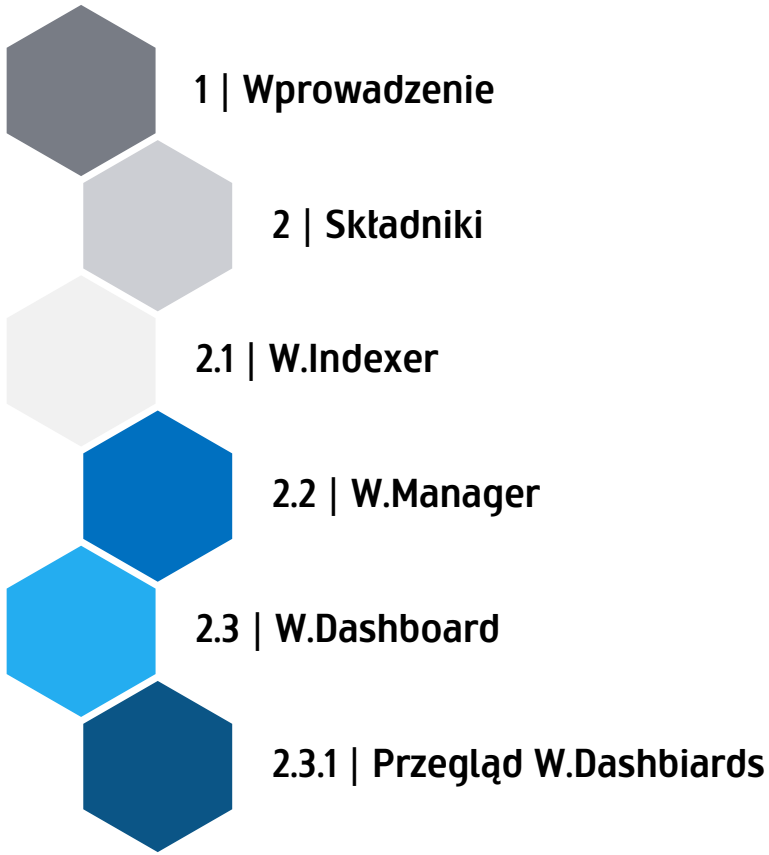
Wazuh: Open Source SIEM dla skutecznej ochrony przed cyberzagrożeniami

Adam Pielak, IT Security, Beyond.pl

Poznań Security Meetup, 09.04.2024

Agenda



1 | Wprowadzenie

2 | Składniki

2.1 | W.Indexer

2.2 | W.Manager

2.3 | W.Dashboard

2.3.1 | Przegląd W.Dashbiards

3 | W.Agents

3.1 | Architektura

3.2 | Komponenty

3.3 | Możliwości

4 | Monitoring logów

5 | Aktywne reagowanie

6 | Integracje

7 | Podsumowanie

Wprowadzenie

- zbudowany na projekcie OSSEC
- rozwijany od ponad 9 lat
- znaczna rozbudowa od samego projektu OSSEC OS
- integracja z innymi narzędziami i usługami

XDR

wazuh.
The Open Source Security Platform

SIEM

Architektura

Wazuh Indexer (OpenSearch fork)

Indeksowanie oraz przechowywanie zdarzeń bezpieczeństwa.

Możliwość konfiguracji jednowęzłowej instancji lub jako wielowęzłowy klaster.

Główe indeksy:

- wazuh-alerts
- wazuh-archives
- wazuh-monitoring
- wazuh-statistics

Wazuh Manager (OSSEC fork)

Główny serwer przetwarzający i identyfikujący zdarzenia bezpieczeństwa które są dostarczane za pośrenidctwem Filebeat do W.Indexer.

Moduły:

- Obsługa agentów
- Silnik analizy
- RESTfulAPI
- Klaster Wazuh
- Filebeat

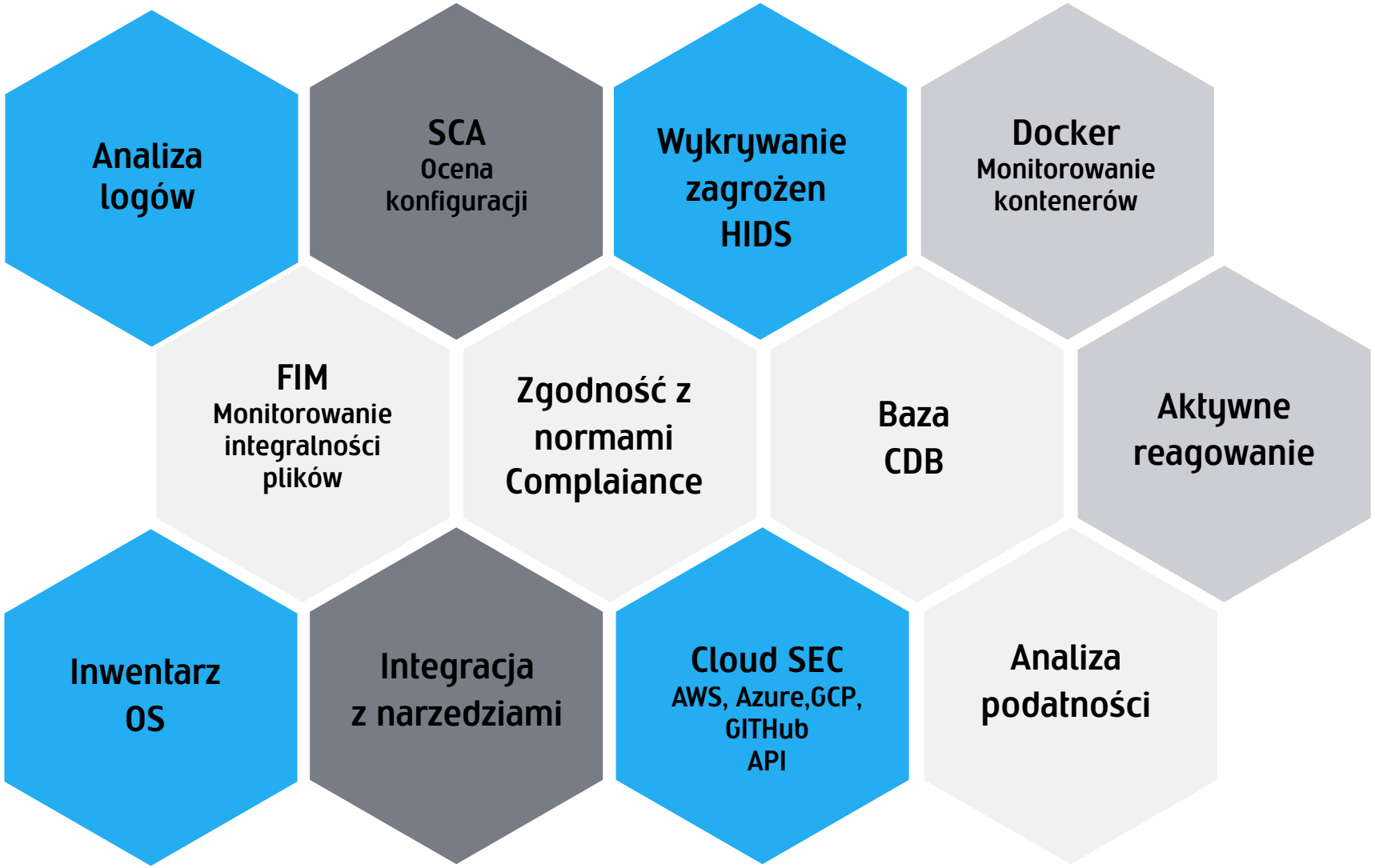
Wazuh Dashboard (OpenSearch Dash. fork)

Wizualizacja przetworzonych danych.

Pulpity podzielone na:

- Zdarzenia bezpieczeństwa
- Zgodności z przepisami
- Podatności
- FIM
- Zarządzanie agentami
- Konfiguracja
- Monitoring, statystyki itp.

Wazuh Manager – Funkcje



Możliwości

Zbieranie danych dziennika

Gromadzenie danych dziennika to proces ciągłego gromadzenia i analizowania rekordów dziennika z serwerów, urządzeń i innych źródeł w czasie rzeczywistym za pośrednictwem plików tekstowych lub dzienników zdarzeń systemu Windows. Może również bezpośrednio odbierać zdalne dzienniki systemowe z zapór ogniowych i podobnych urządzeń.

Wykrywanie podatności

Moduł „Vulnerability Detector" pomaga wykrywać luki w systemie operacyjnym i aplikacjach zainstalowanych na punktach końcowych. Źródła te utrzymują bazy danych znanych luk w zabezpieczeniach obecnych w programach i OS. Są one indeksowane przez Canonical, Debian, Red Hat, Arch, ALAS, Microsoft oraz NVD.

Monitorowanie poleceń

Monitorowanie wyników określonych poleceń, które nie pojawiły się w logach. Aby ta możliwość działała, agent musi akceptować polecenia zdalne od menedżera.

Bezpieczeństwo Dockerów

Platformy kontenerowe są monitorowane poprzez scentralizowane logowanie w czasie rzeczywistym oraz skanowane w poszukiwaniu luk w zabezpieczeniach.

Inwentaryzacja systemu

Zawiera informacje o zasobach monitorowanego środowiska, które są wyświetlane na pulpicie nawigacyjnym agenta.

