



PARTNERZY



ORGANIZACJE

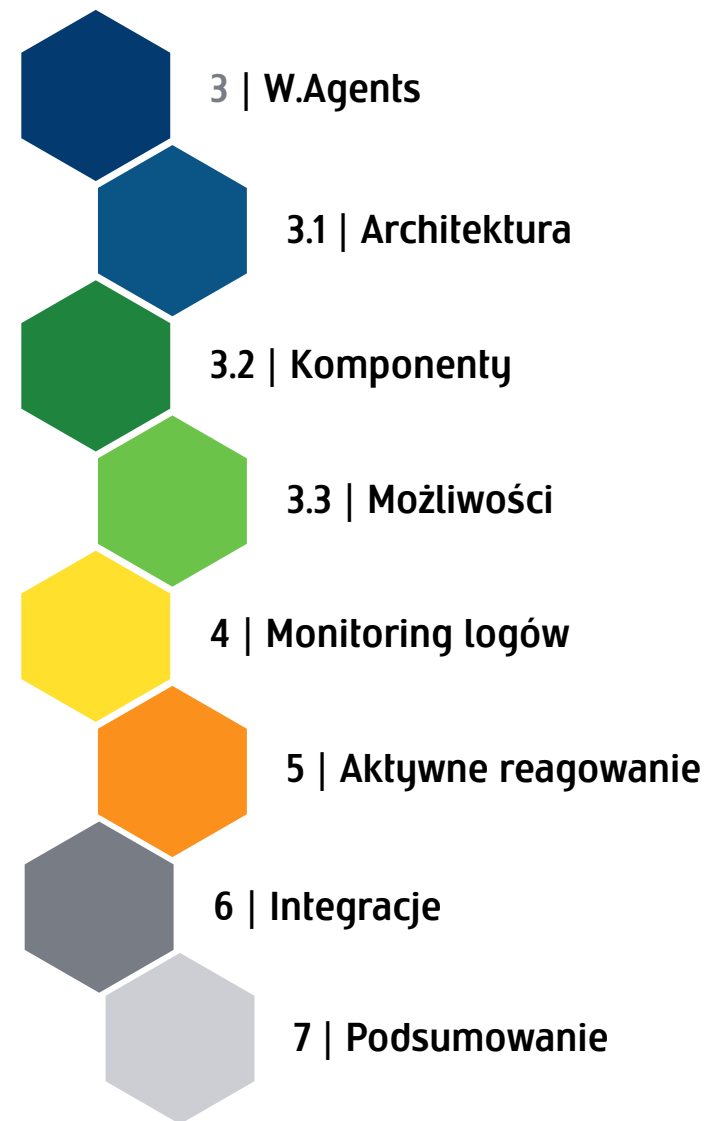
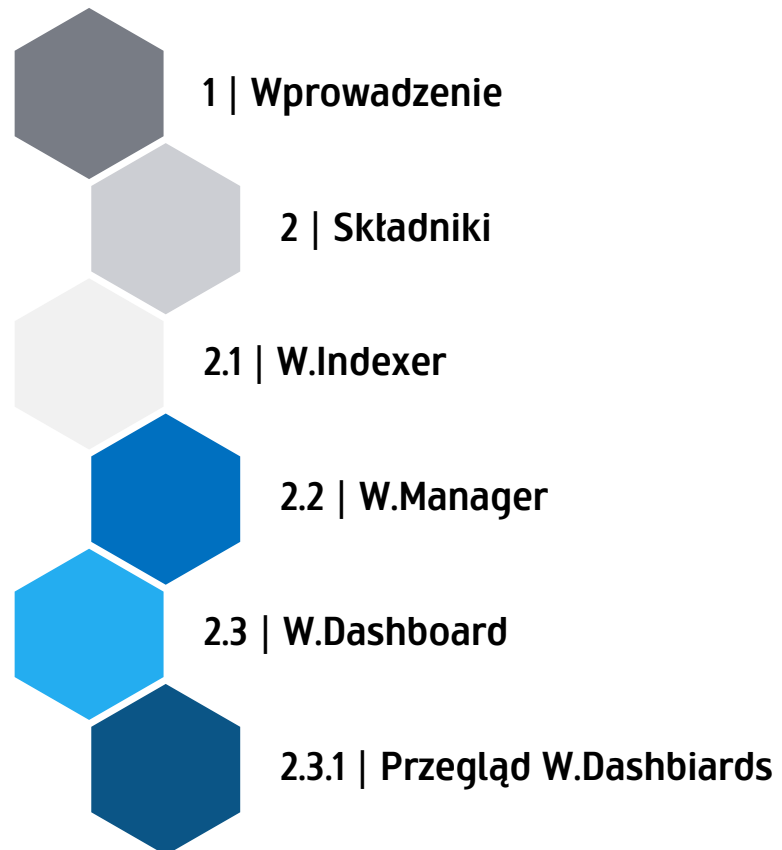


