initMAX

ISP Alliance 2026

Wazuh for ISPs
Features and capabilities

Martin Krupka, initMAX
20 October 2026, Jičín

initMAX

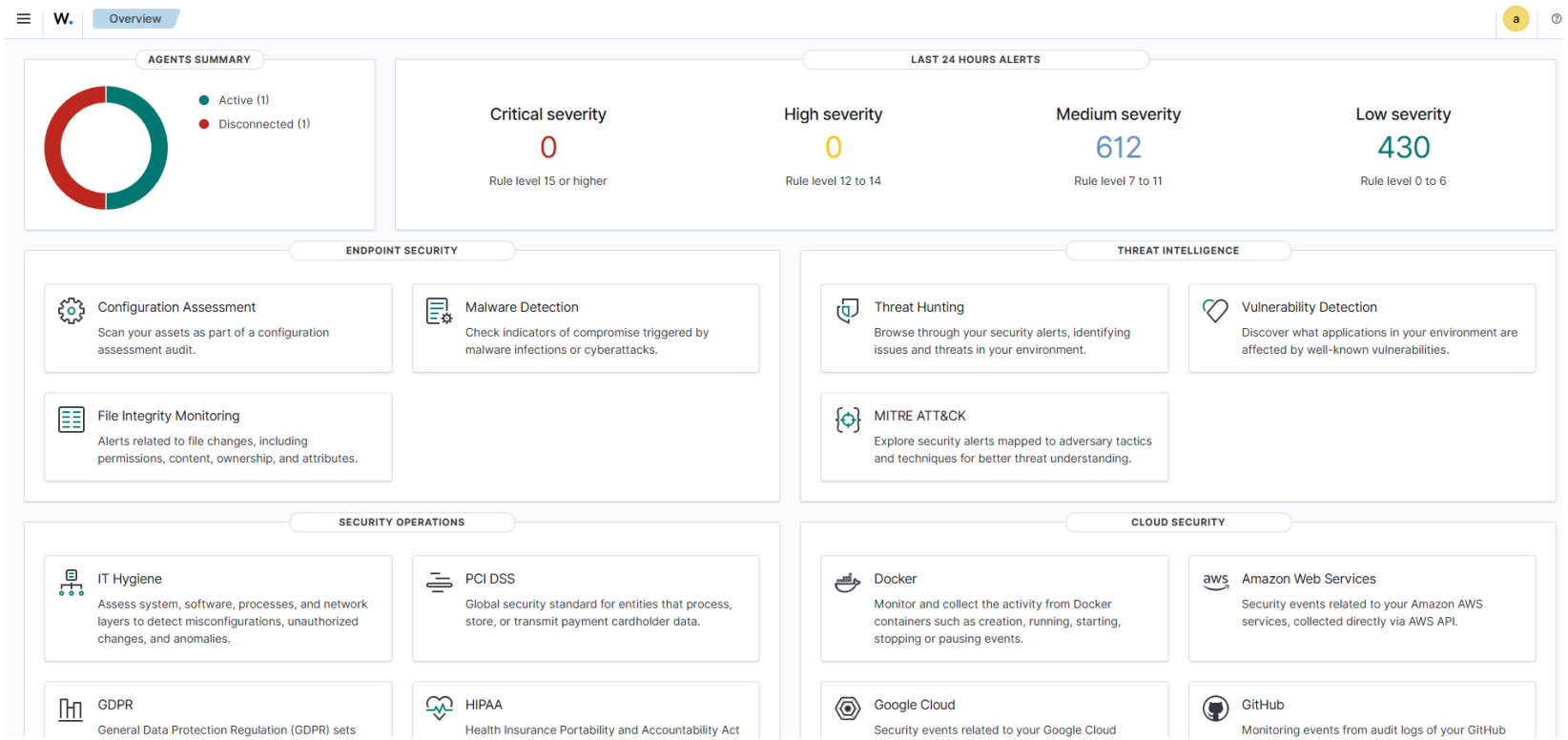
Wazuh in practice

Security overview in one place

Wazuh brings together security events and findings from monitored systems.

Example for ISPs

A morning overview for the person responsible for the network and servers.



Actual Wazuh UI, vendor example

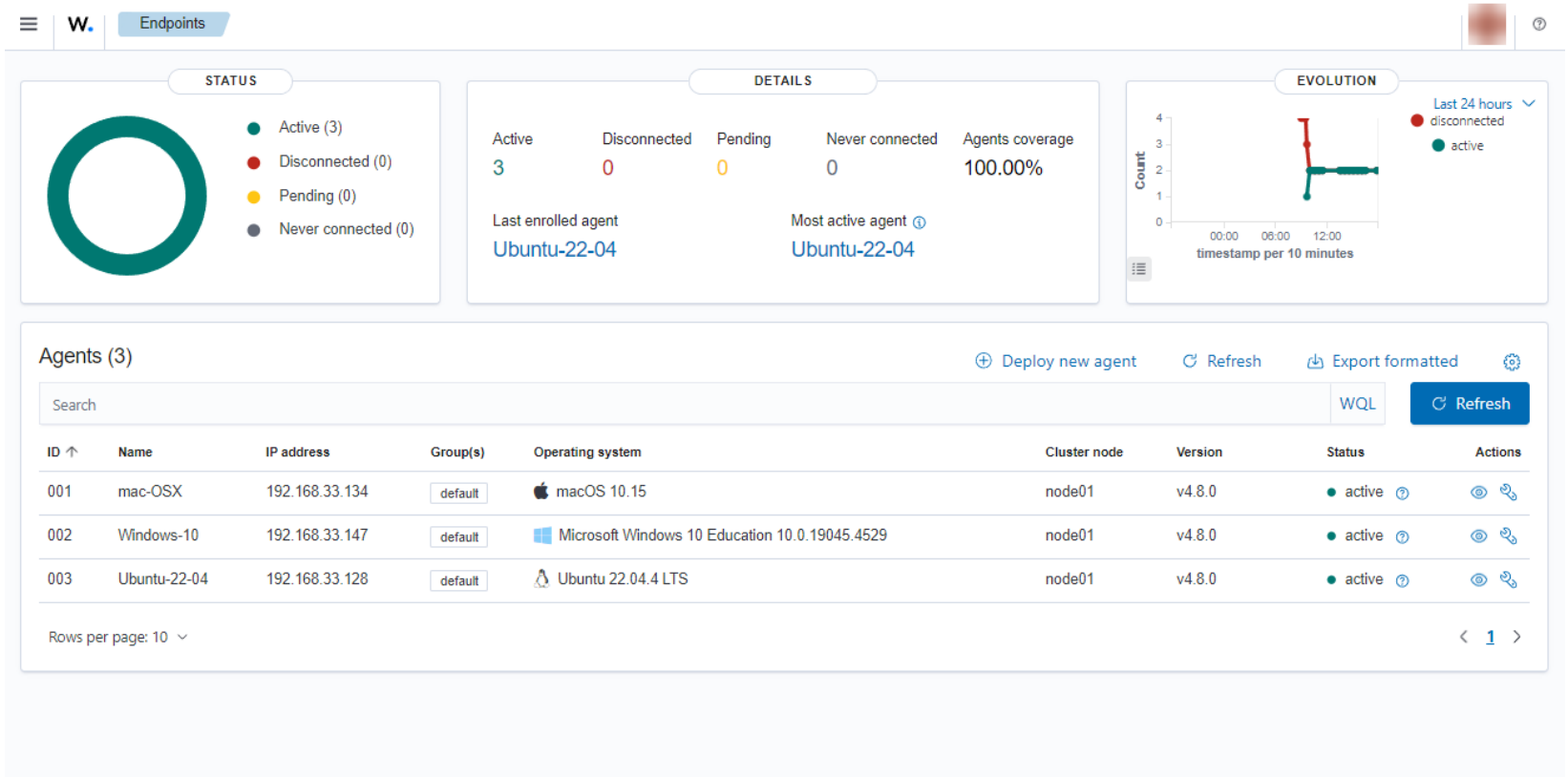
Wazuh in practice

Server and workstation coverage

An overview of registered devices and their agent status.

Example for ISPs

Bastion hosts, DNS servers, the customer portal and technicians' laptops.