Możliwości

Monitorowanie integralności plików FIM

Pliki i katalogi mogą być okresowo skanowane pod kątem wszelkich zmian. Konfiguracje powinny być wykonane w agencie i menedżerze Wazuh, aby określić, które ścieżki i katalogi mają być monitorowane.

Wykrywanie złośliwego oprogramowania

Sam FIM nie może wykryć obecności złośliwego oprogramowania w systemie. FIM powinien być połączony z regułami wykrywania zagrożeń, takimi jak YARA i źródłami informacji o zagrożeniachnp. VirusTotal i listą skrótów plików CDB, aby wykryć złośliwe pliki i wzorce, które pokazują obecność złośliwego oprogramowania.

Listy CDB i analiza zagrożeń

Dzięki zastosowaniu listy CDB, która zawiera listę znanych wskaźników zagrożenia złośliwym oprogramowaniem, Wazuh może wykryć obecność złośliwego pliku, jeśli jego sygnatura zostanie znaleziona na liście. Działa to dobrze z FIM, który skanuje w poszukiwaniu wszelkich zmian w ścieżce, plikach lub katalogach.

Integracja VirusTotal

Alerty są wyzwalane, gdy FIM wykryje wszelkie zmiany w monitorowanych folderach, co powoduje, że integracja VirusTotal wyodrębnia wartość skrótu pliku. Hash jest następnie porównywany z bazą danych VirusTotal przy użyciu API. Następnie otrzymuje się odpowiedź, która może wywołać alert, który może zawierać błąd lub wskazywać na obecność złośliwego pliku.

Monitorowanie integralności plików i YARA

YARA to narzędzie do identyfikacji złośliwego oprogramowania i złośliwych plików poprzez dopasowanie wzorców i reguł. W połączeniu z FIM pliki, które powodują alerty, rozpoczynają skanowanie YARA plików i testują je zgodnie z jego zasadami, aby określić, czy są one złośliwym oprogramowaniem, czy nie. Wyniki skanowania zostaną przekazane menedżerowi w celu dekodowania, analizy i powiadamiania. Dekodery muszą zostać dodane do serwera, aby te skany mogły zostać zdekodowane.

Możliwości

Kolekcja dzienników Windows Defender i innych AV

Agenci w punktach końcowych systemu Windows mogą być skonfigurowani do zbierania dzienników Windows Defender, które zawierają stan usługi i wyniki skanowania na punktach końcowych.

Monitorowanie polityki bezpieczeństwa

Zapewnia, że wszystkie monitorowane punkty końcowe są zgodne z predefiniowanymi regułami dotyczącymi ustawień konfiguracji i zatwierdzonego użytkowania aplikacji (*Rootcheck*, *OpenSCAP* i *CIS-CAT*)

Niestandardowe reguły wykrywania złośliwego oprogramowania IOC

Pozwala na zbudowanie niestandardowego zestawu reguł w celu wykrywania nowych wariantów złośliwego oprogramowania, które mają nowe wskaźniki i wzorce zachowań.

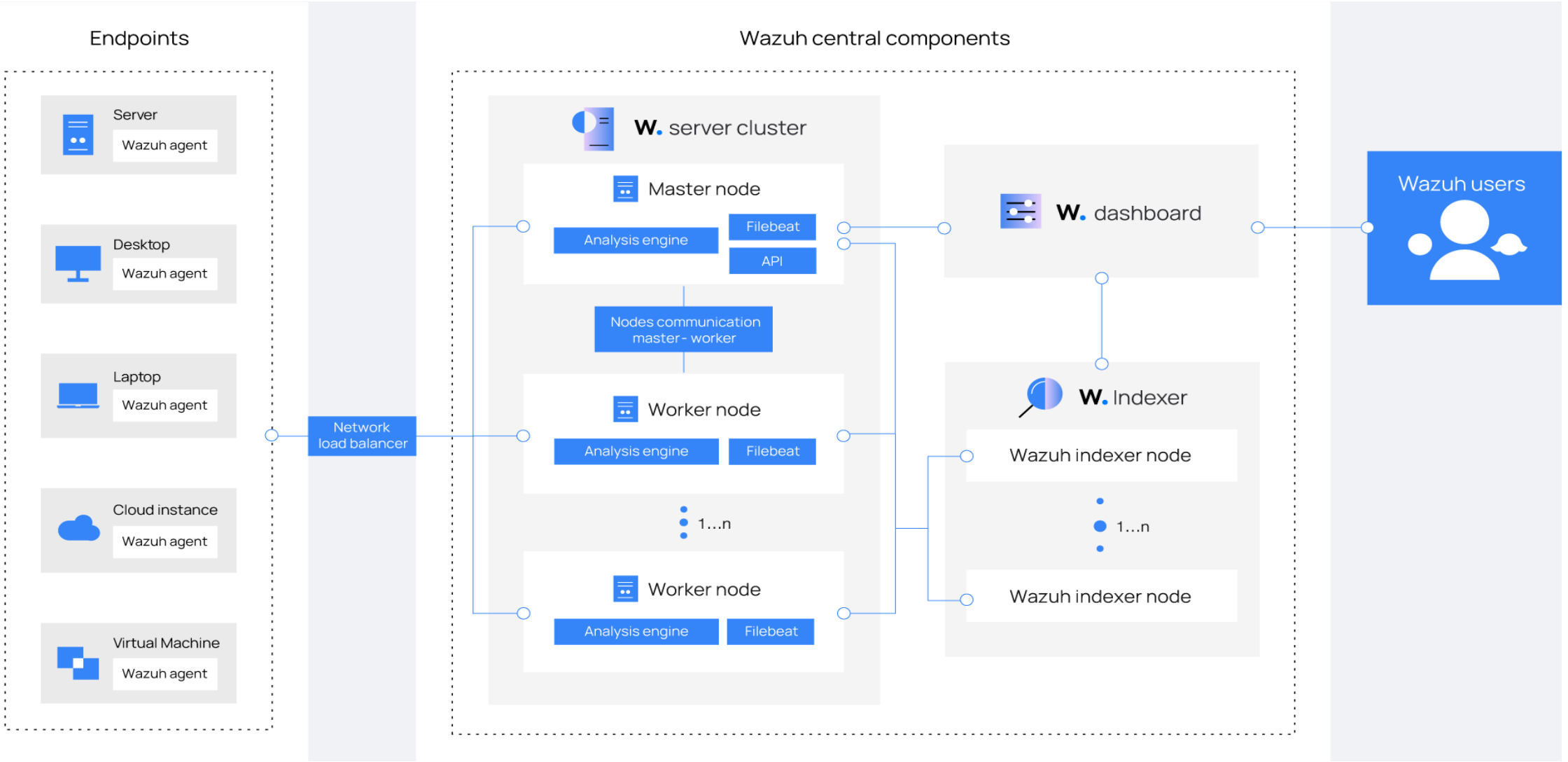
Ocena konfiguracji bezpieczeństwa

Hardening to proces zabezpieczania punktów końcowych poprzez zmniejszenie ich powierzchni podatności. Ocena konfiguracji bezpieczeństwa (SCA) analizuje i potwierdza, czy system przestrzega z góry określonych ustawień konfiguracji aplikacji. Moduł SCA przeprowadza amnalizę w celu zidentyfikowania wszelkich błędnych konfiguracji i słabości w punkcie końcowym oraz zaleca środki zaradcze.

