WOCSA

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

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

www.wocsa.org

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

What is a SIEM?

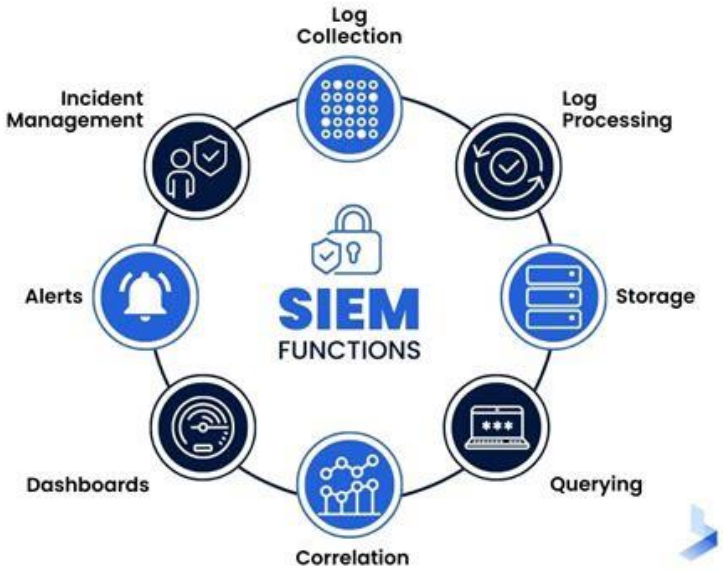
SIEM-EDR

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

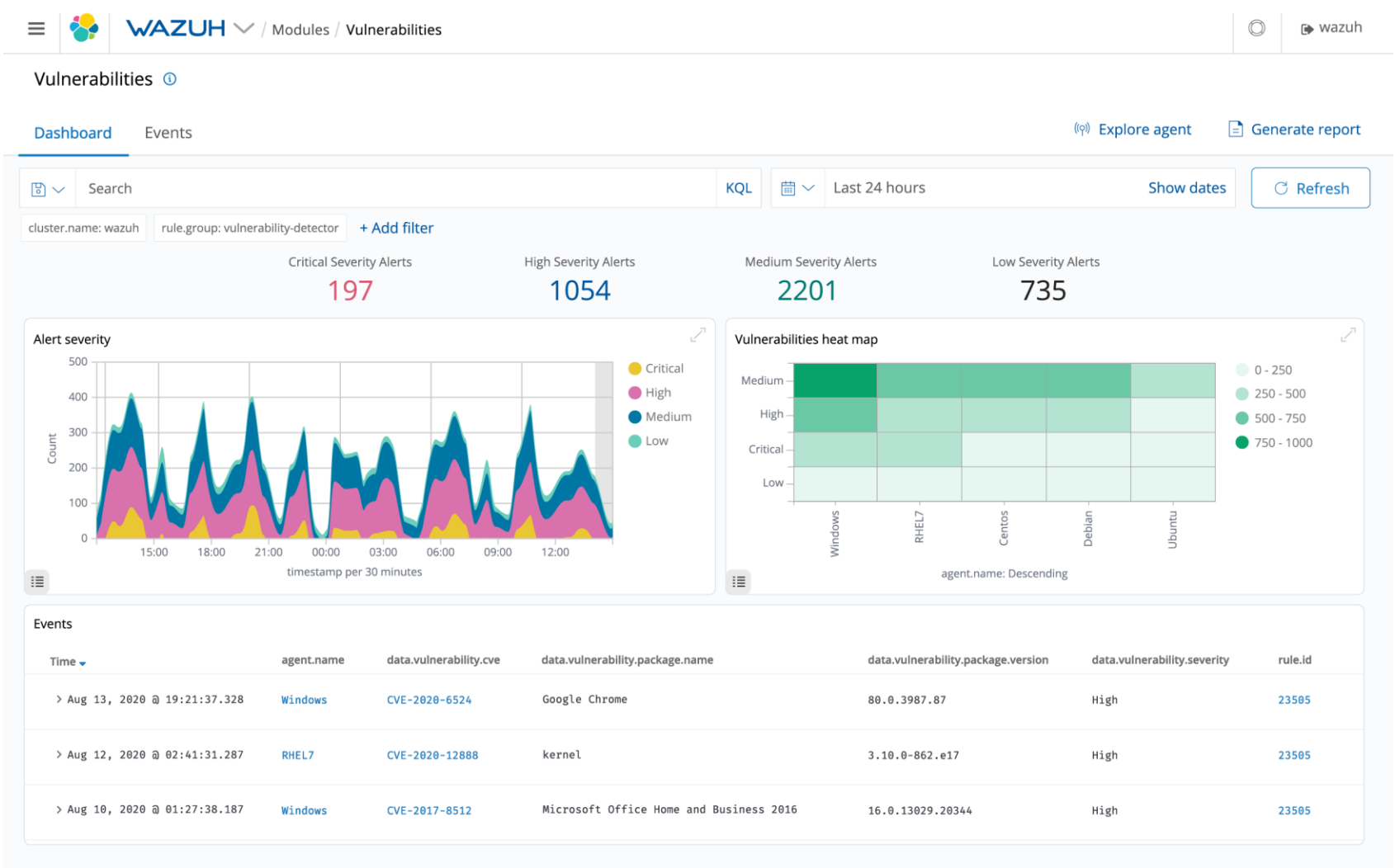
Wazuh

- **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.