Actual Wazuh UI, vendor example

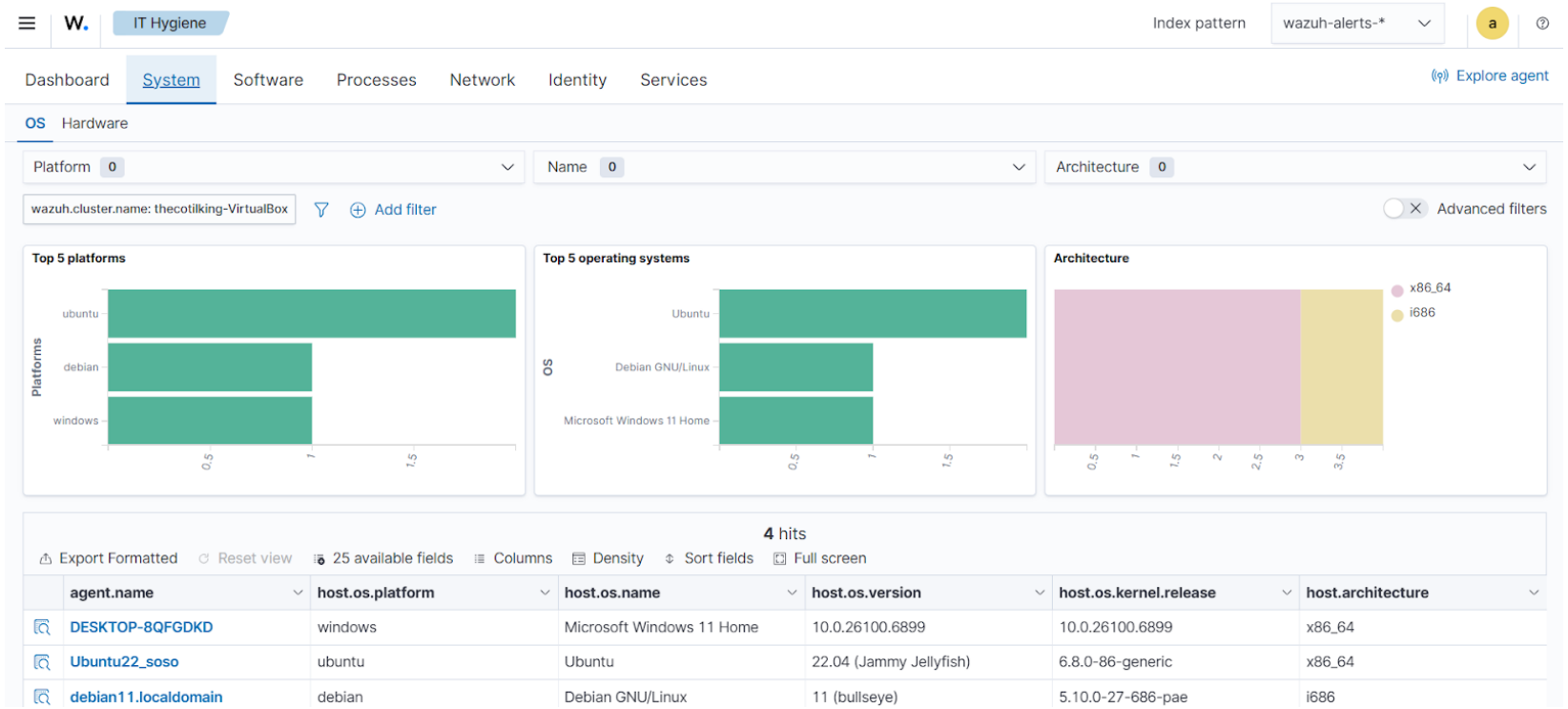
Wazuh in practice

System inventory

A central view of operating systems and hardware.

Example for ISPs

Linux versions on operational servers and Windows versions in the office.



Actual Wazuh UI, vendor example

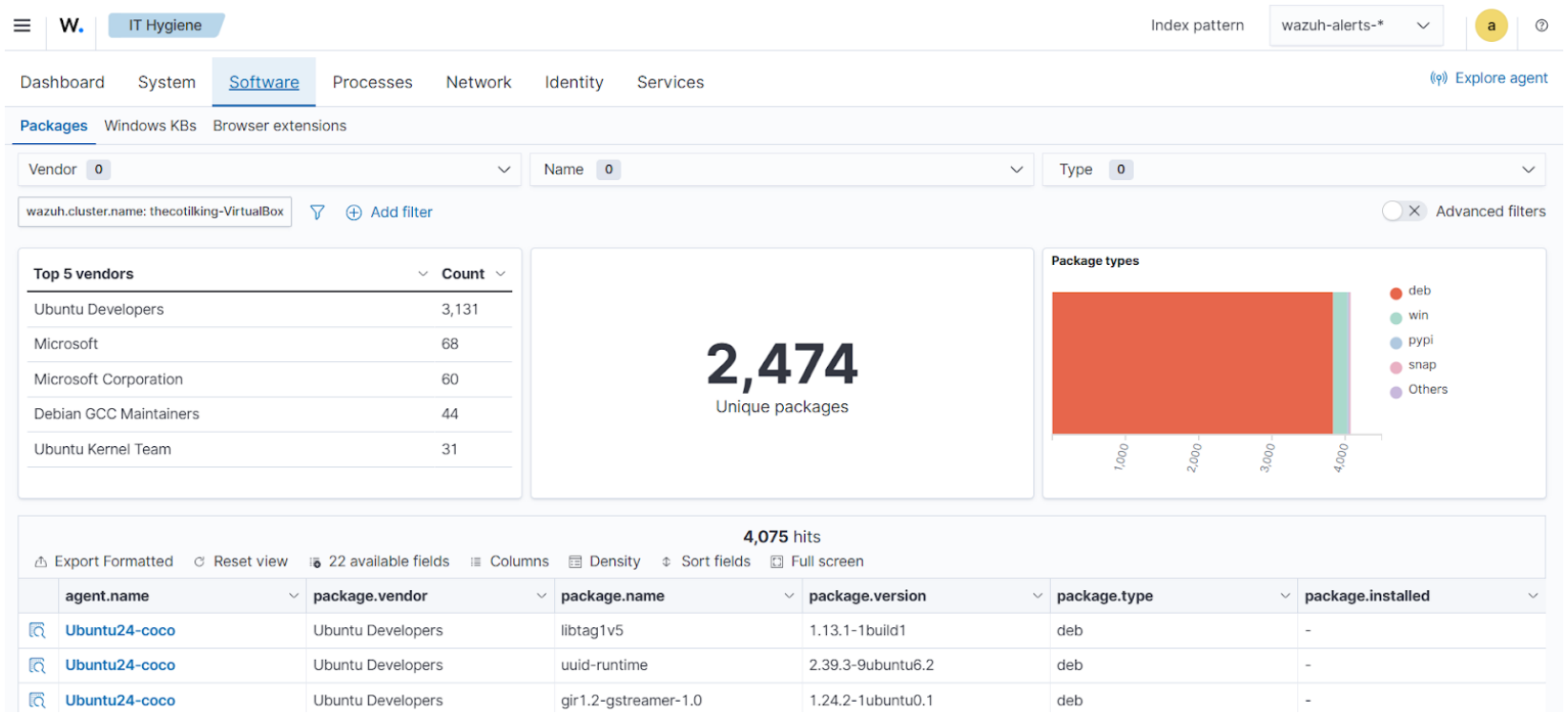
Wazuh in practice

Installed software

Packages and applications linked to individual hosts.

Example for ISPs

Which servers run a specific version of OpenSSH?



Actual Wazuh UI, vendor example

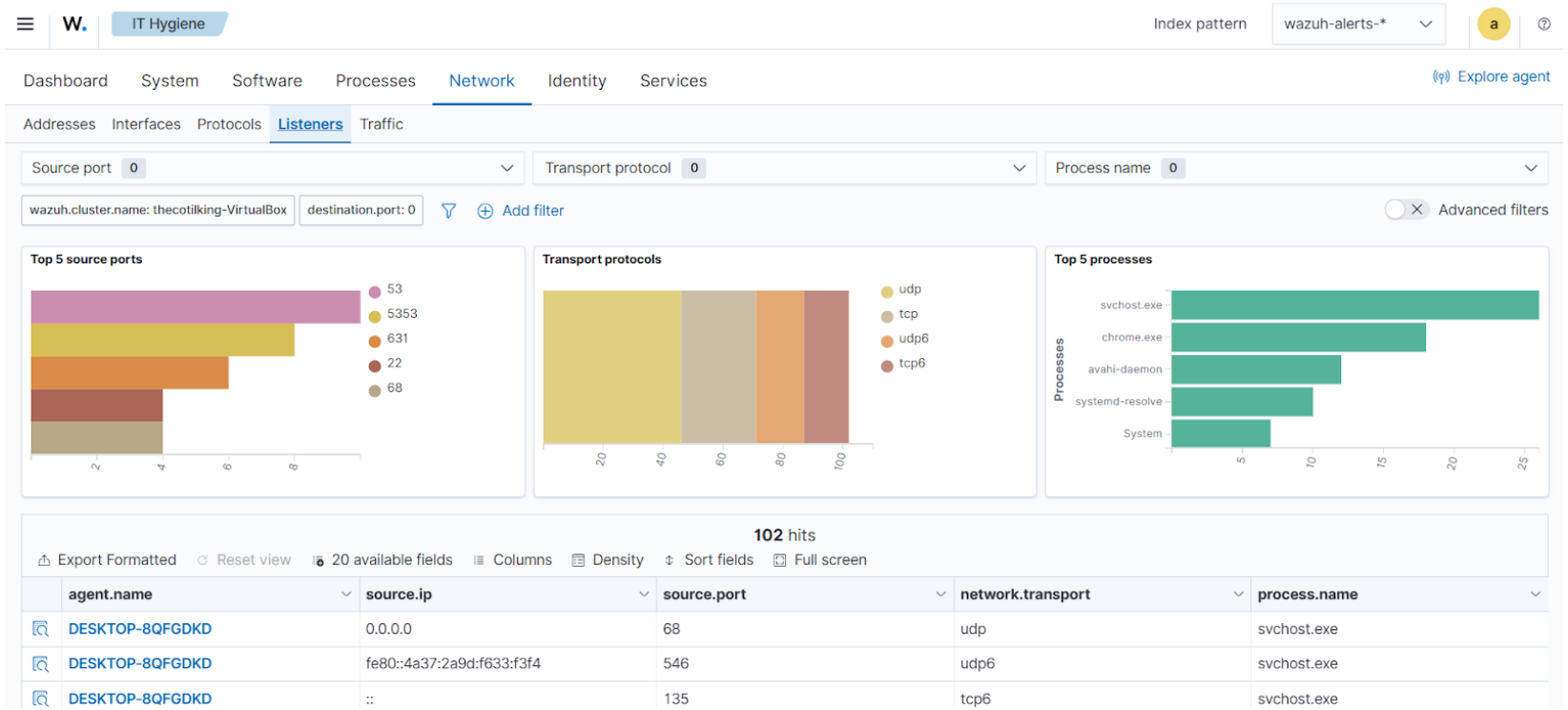
Wazuh in practice

Host services and network ports

An inventory of network information from monitored servers.