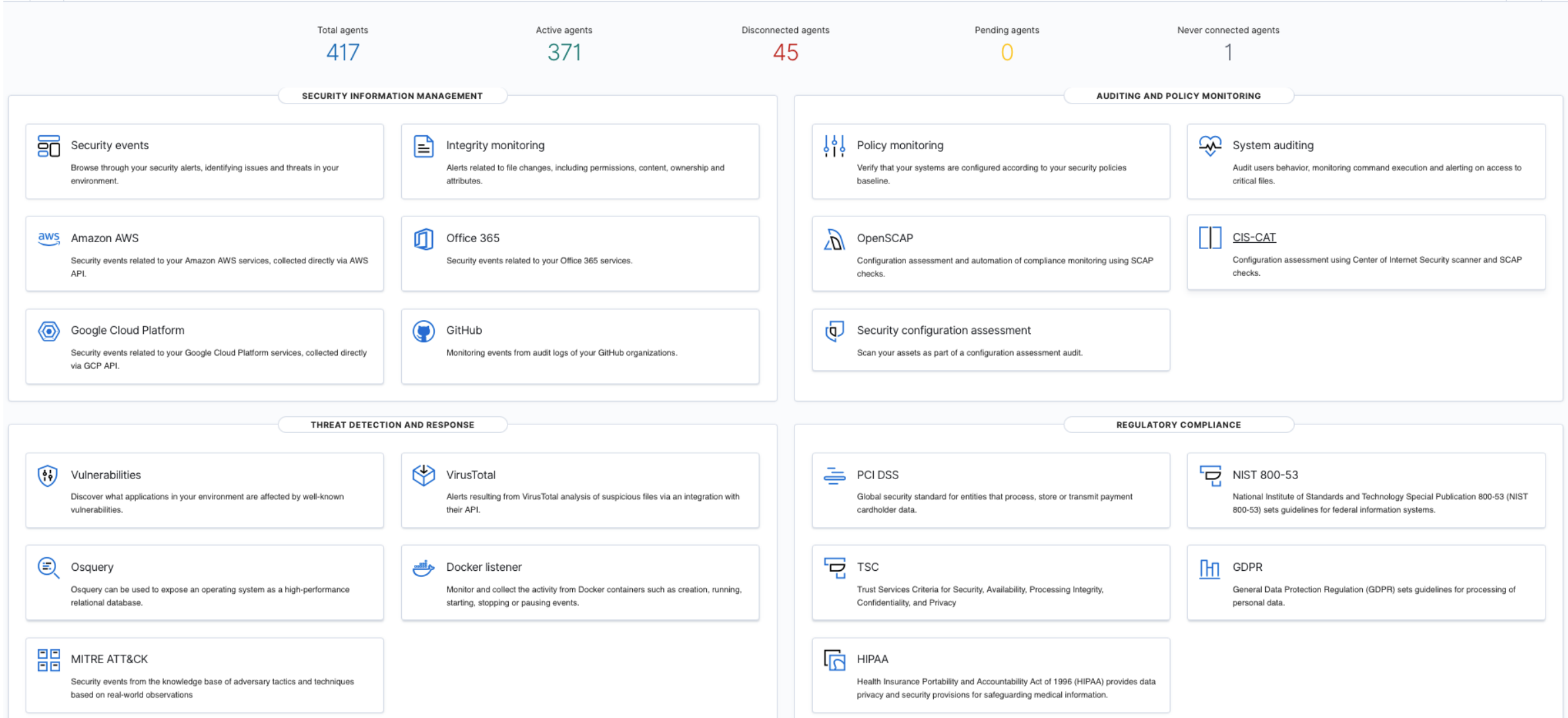
Aktywna reagowanie na zagrożenia

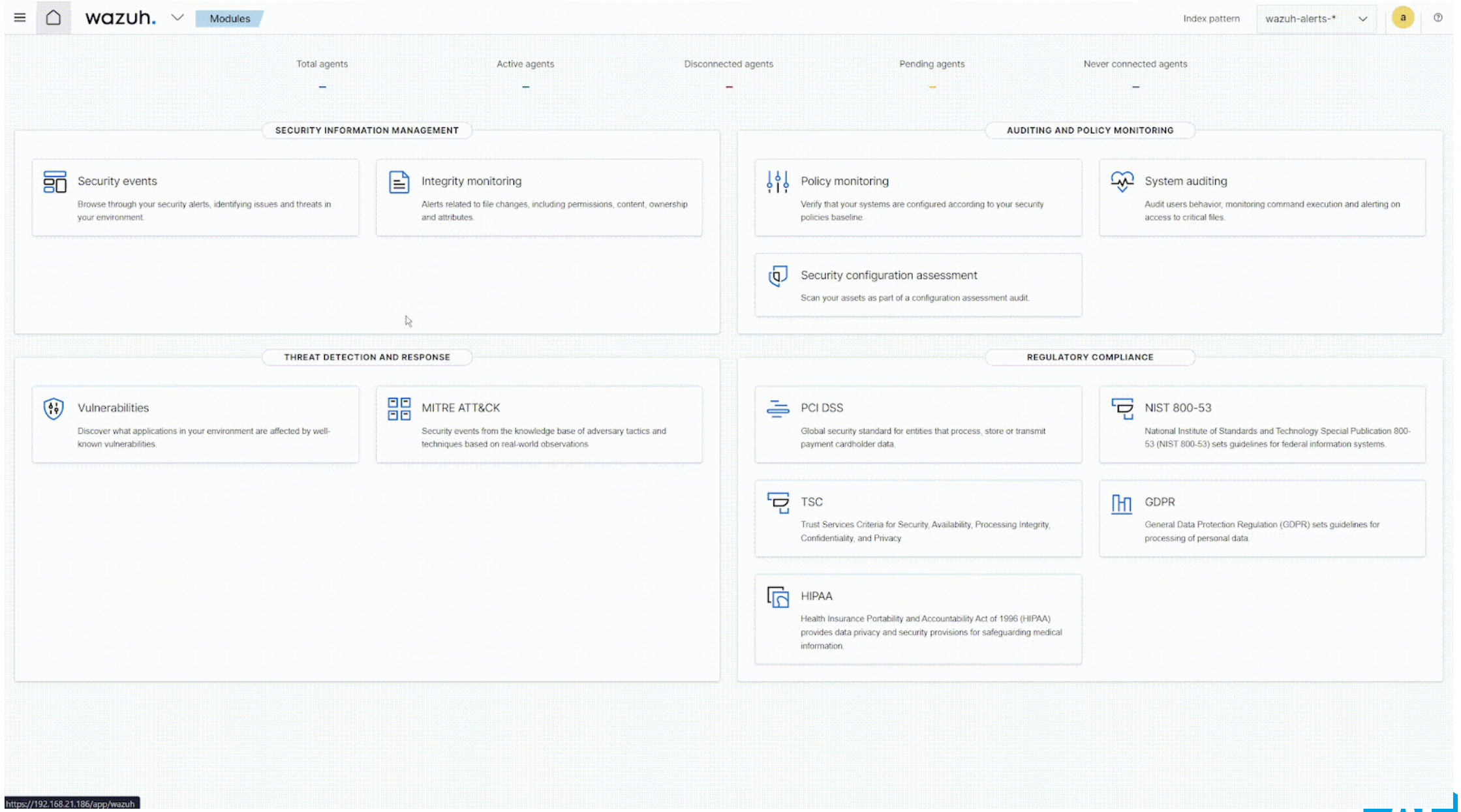
Korzyści z aktywnej reakcji obejmują: zapewnienie wglądu w zdarzenia bezpieczeństwa w czasie rzeczywistym, zmniejszenie ilości alarmów, automatyzację działań reagowania na zagrożenia, dostarczanie nieszablonowych skryptów odpowiedzi.