# Wazuh: Open Source SIEM dla skutecznej ochrony przed cyberzagrozeniami

Adam Pielak, IT Security, Beyond.pl

Poznań Security Meetup, 09.04.2024

# Agenda



# Wprowadzenie

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



**wazuh.**  
The Open Source Security Platform





## Wazuh Indexer (OpenSearch fork)

Indeksowanie oraz przechowywanie zdarzeń bezpieczeństwa.

Możliwość konfiguracji jednowęzłowej instancji lub jako wielowęzłowy klaster.

Główne indeksy:

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



## Wazuh Manager (OSSEC fork)

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

Moduły:

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



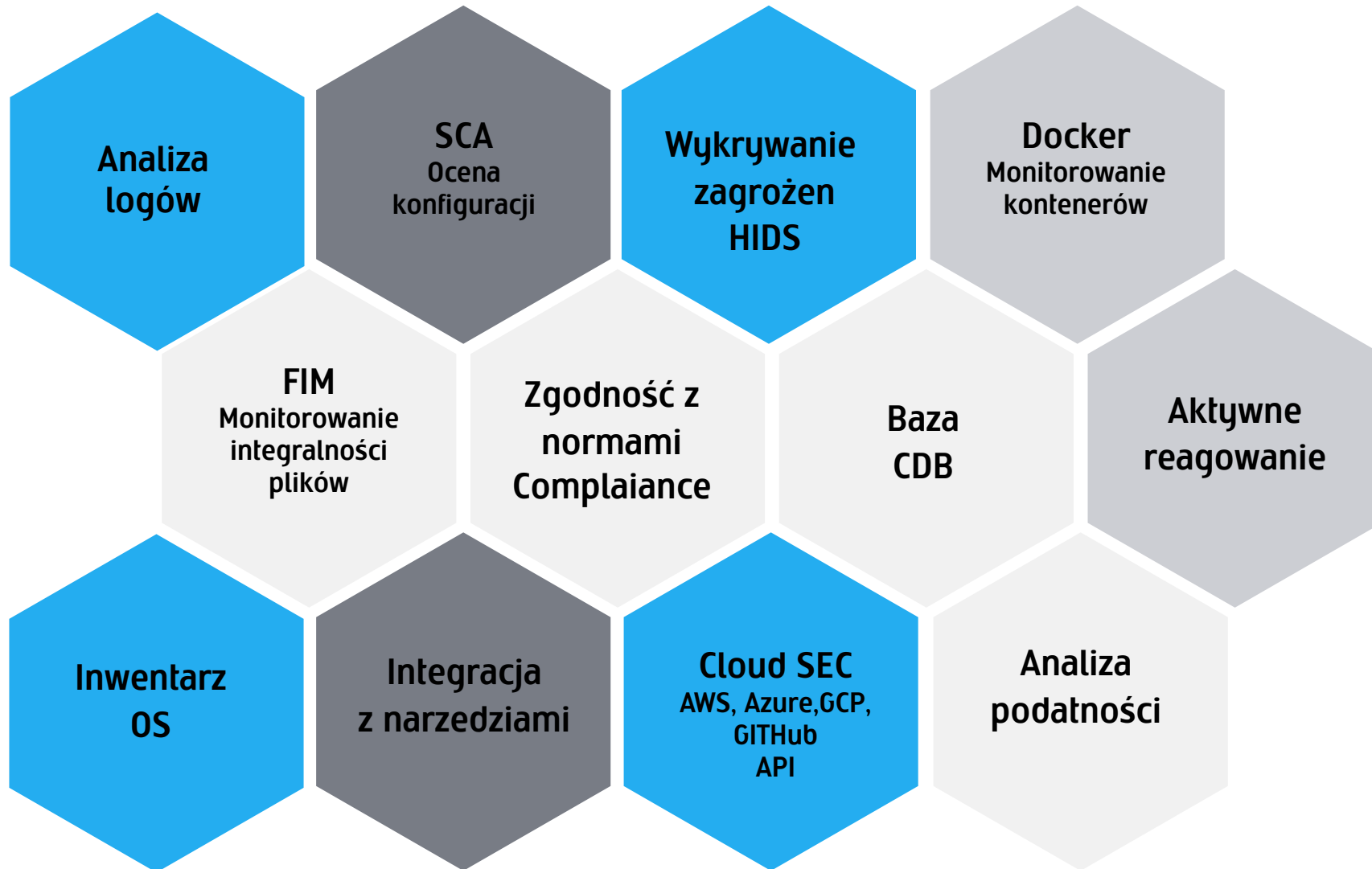
## Wazuh Dashboard (OpenSearch Dash. fork)