Example for ISPs

Check whether an unnecessary service is running on the production DNS server.



Actual Wazuh UI, vendor example

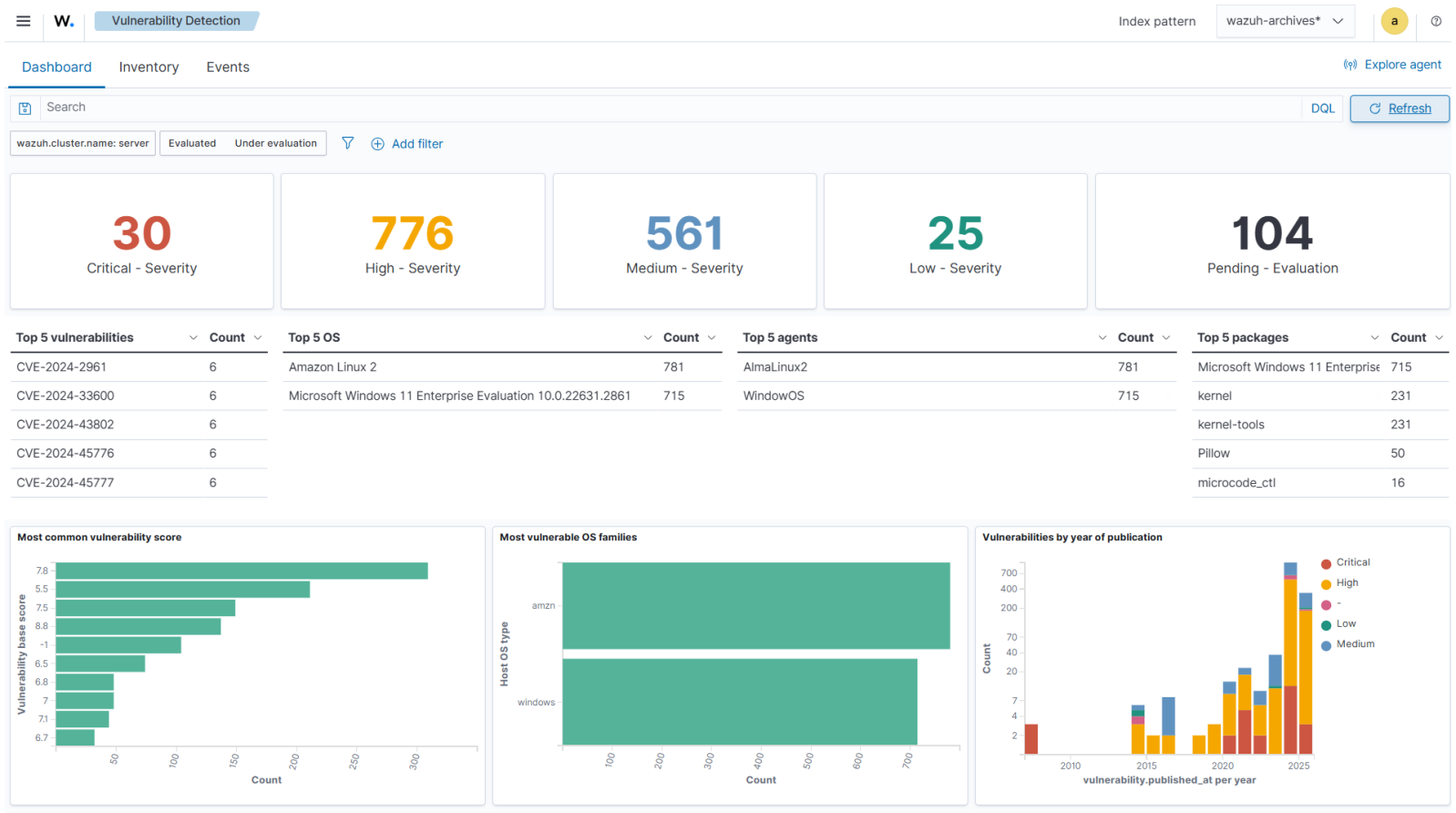
Wazuh in practice

Vulnerability overview

Known security vulnerabilities in installed software.

Example for ISPs

Plan patches for bastion hosts and internet-facing servers.



Actual Wazuh UI, vendor example

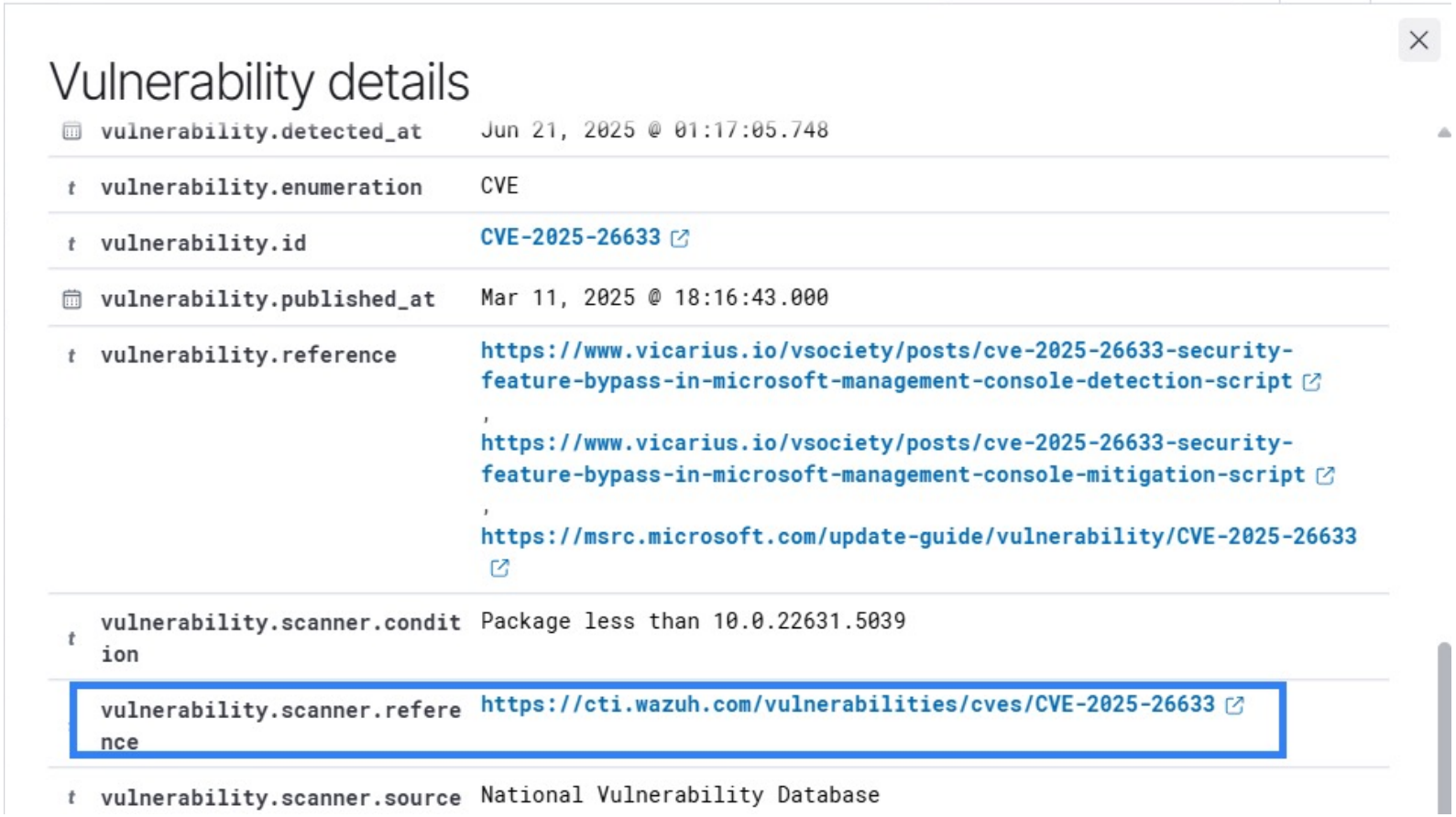
Wazuh in practice

Finding details and remediation evidence

Open a specific package and vulnerability from the overview.