Architektura



Wazuh Dashboard



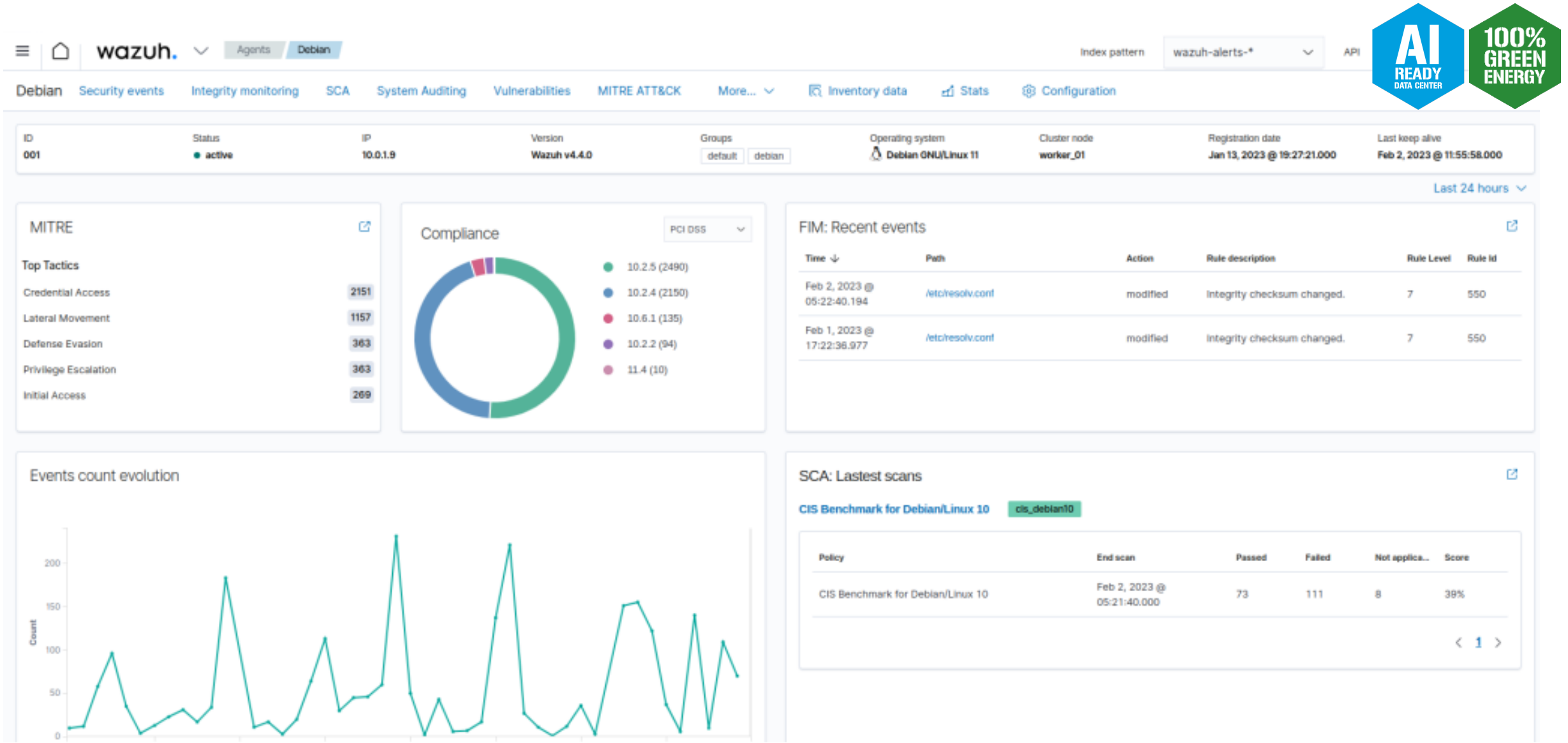


Wazuh Agent & Agentless

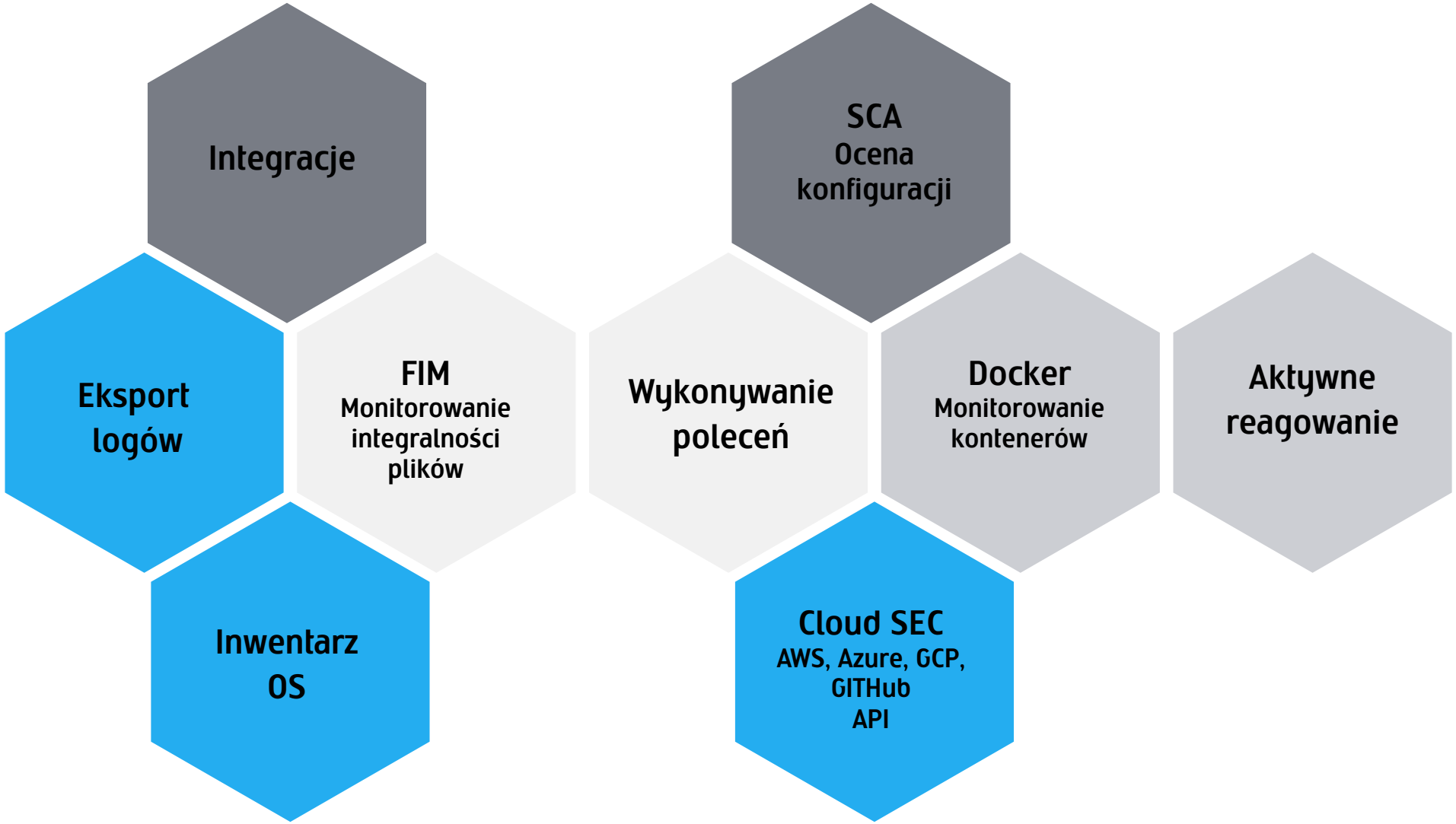
Agenci dostępni na różne platformy




- Połączenia Agent–Manager port tcp/udp 1514 szyfrowanie AES (dla każdego z agentów)
- Serwer może akceptować połączenia po porcie 514 (syslog).
- W celu scentralizowania zbierania logów, serwer syslog może również być uruchomiony na Agencie jak i Managerze.


wazuh.
Agents
Debian
Index pattern
wazuh-alerts-*
API
Debian
Security events
Integrity monitoring
SCA
System Auditing
Vulnerabilities
MITRE ATT&CK
More...
Inventory data
Stats
Configuration
ID
001
Status
active
IP
10.0.1.9
Version
Wazuh v4.4.0
Groups
default
debian
Operating system
Debian GNU/Linux 11
Cluster node
worker_01
Registration date
Jan 13, 2023 @ 19:27:21.000
Last keep alive
Feb 2, 2023 @ 11:55:58.000
Last 24 hours
MITRE
Top Tactics
Credential Access 2151
Lateral Movement 1157
Defense Evasion 363
Privilege Escalation 363
Initial Access 269
Compliance
PCI DSS
10.2.5 (2490)
10.2.4 (2150)
10.6.1 (135)
10.2.2 (94)
11.4 (10)
FIM: Recent events
Time
Path
Action
Rule description
Rule Level
Rule Id
Feb 2, 2023 @ 05:22:40.194
/etc/resolv.conf
modified
Integrity checksum changed.
7
550
Feb 1, 2023 @ 17:22:38.977
/etc/resolv.conf
modified
Integrity checksum changed.
7
550
Events count evolution
Count
200
150
100
50
0
SCA: Lastest scans
CIS Benchmark for Debian/Linux 10
cis_debian10
Policy
End scan
Passed
Failed
Not applica...
Score
CIS Benchmark for Debian/Linux 10
Feb 2, 2023 @ 05:21:40.000
73
111
8
38%
1

Komponenty Wazuh Agent



Monitorowanie logów oraz danych wyjściowych

```
<localfile>
   <log_format>syslog</log_format>
   <location>/var/log/messages</location>
</localfile>
```

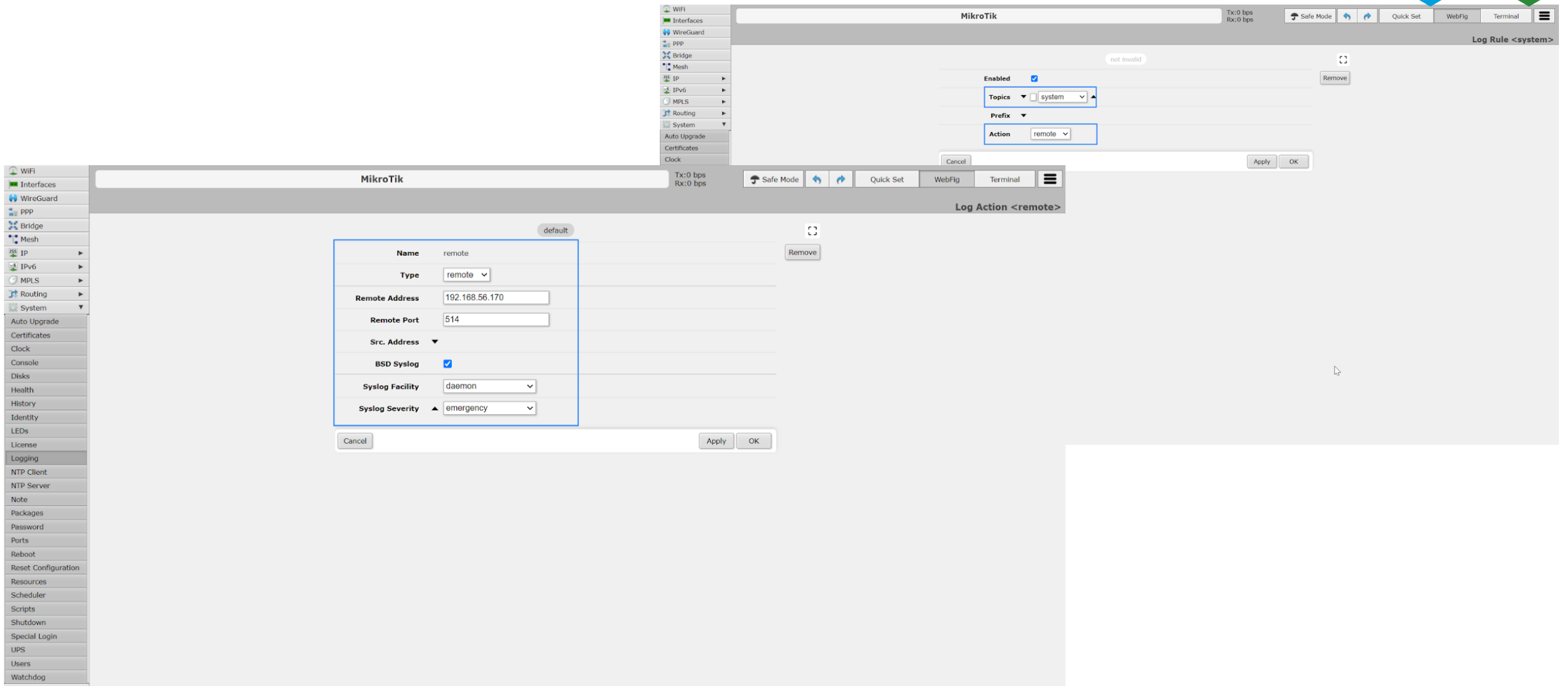
```
<localfile>
  <log_format>eventchannel</log_format>
  <location>Application</location>
</localfile>
```

```
<localfile>
  <log_format>json</log_format>
  <location>/var/log/suricata/eve-*.json</location>
  <label key="@source">suricata</label>
</localfile>
```