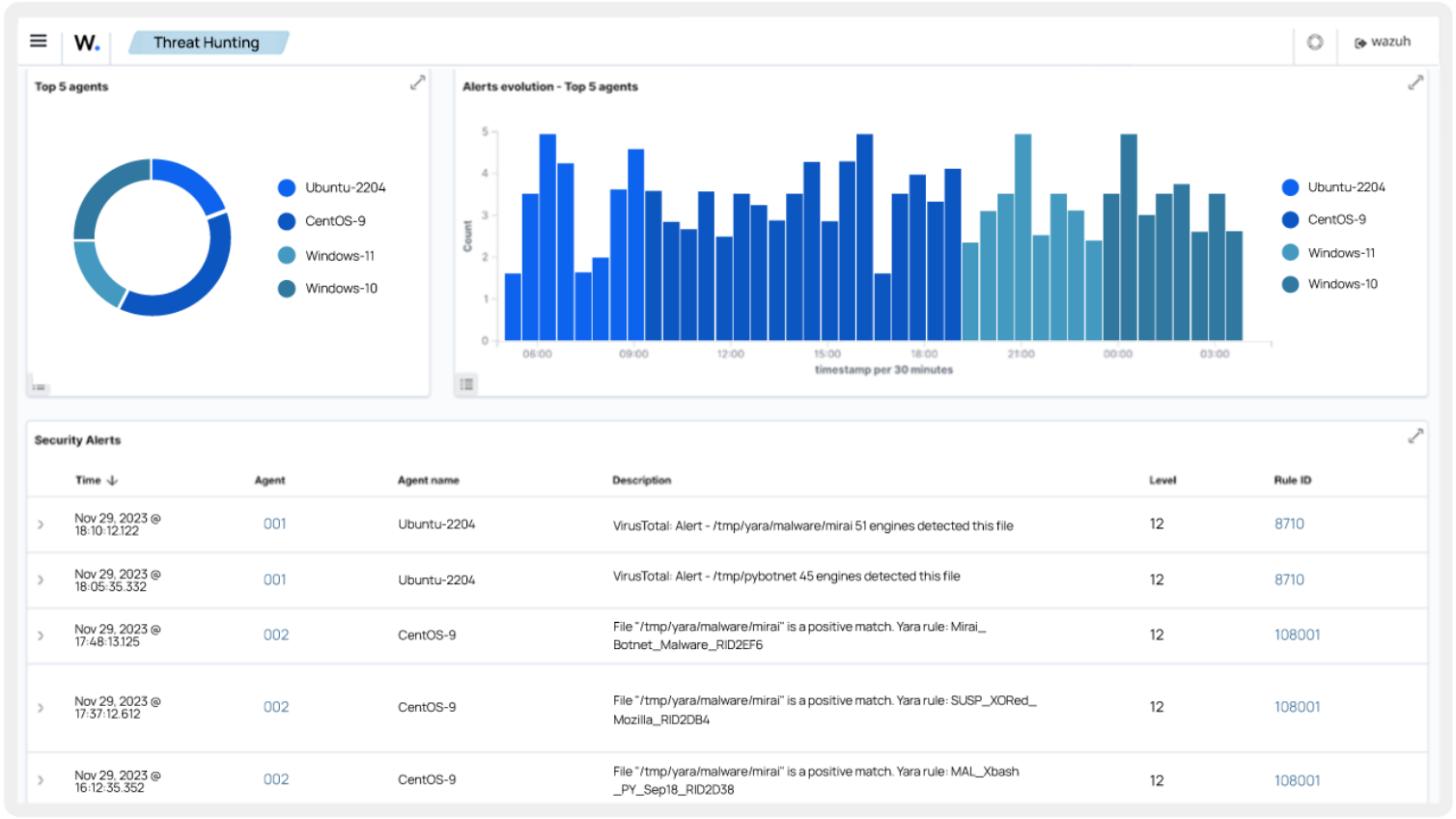
SIEM-EDR

Wazuh Alerts



SIEM-EDR

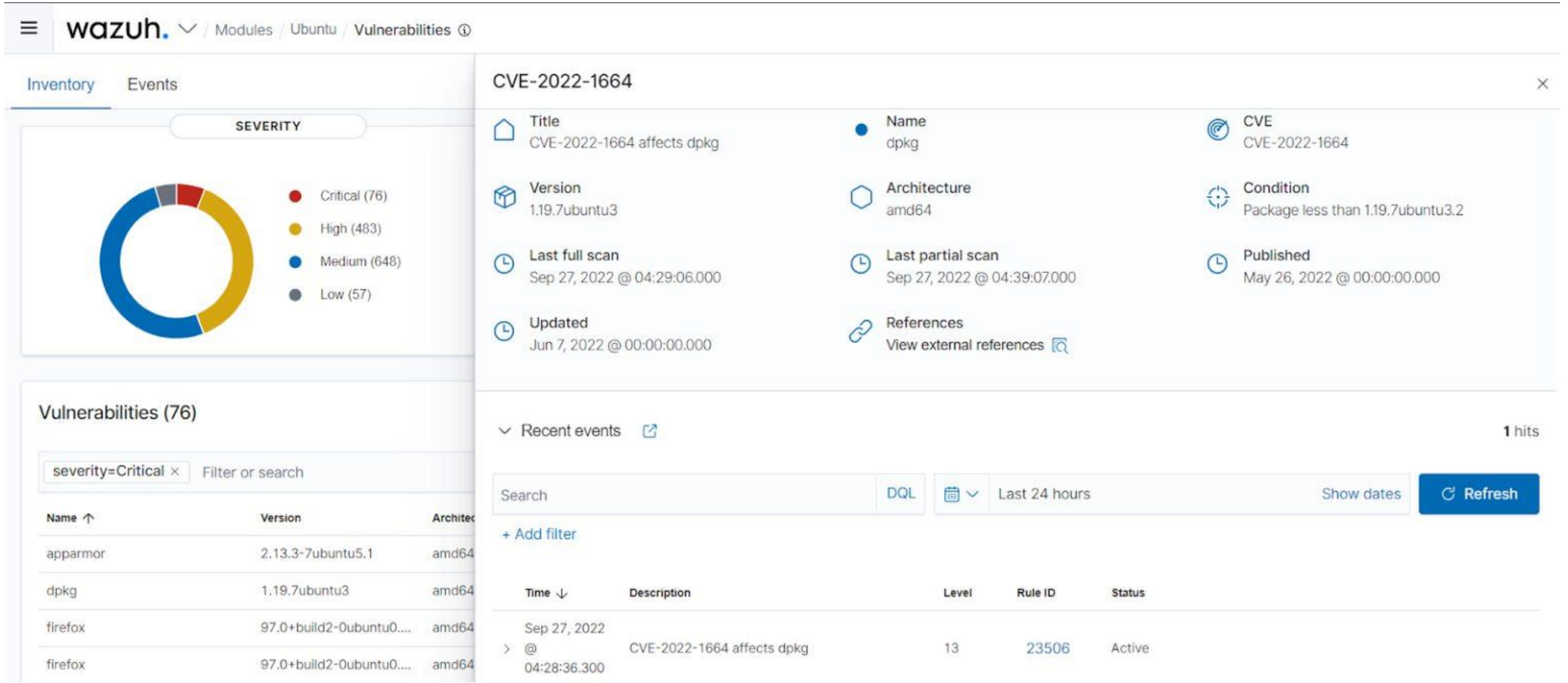
Wazuh Threat Hunting



wazuh.
Threat Hunting

SIEM-EDR

Wazuh Vulnerability Scanner



WOCSA

Join Us!

www.wocsa.org

contact@wocsa.org

@WOCSA-rx2mn

https://discord.gg/pDunje3tpb

@wocsa

@wocsa_asso

@wocsa

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