Example for ISPs

The administrator gets the exact server and package to investigate.



Actual Wazuh UI, vendor example

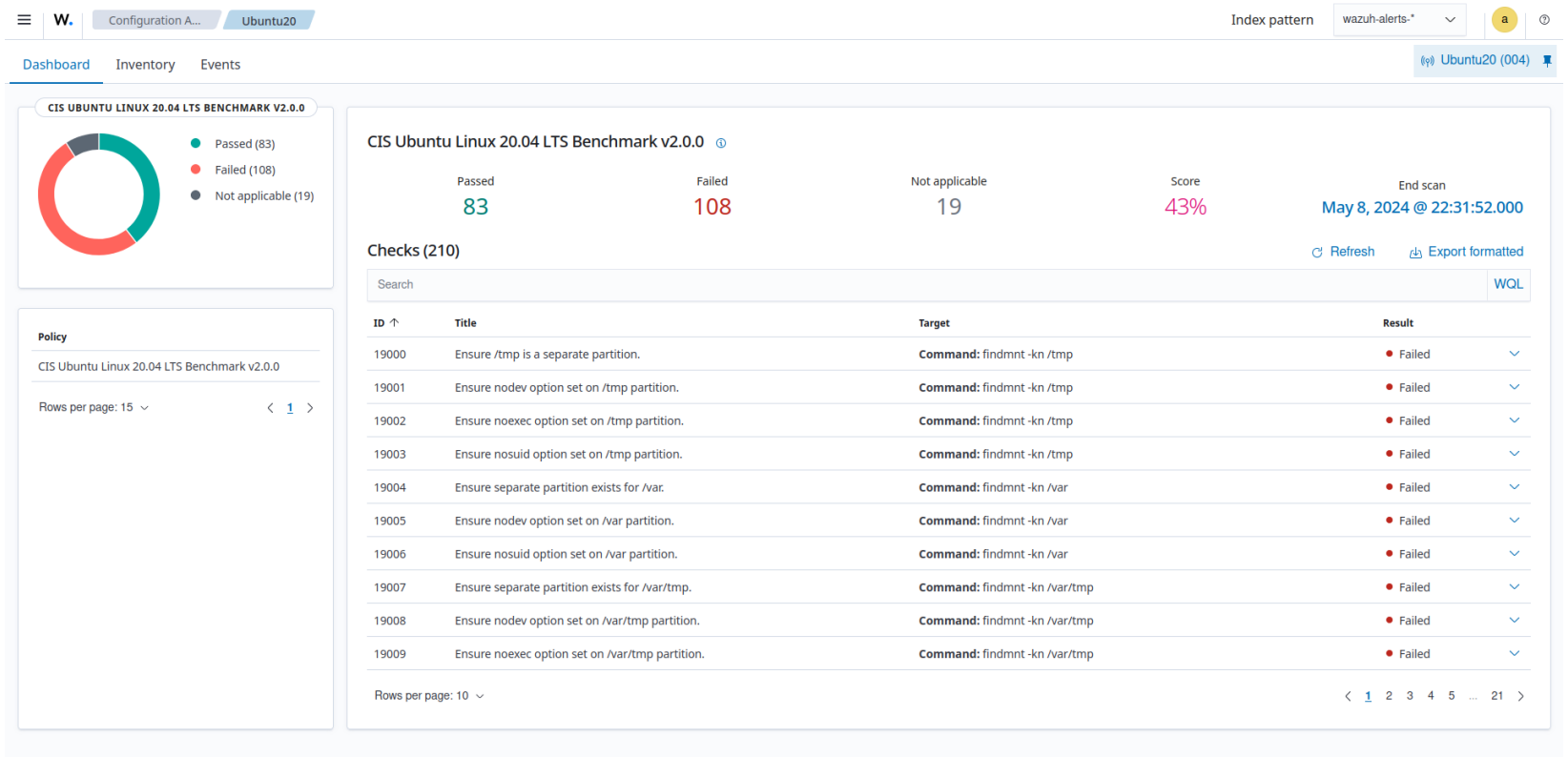
Wazuh in practice

Security configuration checks

Regular configuration checks against the selected policy.

Example for ISPs

Check authentication and security settings on operational servers.



Actual Wazuh UI, vendor example

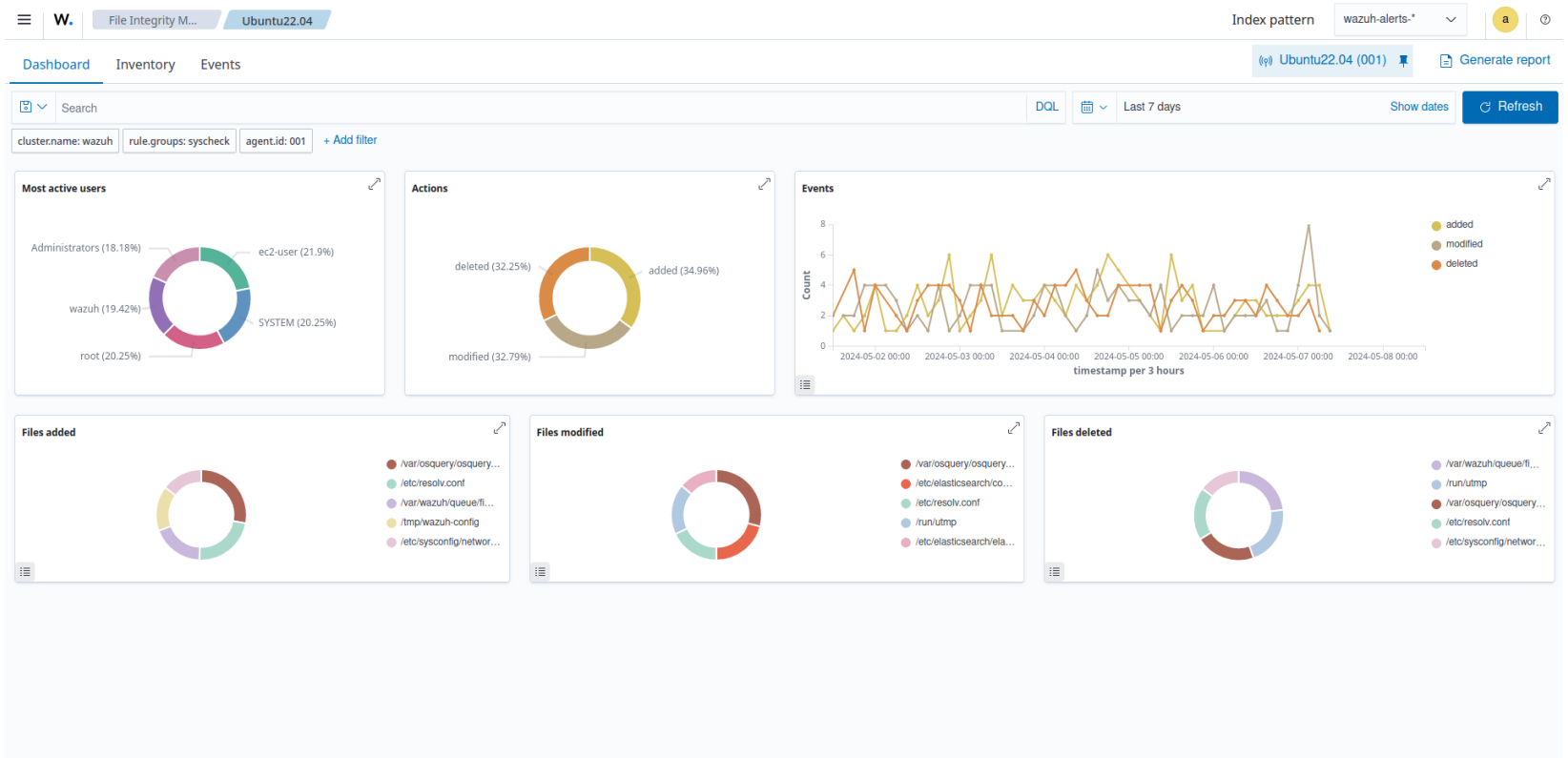
Wazuh in practice

Changes to important files

An overview of new, modified and deleted files.

Example for ISPs

DNS configuration, customer portal files or SSH settings.