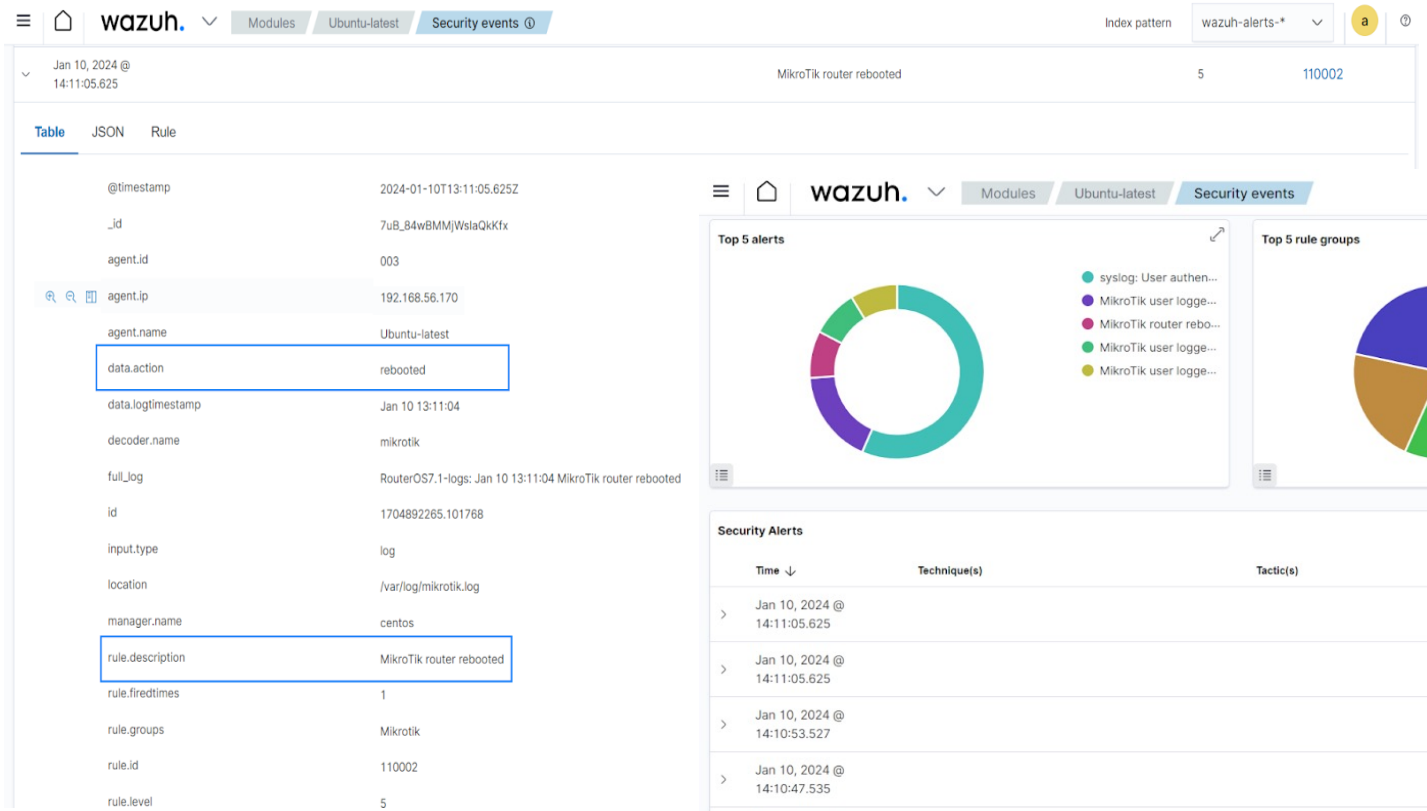
```
<localfile>
   <log_format>full_command</log_format>
   <command>netstat -natp | grep '^tcp .*LISTEN ' | sort | sed 's/LISTEN \+[0-9]\+\///g'
   | grep -v "127.0.0.1:" | awk '{print $4"\t"$6}'</command>
   <frequency>300</frequency>
   <alias>netstat listening ports</alias>
</localfile>
```

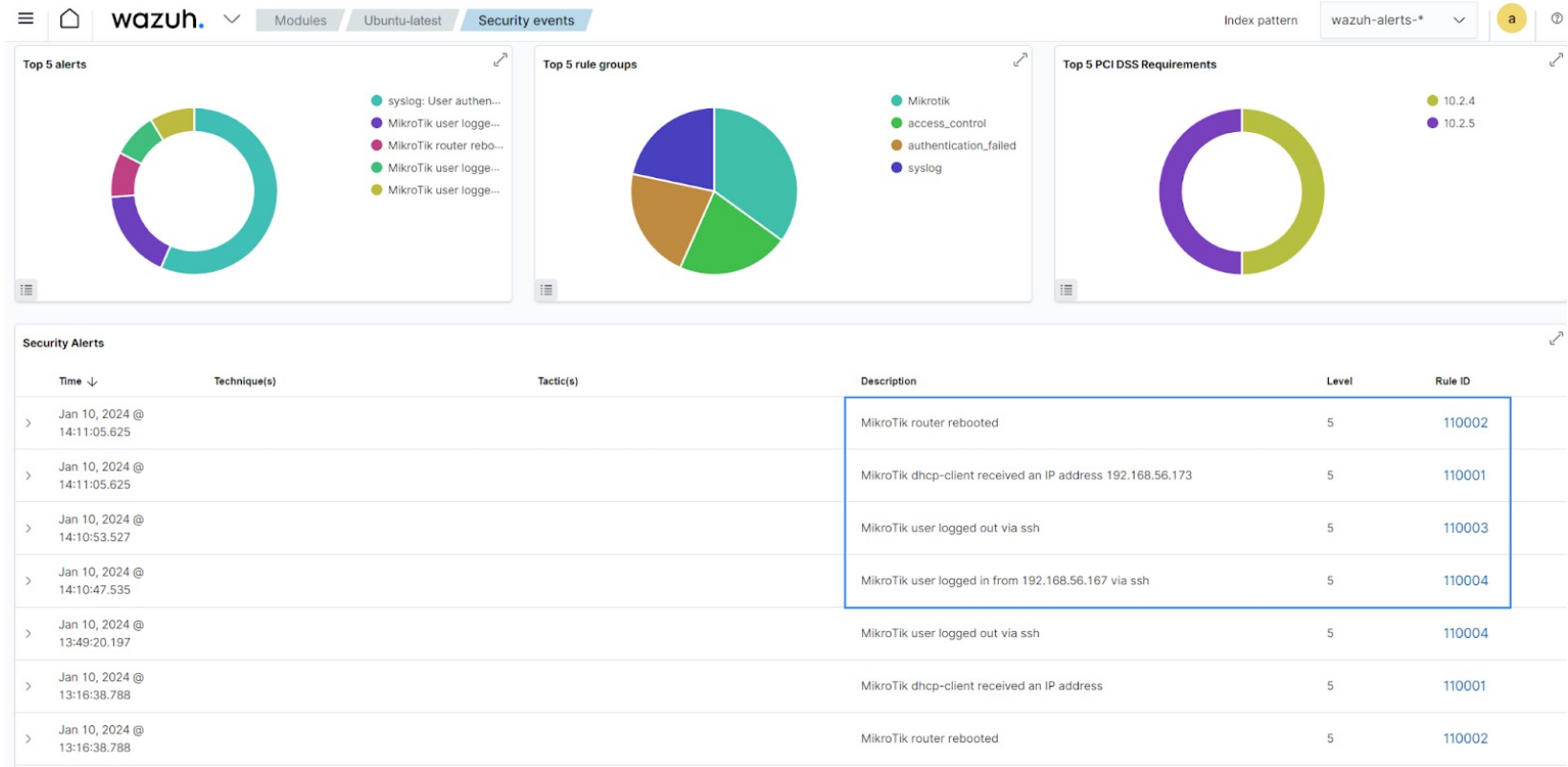
```
<rule id="533" level="7">
  <if_sid>530</if_sid>
  <match>ossec: output: 'netstat listening ports</match>
  <check_diff />
  <description>Listened ports status (netstat) changed (new port opened or closed).
  </description>
  <group>pci_dss_10.2.7,pci_dss_10.6.1,gpg13_10.1,gdpr_IV_35.7.d,hipaa_164.312.b,
  nist_800_53_AU.14,nist_800_53_AU.6,tsc_CC6.8,tsc_CC7.2,tsc_CC7.3,</group>
</rule>
```