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.



## Monitorowanie integralności plików FIM

Pliki i katalogi mogą być okresowo skanowane pod kątem wszelkich zmian. Konfiguracje powinny być wykonane w agencji 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 zagrożeniach np. 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 użytkownika 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 analizę w celu zidentyfikowania wszelkich błędnych konfiguracji i słabości w punkcie końcowym oraz zaleca środki zaradcze.

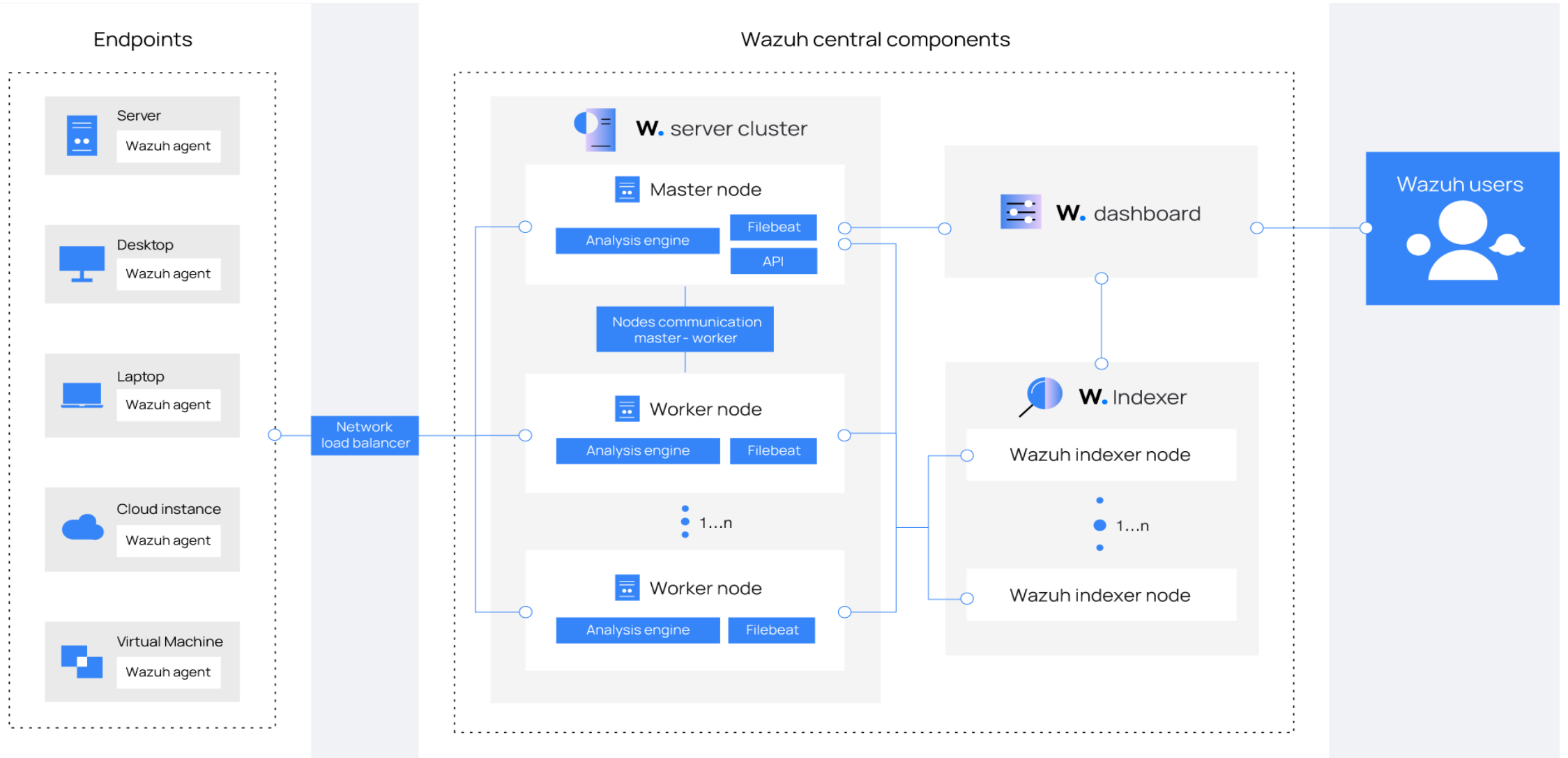


## Aktywne reagowanie na zagrożenia

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



Total agents  
417

Active agents  
371

Disconnected agents  
45

Pending agents  
0

Never connected agents  
1

## SECURITY INFORMATION MANAGEMENT



### Security events

Browse through your security alerts, identifying issues and threats in your environment.



### Integrity monitoring

Alerts related to file changes, including permissions, content, ownership and attributes.



### Amazon AWS

Security events related to your Amazon AWS services, collected directly via AWS API.



### Office 365

Security events related to your Office 365 services.



### Google Cloud Platform

Security events related to your Google Cloud Platform services, collected directly via GCP API.



### GitHub

Monitoring events from audit logs of your GitHub organizations.

## AUDITING AND POLICY MONITORING



### Policy monitoring

Verify that your systems are configured according to your security policies baseline.



### System auditing

Audit users behavior, monitoring command execution and alerting on access to critical files.



### OpenSCAP

Configuration assessment and automation of compliance monitoring using SCAP checks.



### CIS-CAT

Configuration assessment using Center of Internet Security scanner and SCAP checks.



### Security configuration assessment

Scan your assets as part of a configuration assessment audit.

## THREAT DETECTION AND RESPONSE



### Vulnerabilities

Discover what applications in your environment are affected by well-known vulnerabilities.