Actual Wazuh UI, vendor example

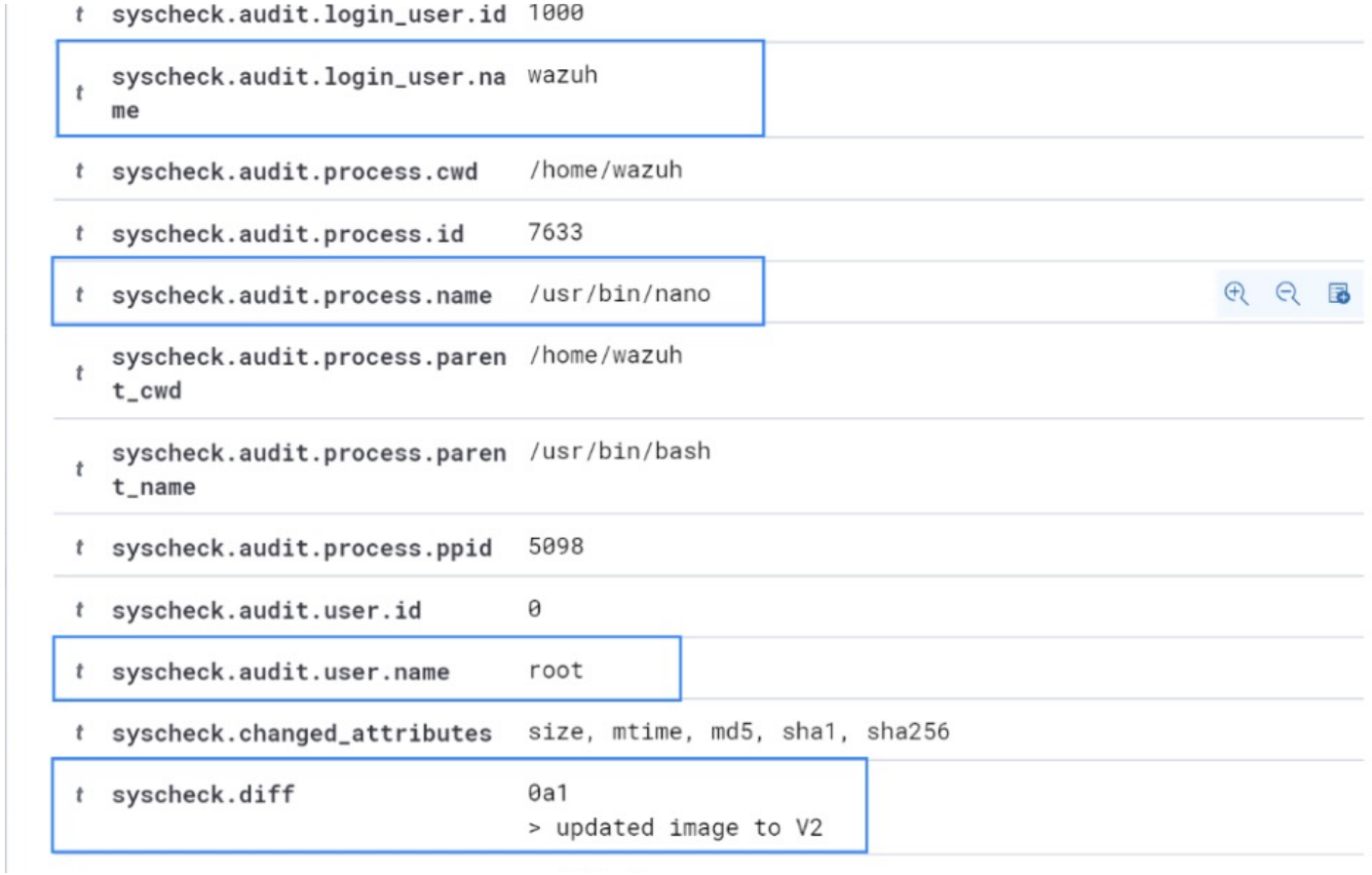
Wazuh in practice

File change context

Open the details of an individual change from the overview.

Example for ISPs

Compare a configuration change with the maintenance request.



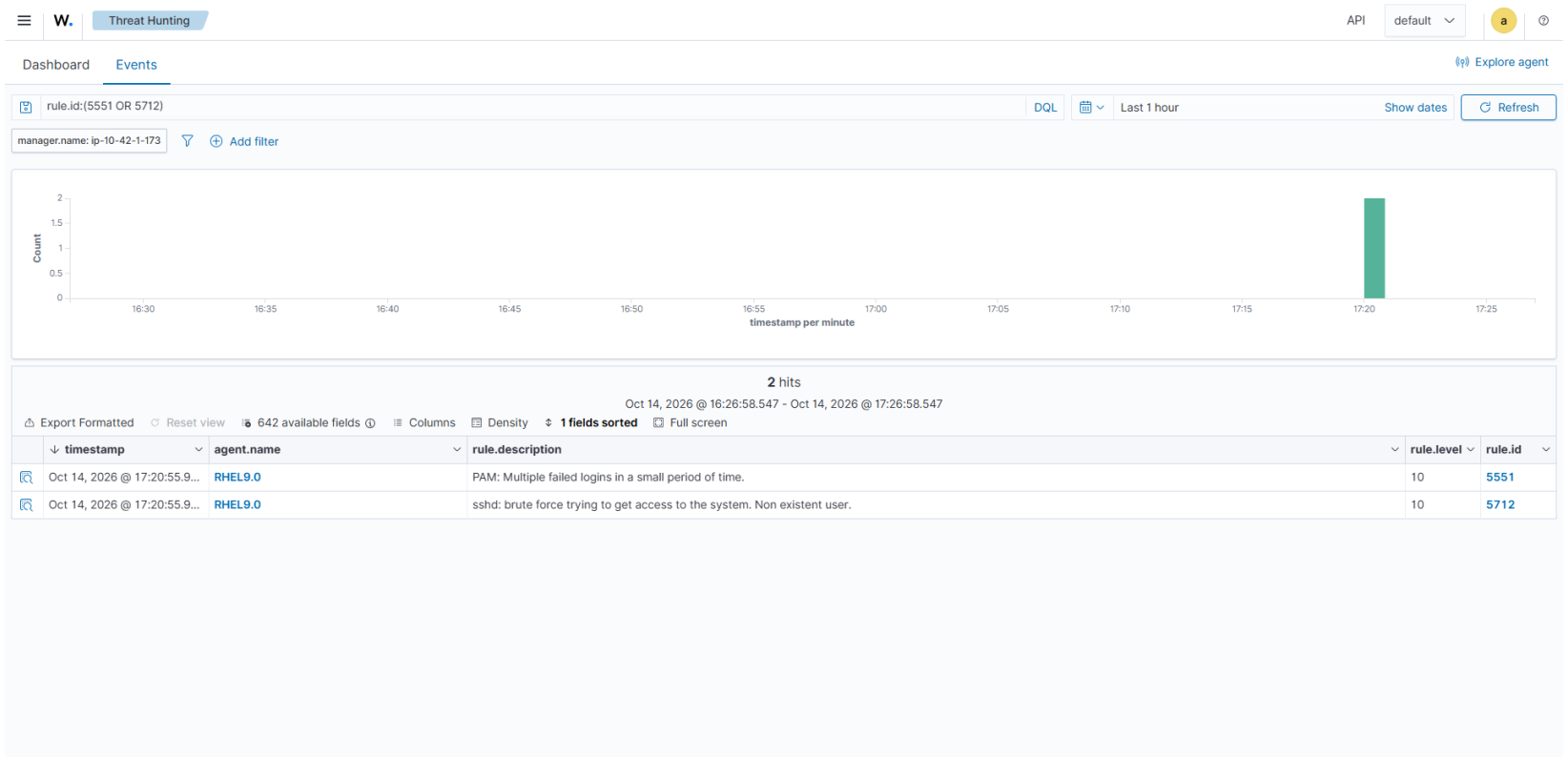
t	syscheck.audit.login_user.id	1000
t	syscheck.audit.login_user.name	wazuh
t	syscheck.audit.process.cwd	/home/wazuh
t	syscheck.audit.process.id	7633
t	syscheck.audit.process.name	/usr/bin/nano
t	syscheck.audit.process.parent_cwd	/home/wazuh
t	syscheck.audit.process.parent_name	/usr/bin/bash
t	syscheck.audit.process.ppid	5098
t	syscheck.audit.user.id	0
t	syscheck.audit.user.name	root
t	syscheck.changed_attributes	size, mtime, md5, sha1, sha256
t	syscheck.diff	0a1 > updated image to V2

Actual Wazuh UI, vendor example

Wazuh in practice

Logins and repeated attempts

An overview of failed and successful logins.



Example for ISPs

Overnight access to a bastion host or an administrator's remote desktop.