Monitoring syslog – Mikrotik



Monitoring syslog – Mikrotik





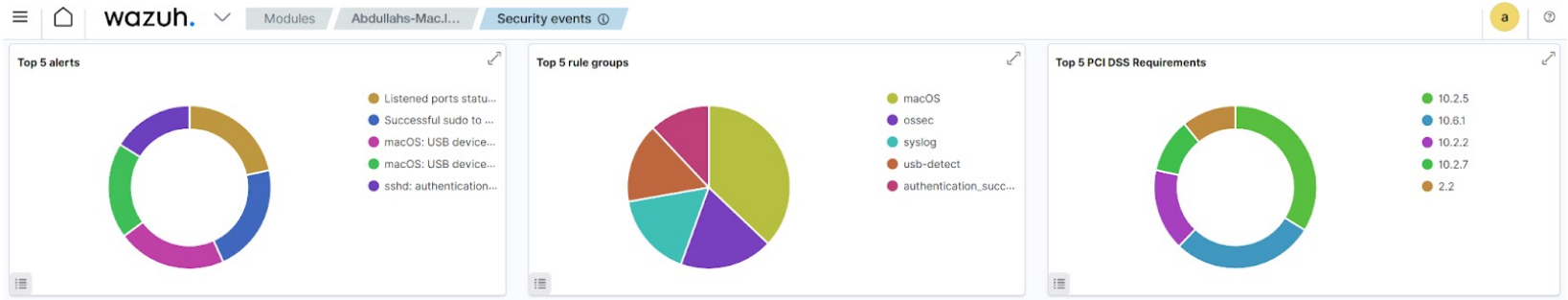
Mikrotik Agentless – Active Response

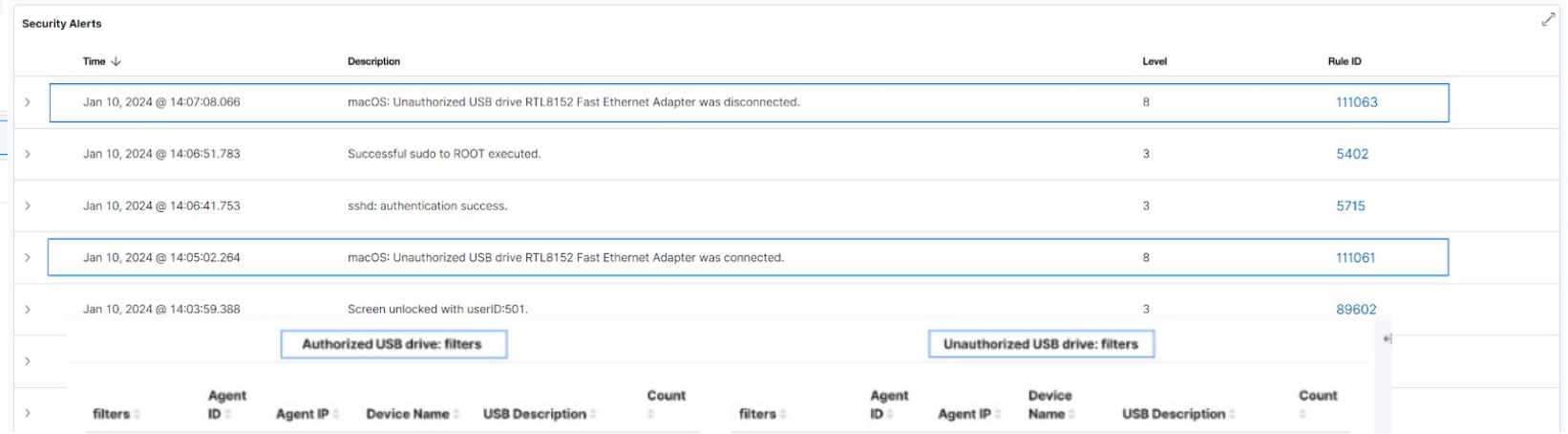
```
echo "`date` $0 $ALERT" >> $LOG_AR

if [[ $ACTION == "add" ]]; then
        # Send control message to execd
        printf '{"version":1,"origin":{"name":"remove-threat","module":"active-response"},"command":"check_keys", "parameters":{"keys":["$IP"]}}\n'

        read RESPONSE
        COMMAND2=$(echo $RESPONSE | jq -r .command)
        if [ ${COMMAND2} != "continue" ]; then
                echo "`date '+%Y/%m/%d %H:%M:%S'` $0: $ALERT" >> ${LOG_AR}
                exit 0;
        fi
        ssh -i $SSH_KEY -l $SSH_USER $IP_MIKROTIK /ip firewall filter add action=drop chain=input src-address=$IP comment=$ALERT_ID
elif [[ $ACTION == "delete" ]]; then
        ssh -i $SSH_KEY -l $SSH_USER $IP_MIKROTIK /ip firewall filter remove [find comment=$ALERT_ID]
else
        echo "`date` $0 'Unable to run - '$ALERT" >> $LOG_AR
fi
```

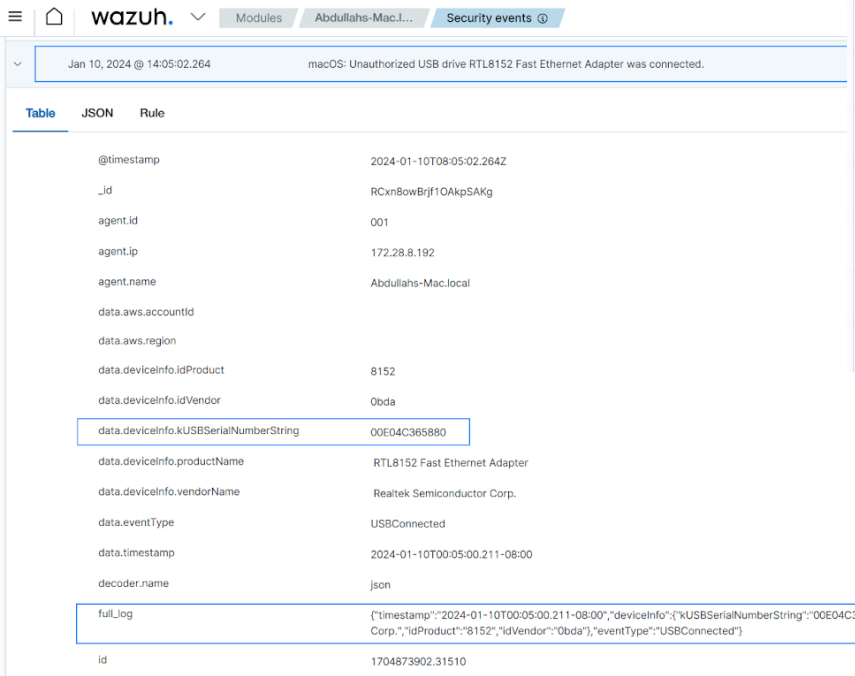
Jan 10, 2024 @ 14:11:05.625	MikroTik dhcp-client received an IP address 192.168.56.173	5	110001
Jan 10, 2024 @ 14:10:53.527	MikroTik user logged out via ssh	5	110003
Jan 10, 2024 @ 14:10:47.535	MikroTik user logged in from 192.168.56.167 via ssh	5	110004
Jan 10, 2024 @ 13:49:20.197	MikroTik user logged out via ssh	5	110004
Jan 10, 2024 @ 13:16:38.788	MikroTik dhcp-client received an IP address	5	110001
Jan 10, 2024 @ 13:16:38.788	MikroTik router rebooted	5	110002

Monitoring USB

```
<!-- Rule for USB monitoring in Linux-->
<group name="Linux, usb,">
  <rule id="111010" level="7">
    <field name="serial">\w+</field>
    <field name="type">usb_device</field>
    <description>A PNP device $(vendor) $(model) was connected to $(hostname).</description>
  </rule>

  <rule id="111011" level="8">
    <if_sid>111010</if_sid>
    <list field="serial" lookup="not_match_key">etc/lists/usb-drives</list>
  <description>Unauthorized PNP device $(vendor) $(model) was connected to $(hostname).</descriptio
  </rule>
</group>
```







Authorized USB drive: filters

filters	Agent ID	Agent IP	Device Name	USB Description	Count
Authorized USB drive	003	172.28.8.139	WIN11LAB	ADATA USB Flash Drive USB Device	6
Authorized USB drive	003	172.28.8.139	WIN11LAB	USB Mass Storage Device	3
Authorized USB drive	003	172.28.8.139	WIN11LAB	ADATA	2
Authorized USB drive	003	172.28.8.139	WIN11LAB	Volume	2
Authorized USB drive	004	172.28.8.158	WIN-IEPF03BFT0D	ADATA USB Flash Drive USB Device	1
					14

