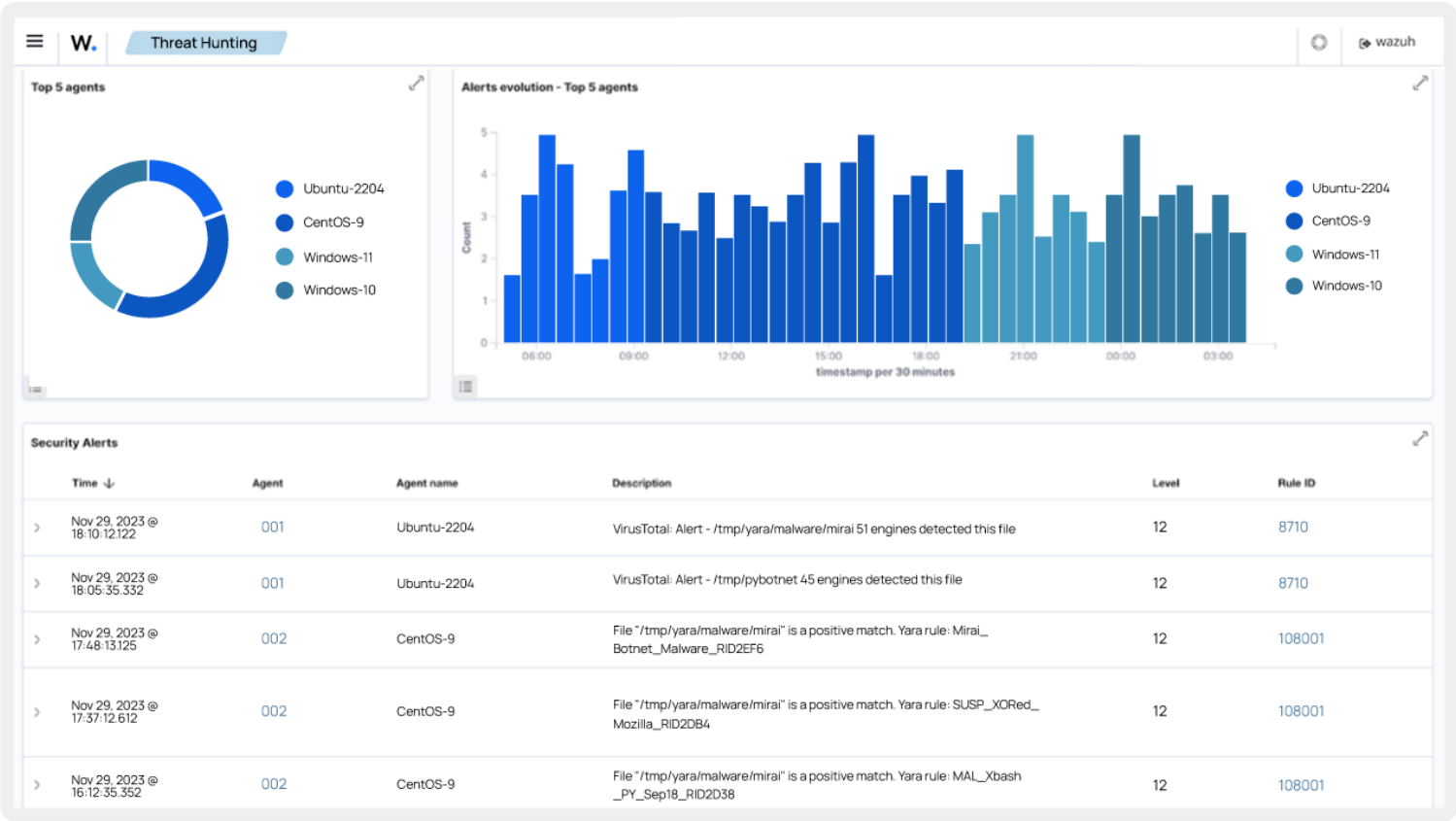
agent.name: Descending

Events

Time ▼	agent.name	data.vulnerability.cve	data.vulnerability.package.name	data.vulnerability.package.version	data.vulnerability.severity	rule.id
> Aug 13, 2020 @ 19:21:37.328	Windows	CVE-2020-6524	Google Chrome	88.0.3987.87	High	23505
> Aug 12, 2020 @ 02:41:31.287	RHEL7	CVE-2020-12888	kernel	3.10.0-862.e17	High	23505
> Aug 10, 2020 @ 01:27:38.187	Windows	CVE-2017-8512	Microsoft Office Home and Business 2016	16.0.13029.20344	High	23505

# SIEM-EDR

## Wazuh Threat Hunting



# SIEM-EDR

## Wazuh Vulnerability Scanner

Inventory

Events

SEVERITY

Critical (76)

High (483)

Medium (648)

Low (57)

Vulnerabilities (76)

severity=Critical ×

Filter or search

Name ↑	Version	Architecture
apparmor	2.13.3-7ubuntu5.1	amd64
dpkg	1.19.7ubuntu3	amd64
firefox	97.0+build2-0ubuntu0....	amd64
firefox	97.0+build2-0ubuntu0....	amd64

CVE-2022-1664

×

Title

CVE-2022-1664 affects dpkg

Version

1.19.7ubuntu3

Last full scan

Sep 27, 2022 @ 04:29:06.000

Updated

Jun 7, 2022 @ 00:00:00.000

Name

dpkg

Architecture

amd64

Last partial scan

Sep 27, 2022 @ 04:39:07.000

References

View external references 🔗

CVE

CVE-2022-1664

Condition

Package less than 1.19.7ubuntu3.2

Published

May 26, 2022 @ 00:00:00.000

Recent events

🔗

1 hits

Search

DQL

📅

Last 24 hours

Show dates

Refresh

+ Add filter

Time ↓	Description	Level	Rule ID	Status
Sep 27, 2022 @ 04:28:36.300	CVE-2022-1664 affects dpkg	13	23506	Active

# WOCSA

## Join Us!



[www.wocsa.org](http://www.wocsa.org)



[@wocsa](#)



[contact@wocsa.org](mailto:contact@wocsa.org)



[@wocsa\\_asso](#)



[@WOCSA-rx2mn](#)



[@wocsa](#)



<https://discord.gg/pDunje3tpb>



Join us to change the digital world:  
<https://www.helloasso.com/associations/wocsa/adhesions/bulletin-d-adhesion-2>



Please provide your feedback for our quality check process:  
<https://www.wocsa.org/qcheck.php>