Actual Wazuh UI, vendor example

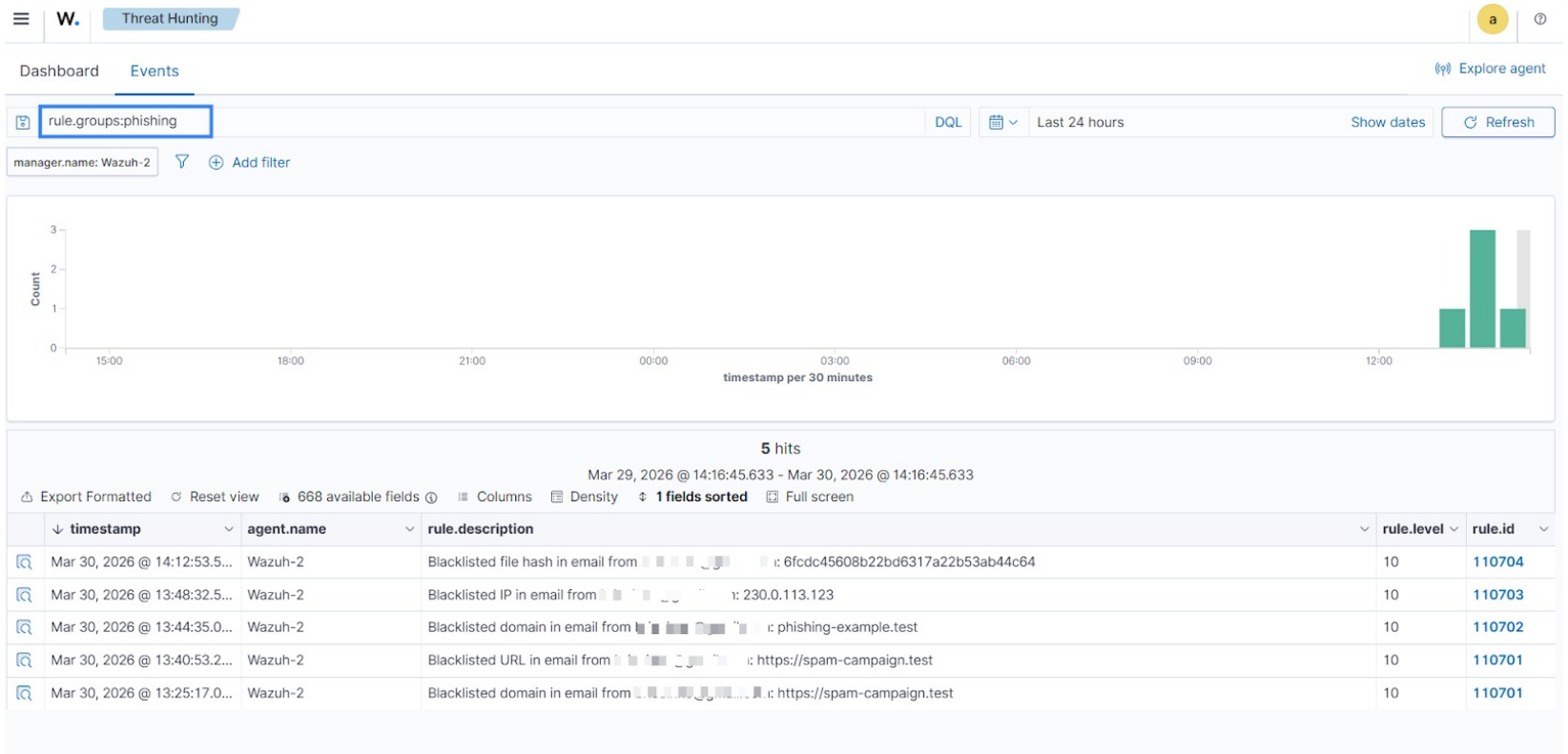
Wazuh in practice

Connecting related events

Filter security events to answer the operator's question.

Example for ISPs

What happened on the server while a colleague investigated unusual access?



Actual Wazuh UI, vendor example

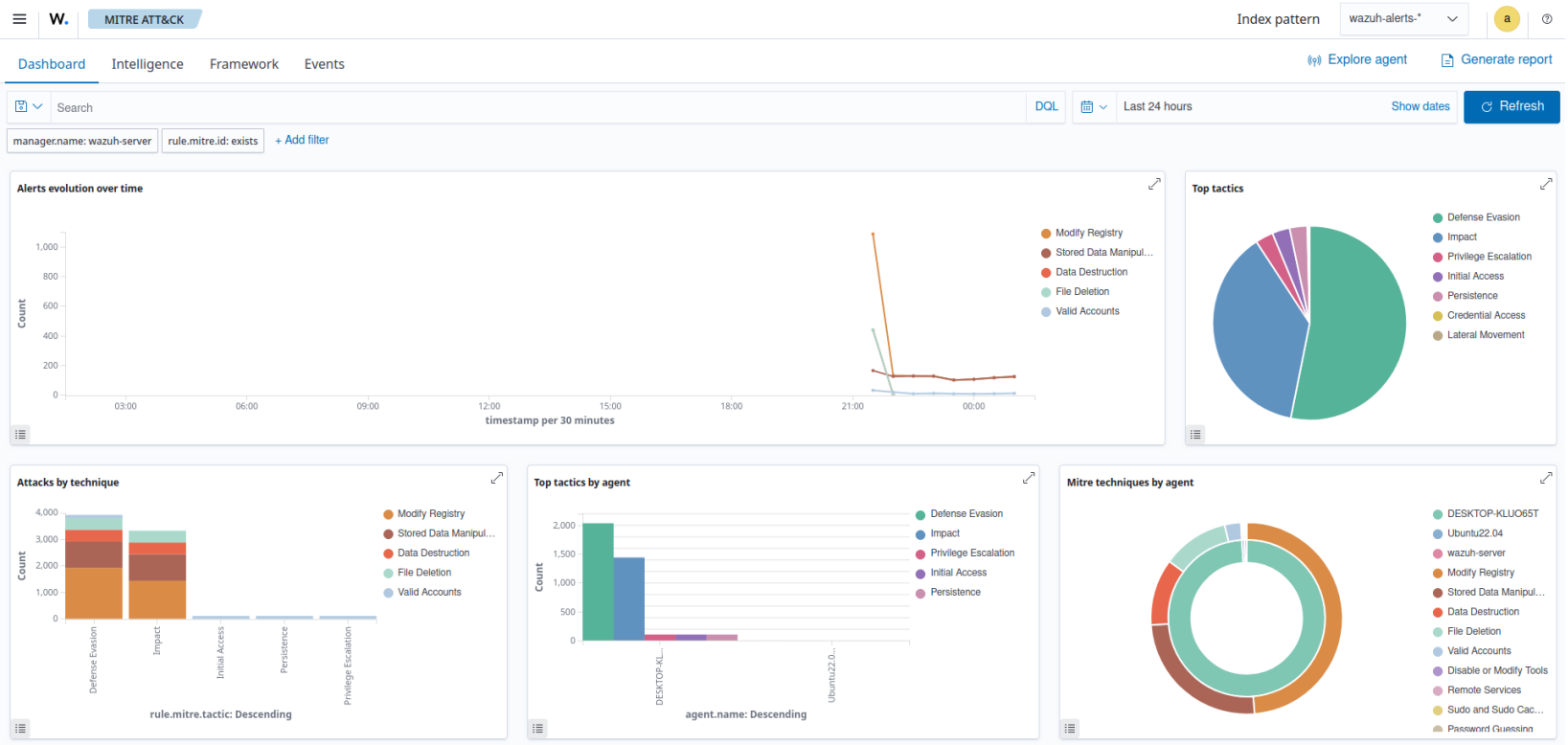
Wazuh in practice

MITRE ATT&CK overview

Security events in the context of known attack techniques.

Example for ISPs

Check whether different suspicious activities occur on the same host.



Actual Wazuh UI, vendor example

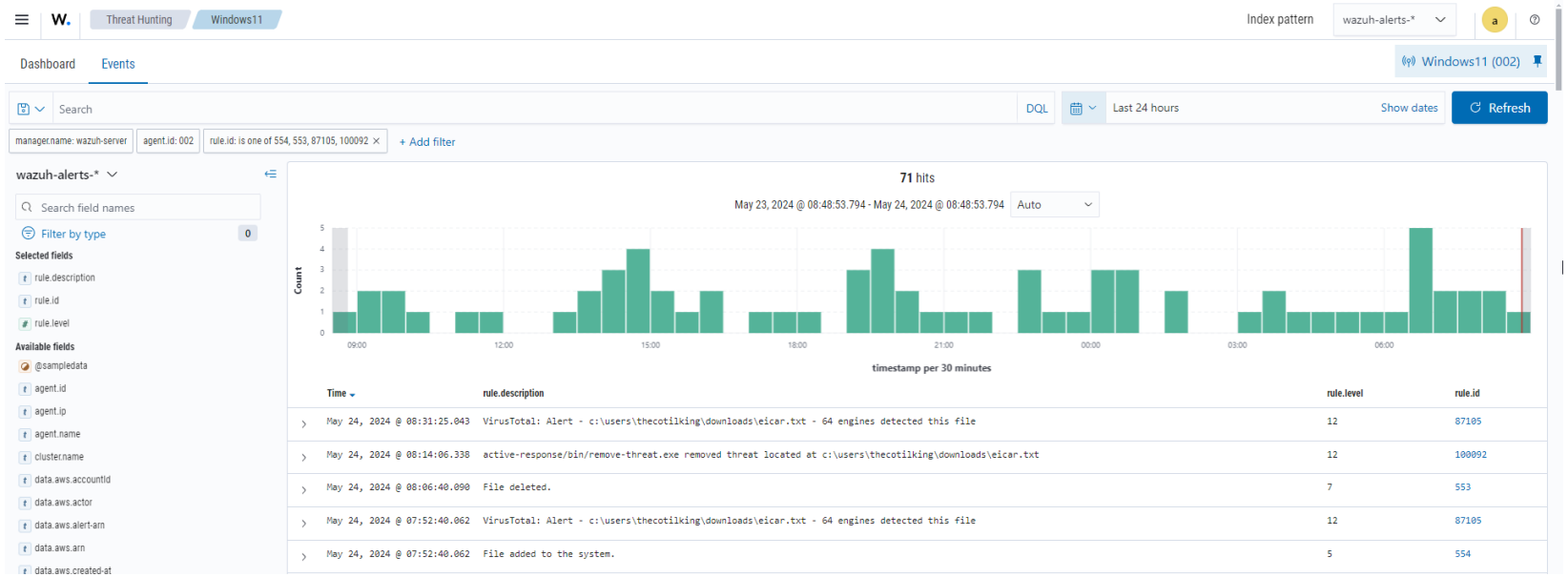
Wazuh in practice

Malware and suspicious files

Suspicious file detection results in the event overview.