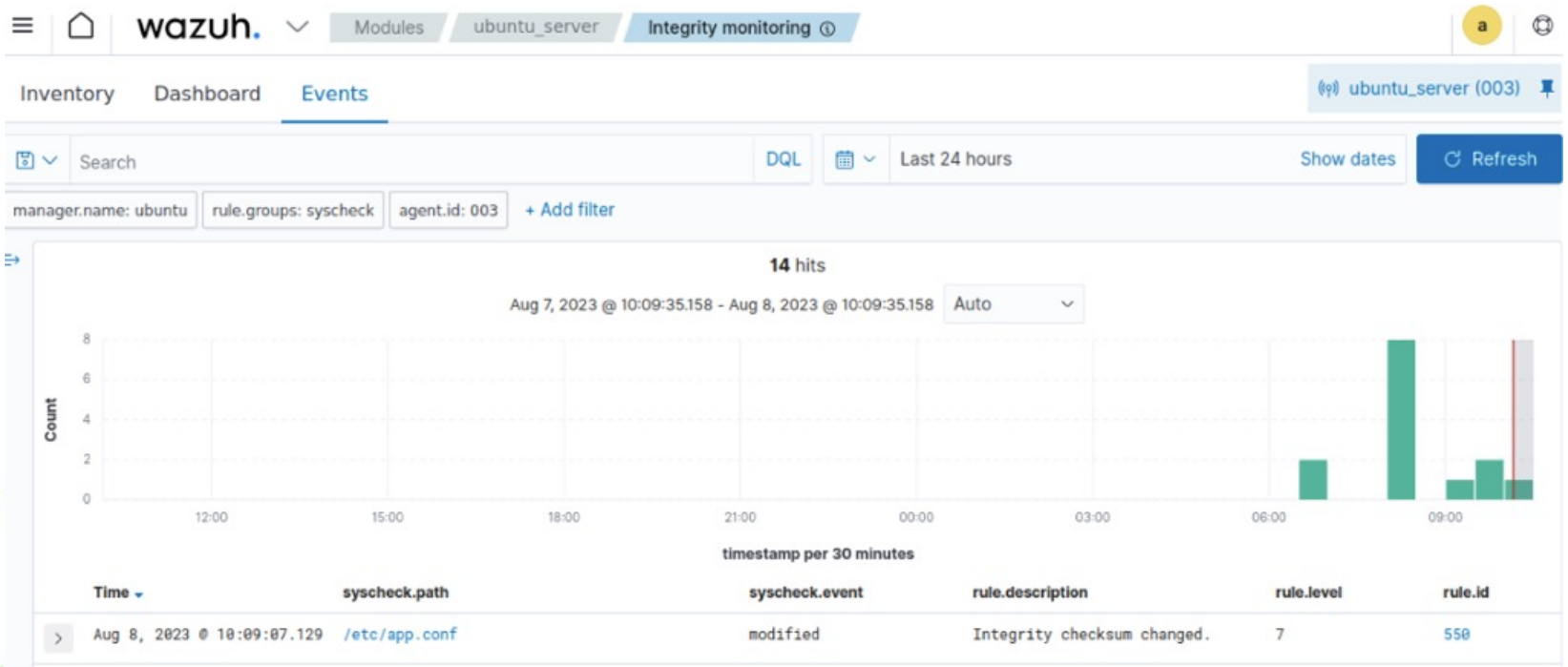
Export: Raw Formatted

Unauthorized USB drive: filters

filters	Agent ID	Agent IP	Device Name	USB Description	Count
Unauthorized USB drive	003	172.28.8.139	WIN11LAB	Volume	10
Unauthorized USB drive	003	172.28.8.139	WIN11LAB	New Volume	6
Unauthorized USB drive	003	172.28.8.139	WIN11LAB	WDC WD10 JPVX-75JC3T0 USB Device	6
Unauthorized USB drive	003	172.28.8.139	WIN11LAB	ADATA USB Flash Drive USB Device	3
Unauthorized USB drive	003	172.28.8.139	WIN11LAB	USB Mass Storage Device	3
					28

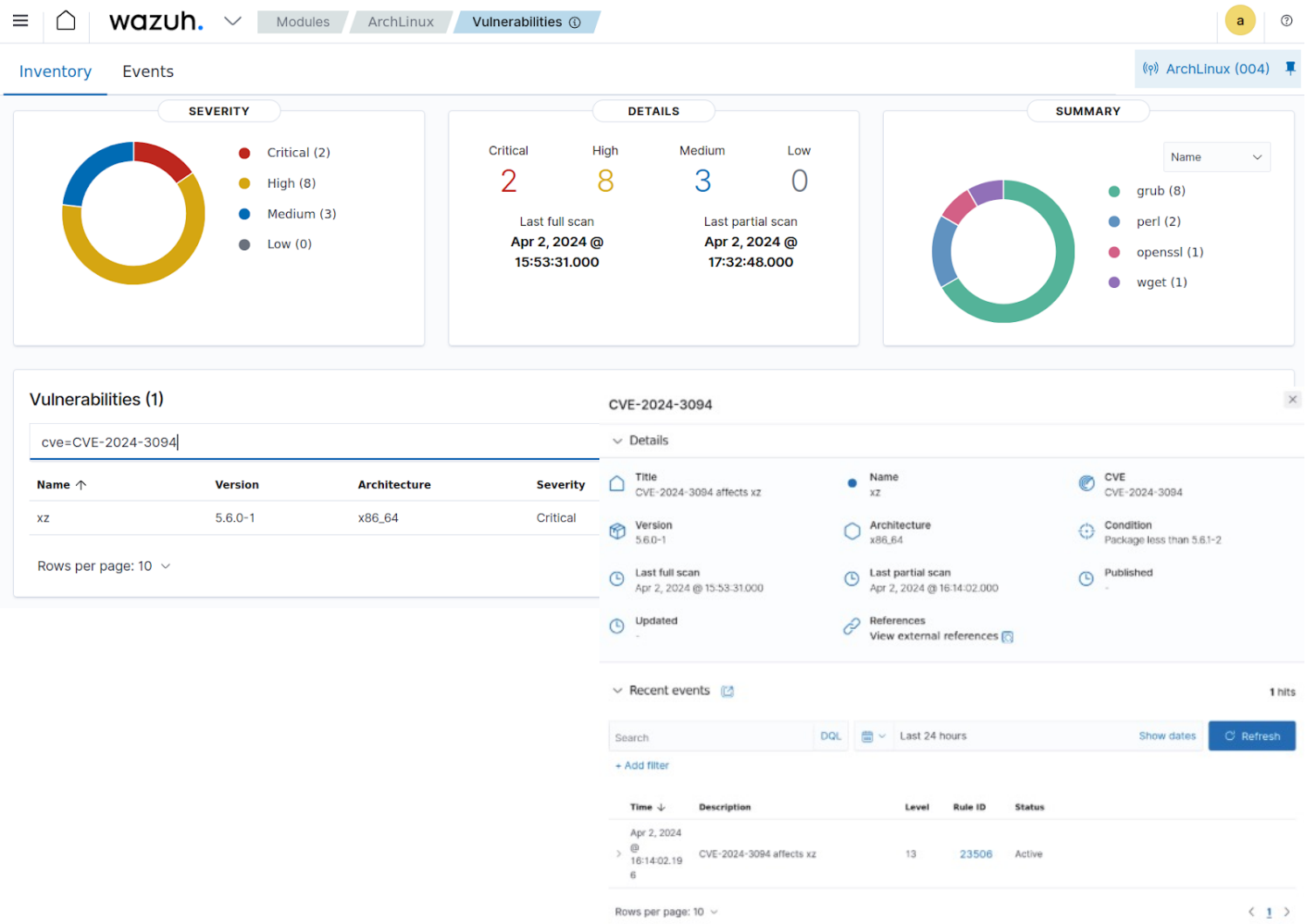
Export: Raw Formatted

Monitorowanie zmian konfiguracji FIM



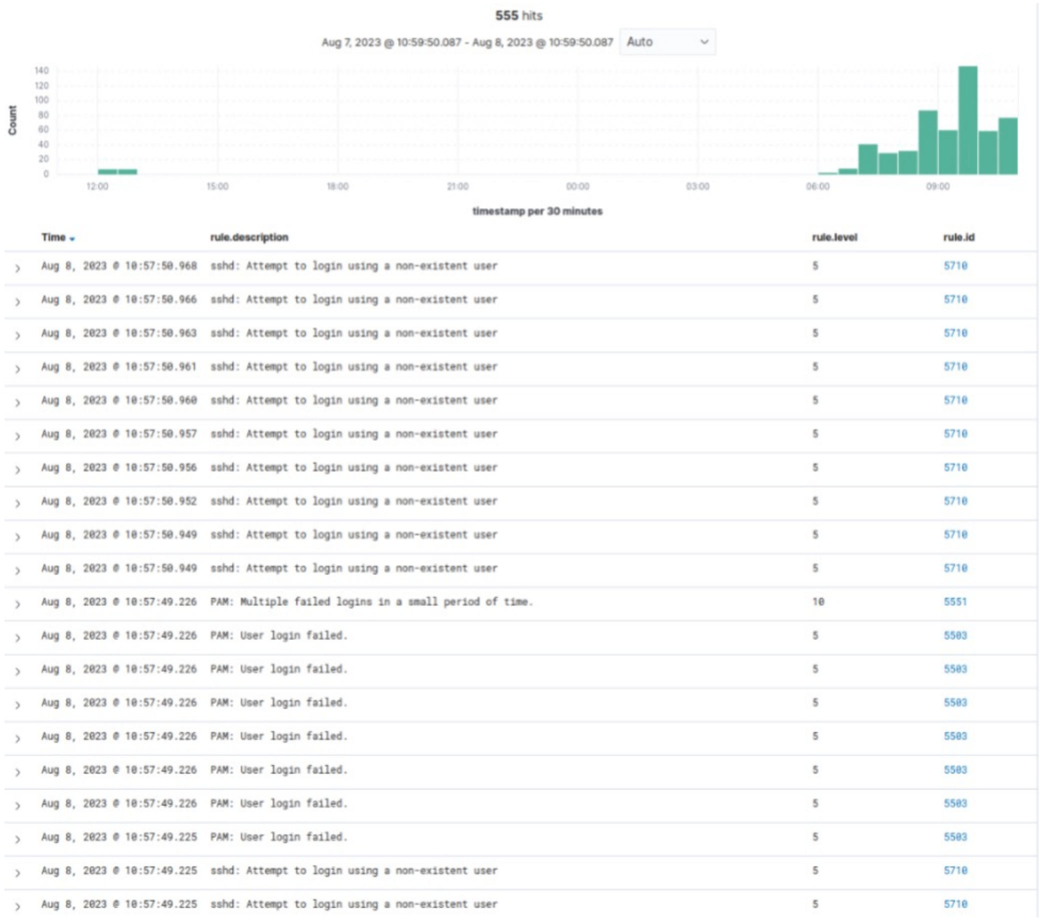

```
<!-- File integrity monitoring -->
<syscheck>
  <disabled>no</disabled>

  <!-- Frequency that syscheck is executed default every
  <frequency>43200</frequency>

  <scan_on_start>yes</scan_on_start>

  <!-- Directories for monitoring-->
  <directories check_all="yes" report_changes="yes" realtime="yes" whodata="yes">/tmp</directories>


  <!-- Detecting account manipulation -->
  <directories whodata="yes">/home/*/.ssh/authorized_keys</directories>

  <!-- Monitoring configuration changes -->
  <directories check_all="yes" report_changes="yes" whodata="yes">/etc/app.conf</directories>

  <!-- Reporting file changes -->
  <directories check_all="yes" report_changes="yes" realtime="yes" whodata="yes">/appfolder</directories>
  <nodiff>/appfolder/private-file.conf</nodiff>
```