### VirusTotal

Alerts resulting from VirusTotal analysis of suspicious files via an integration with their API.



### Osquery

Osquery can be used to expose an operating system as a high-performance relational database.



### Docker listener

Monitor and collect the activity from Docker containers such as creation, running, starting, stopping or pausing events.



### MITRE ATT&CK

Security events from the knowledge base of adversary tactics and techniques based on real-world observations

## REGULATORY COMPLIANCE



### PCI DSS

Global security standard for entities that process, store or transmit payment cardholder data.



### NIST 800-53

National Institute of Standards and Technology Special Publication 800-53 (NIST 800-53) sets guidelines for federal information systems.



### TSC

Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy



### GDPR

General Data Protection Regulation (GDPR) sets guidelines for processing of personal data.



### HIPAA

Health Insurance Portability and Accountability Act of 1996 (HIPAA) provides data privacy and security provisions for safeguarding medical information.



Total agents - Active agents - Disconnected agents - Pending agents - Never connected agents -

SECURITY INFORMATION MANAGEMENT



Security events

Browse through your security alerts, identifying issues and threats in your environment.



Integrity monitoring

Alerts related to file changes, including permissions, content, ownership and attributes.

AUDITING AND POLICY MONITORING



Policy monitoring

Verify that your systems are configured according to your security policies baseline.



System auditing

Audit users behavior, monitoring command execution and alerting on access to critical files.



Security configuration assessment

Scan your assets as part of a configuration assessment audit.

THREAT DETECTION AND RESPONSE



Vulnerabilities

Discover what applications in your environment are affected by well-known vulnerabilities.



MITRE ATT&CK

Security events from the knowledge base of adversary tactics and techniques based on real-world observations

REGULATORY COMPLIANCE



PCI DSS

Global security standard for entities that process, store or transmit payment cardholder data.