Example for ISPs

A suspicious file on a web server or an antivirus finding on a technician's laptop.



Actual Wazuh UI, vendor example

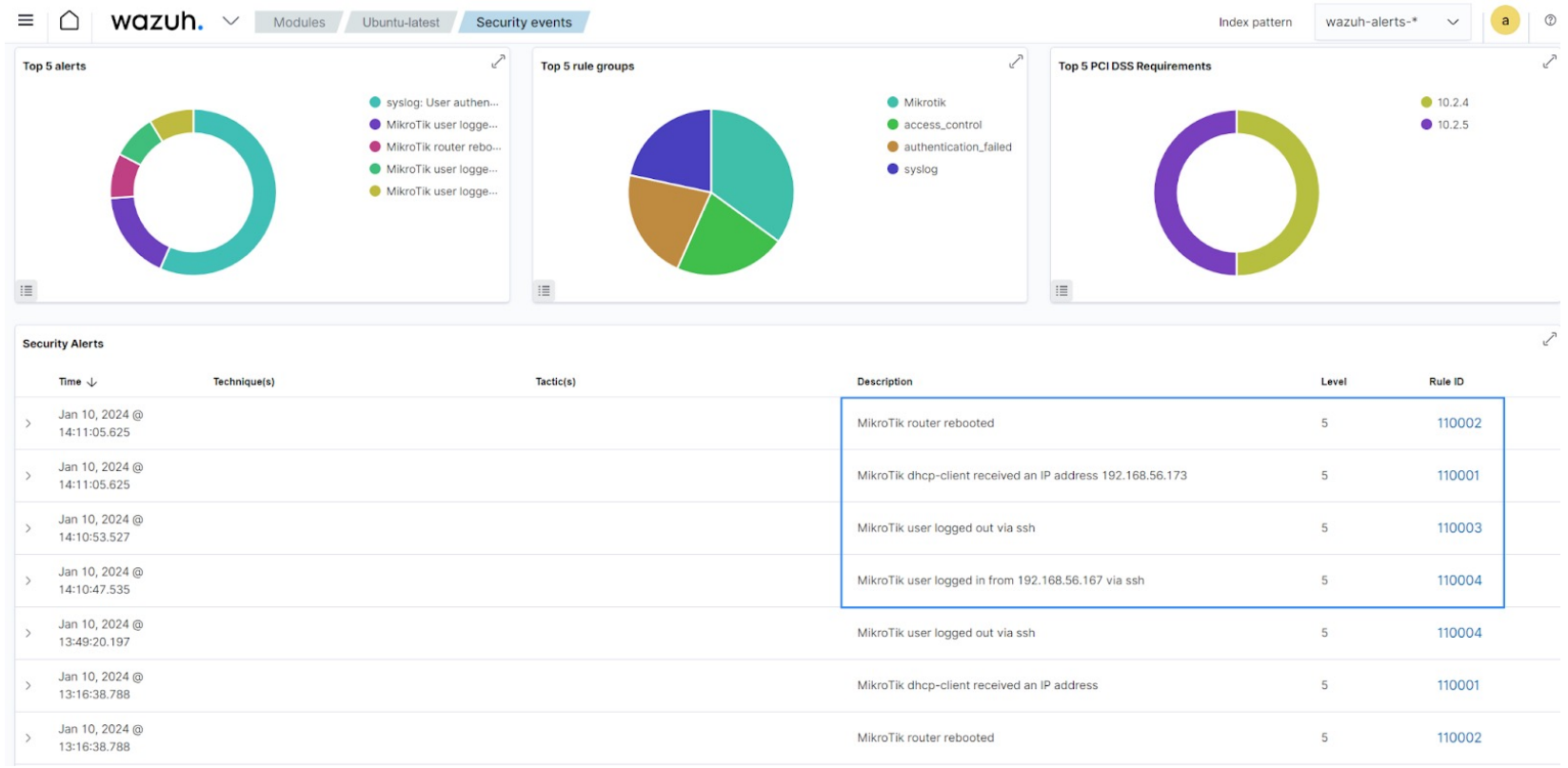
Wazuh in practice

Router and firewall logs

Network events in the same interface as server logs.

Example for ISPs

An administrator logging in to a router or a firewall security event.



Actual Wazuh UI, vendor example of MikroTik integration

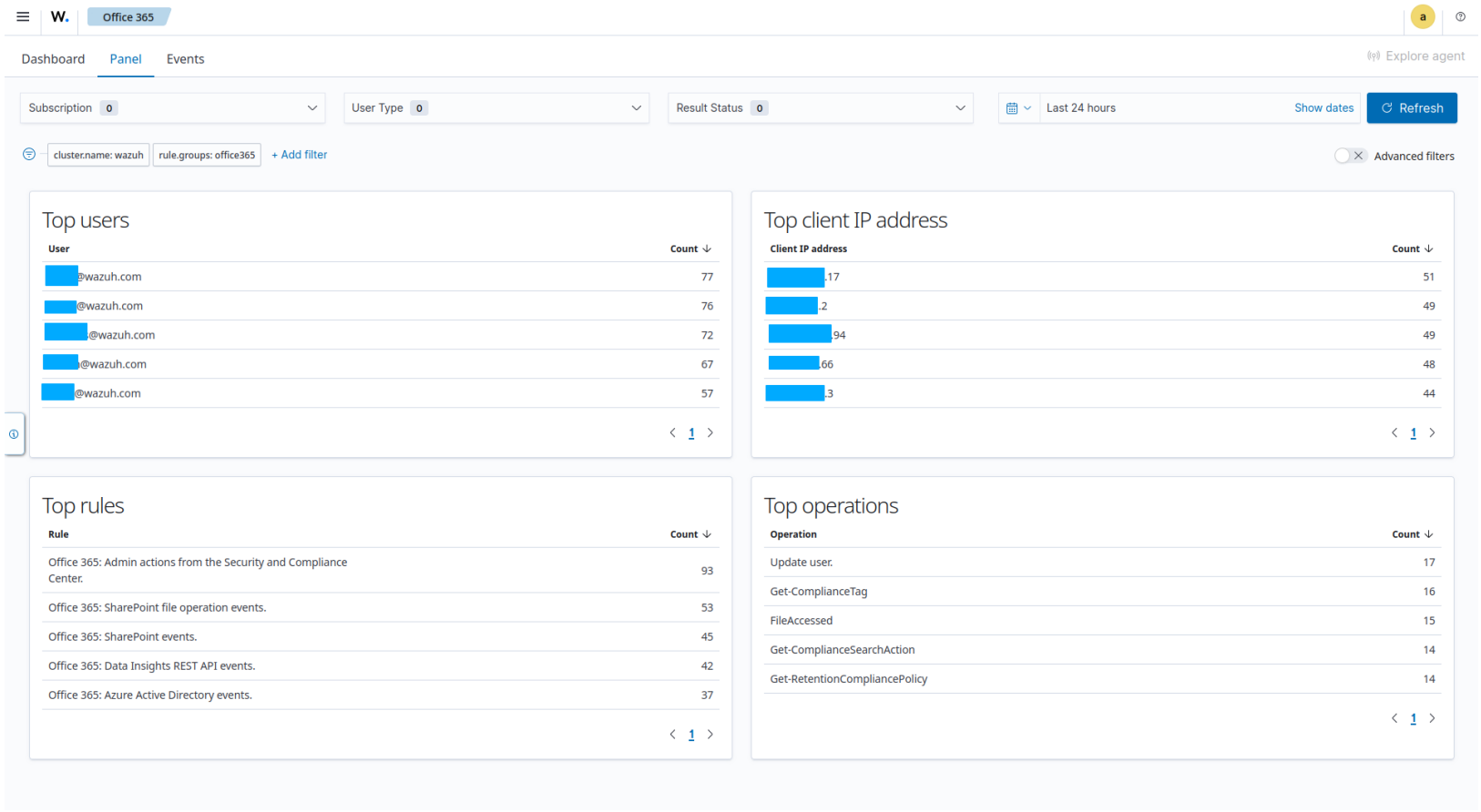
Wazuh in practice

Cloud and Microsoft 365

Audit events from connected cloud services.

Example for ISPs

Investigate an unusual administrative change in the company's Microsoft 365.