Analiza podatności – XZ CVE-2024-3094

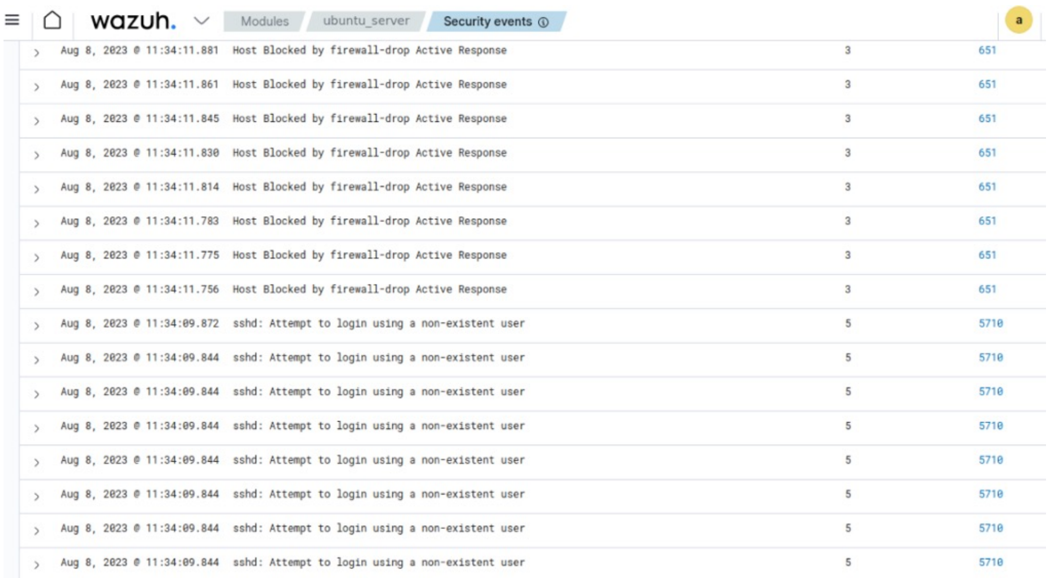



```
<vulnerability-detector>
    <enabled>yes</enabled>
    <interval>5m</interval>
    <min_full_scan_interval>6h</min_full_scan_interval>
    <run_on_start>yes</run_on_start>

    <!-- Ubuntu OS vulnerabilities -->
    <provider name="canonical">
      <enabled>yes</enabled>
      <os>trusty</os>
      <os>xenial</os>
      <os>bionic</os>
      <os>focal</os>
      <os>jammy</os>
      <update_interval>1h</update_interval>
    </provider>

    <!-- Debian OS vulnerabilities -->
    <provider name="debian">
      <enabled>yes</enabled>
      <os>buster</os>
      <os>bullseye</os>
      <os>bookworm</os>
      <update_interval>1h</update_interval>
    </provider>
```

Wykrycie oraz reakcja na ataki




```
<command>
 <name>firewall-drop</name>
 <executable>firewall-drop</executable>
 <timeout_allowed>yes</timeout_allowed>
</command>

<ossec_config>
  <active-response>
    <command>firewall-drop</command>
    <location>local</location>
    <rules_id>5763</rules_id>
    <timeout>180</timeout>
  </active-response>
</ossec_config>
```



Integracje

SHUFFLE

Security orchestration

Threat intelligence and detection

W. server

External alerting and incident response

SURICATA

TheHive

VIRUSTOTAL

Artificial intelligence

AbuseIPDB

slack

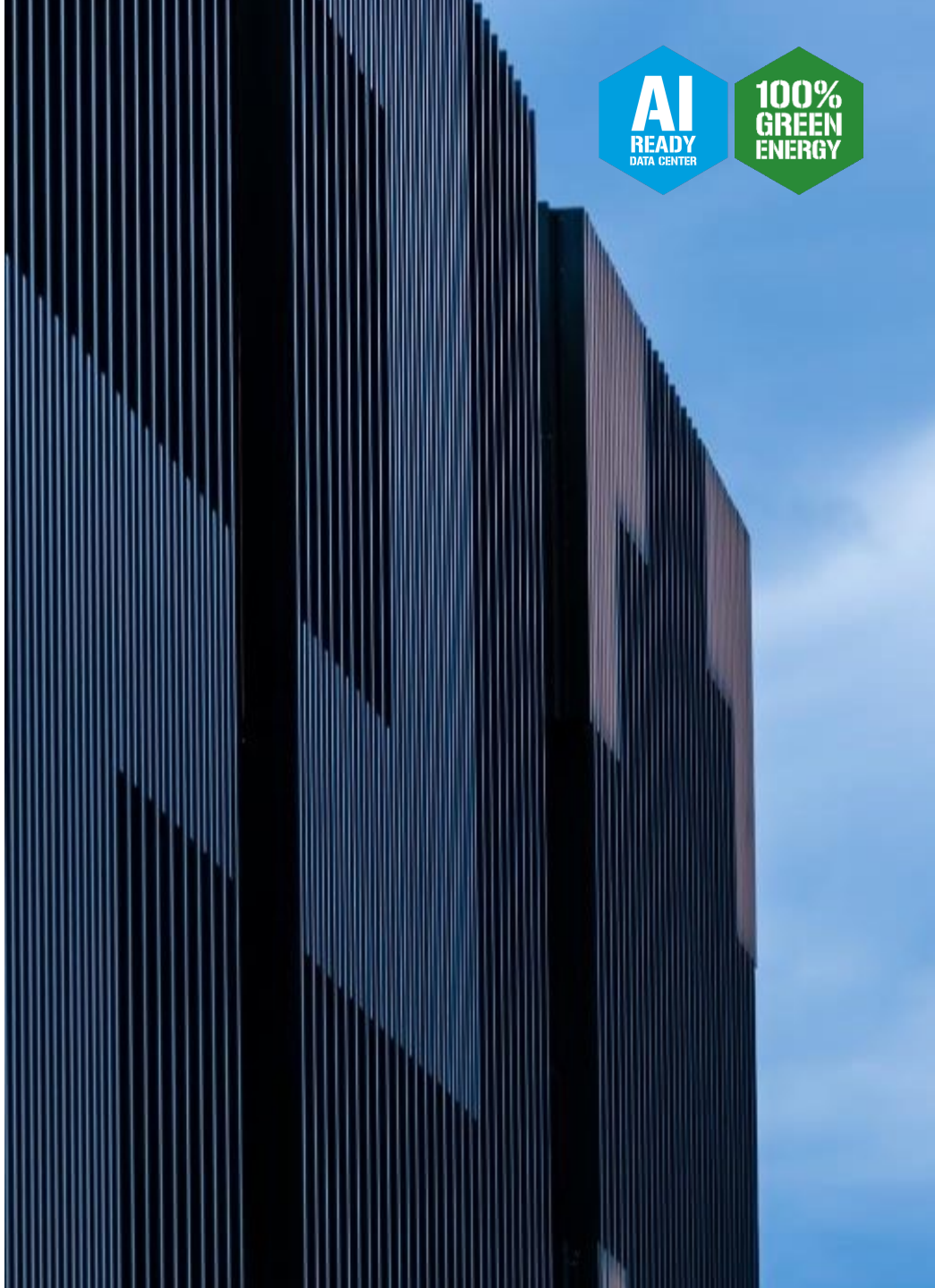
yara

OpenAI

PagerDuty

Podsumowanie Wazuh i obserwacje

- OpenSource + Społeczność (Google Groups, Slack, Discord, Github)
- Edycja reguł/ dekoderów/ konfiguracji wymaga przeładowanie daemona Wazuh (klaster W.Manager)
- Multi-master (rekonfiguracja W.Manager)
- Rozkładanie ruchu (HAProxy, Nginx)
- Synchronizacja konfiguracji (klaster W.Manager)
- Monitoring (Zabbix)
- Reguły i dekodery – próg wejścia dla niestandardowych usług
- Optymalizacja reguł



Wizja Beyond.pl

Być najbardziej zaufanym i szanowanym dostawcą usług przetwarzania danych, Managed Services, środowisk chmurowych i infrastruktury as a service w Polsce i Europie Środkowo-Wschodniej.

Beyond.pl zapewnia najwyższy poziom bezpieczeństwa i ciągłości dostępu do danych, pozwalając klientom i partnerom budować przewagę konkurencyjną, wprowadzać innowacje i stabilnie się rozwijać

Dziękuję za uwagę

Adam Pielak, IT Security
e-mail: a.pielak@beyond.pl

www.beyond.pl