Actual Wazuh UI, vendor example

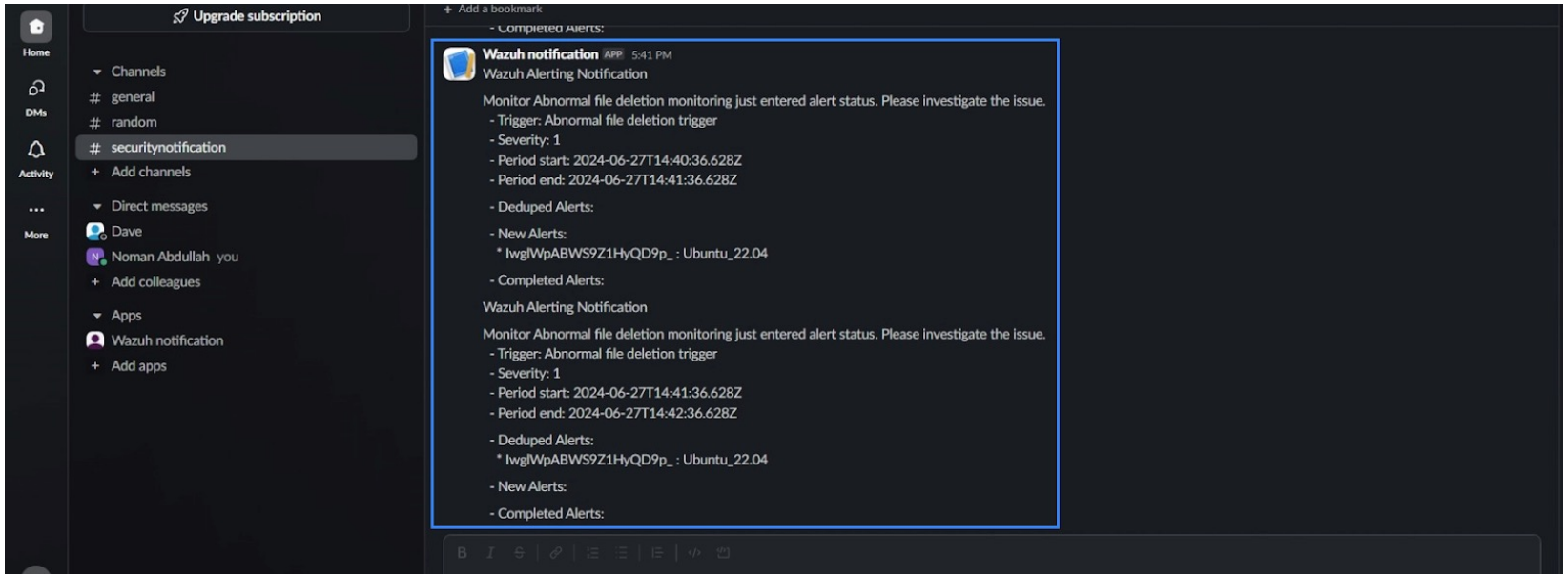
Wazuh in practice

Alerts for operators

Send selected alerts to the team chat.

Example for ISPs

Notify the on-call team when files are deleted in bulk on a server.



Actual Slack UI, vendor example of Wazuh notifications

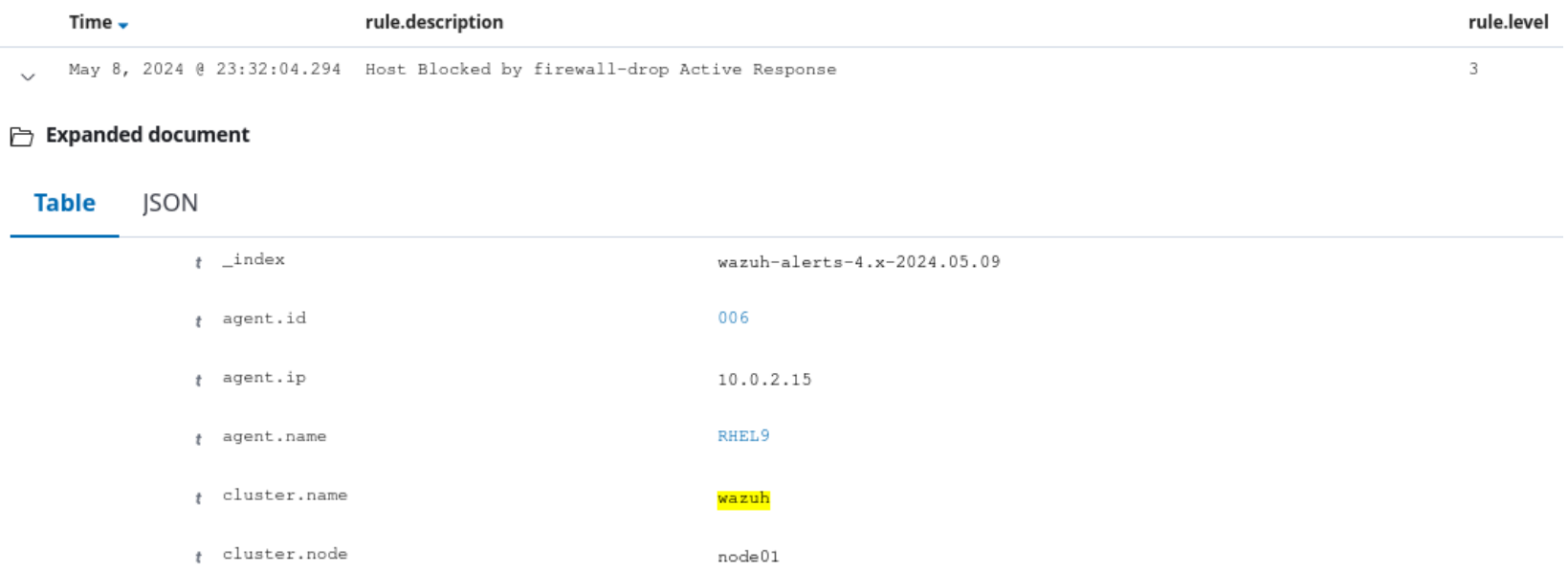
Wazuh in practice

Preconfigured response

A selected detection can trigger a configured response.

Example for ISPs

Temporarily block the source address after repeated SSH login attempts.



Actual Wazuh UI, vendor example

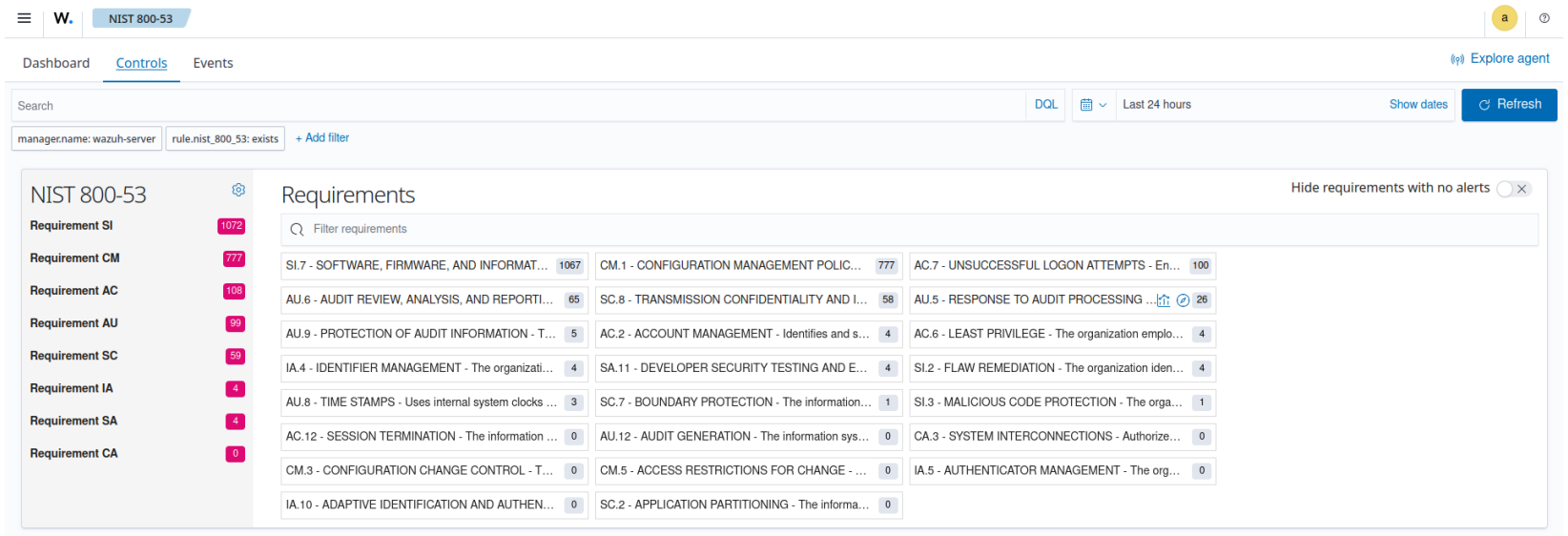
Wazuh in practice

Evidence for audits and reviews

Events and results organized by the selected framework.

Example for ISPs

A regular management overview or evidence for a security audit.



Actual Wazuh UI, vendor example

Wazuh in daily operations

First deployment at a smaller ISP

Initial sources

A bastion host, DNS, the customer portal and one network device.

Initial outputs

Access activity, configuration changes and a vulnerability overview.

Operations

A designated owner, agreed alerts and verification of results.

More from initMAX

initMAX

More examples of Wazuh in practice

Webinars

Practical examples
and recordings.
Free online.

Dates and recordings

Training

Wazuh in practice.
Hands-on labs
and practical guidance.

Courses and dates

Consulting

Your challenge,
pilot or solution
design.

Book a consultation

Questions

www.initmax.com