NIST 800-53

National Institute of Standards and Technology Special Publication 800-53 (NIST 800-53) sets guidelines for federal information systems.



TSC

Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy



GDPR

General Data Protection Regulation (GDPR) sets guidelines for processing of personal data



HIPAA

Health Insurance Portability and Accountability Act of 1996 (HIPAA) provides data privacy and security provisions for safeguarding medical information.

https://192.168.21.186/app/wazuh



# Wazuh Agent & Agentless

# Agenci dostępni na różne platformy



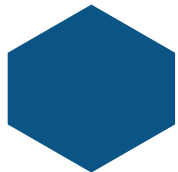
ORACLE  
Solaris



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 Agencji jak i Managerze.





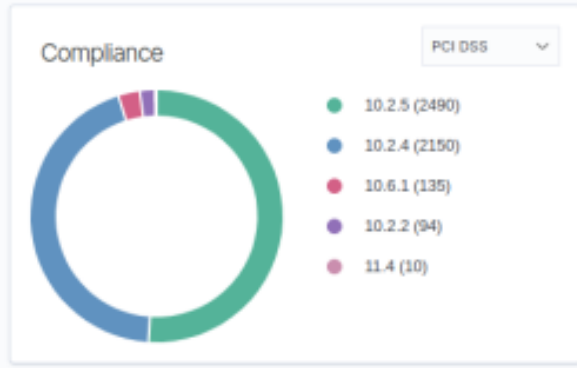
ID	Status	IP	Version	Groups	Operating system	Cluster node	Registration date	Last keep alive
001	● active	10.0.1.9	Wazuh v4.4.0	default <span>debian</span>	Debian GNU/Linux 11	worker_01	Jan 13, 2023 @ 19:27:21.000	Feb 2, 2023 @ 11:55:58.000

Last 24 hours ▼

### MITRE

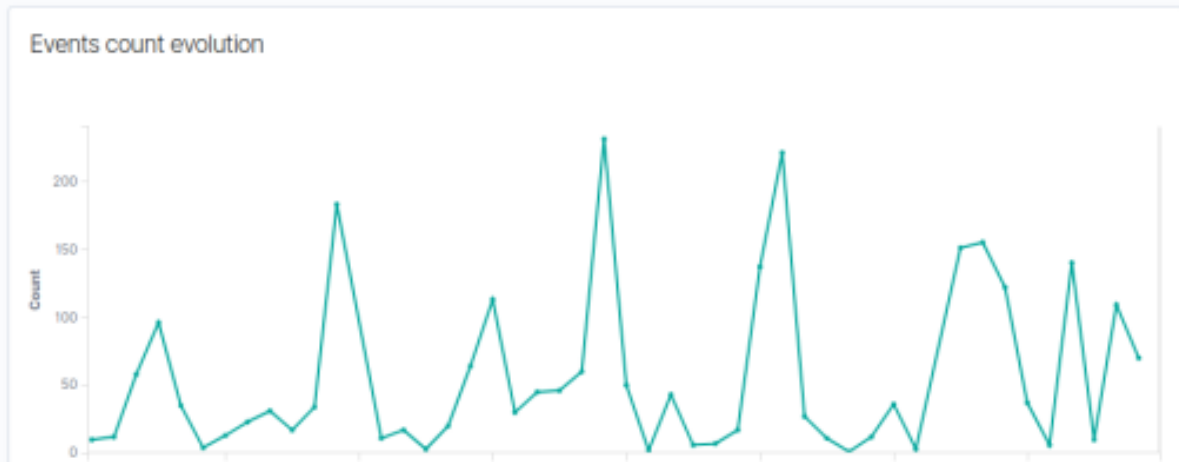
Top Tactics

- Credential Access **2151**
- Lateral Movement **1157**
- Defense Evasion **383**
- Privilege Escalation **363**
- Initial Access **269**



### FIM: Recent events

Time ↓	Path	Action	Rule description	Rule Level	Rule id
Feb 2, 2023 @ 05:22:40.194	<a href="#">/etc/resolv.conf</a>	modified	Integrity checksum changed.	7	550
Feb 1, 2023 @ 17:22:36.977	<a href="#">/etc/resolv.conf</a>	modified	Integrity checksum changed.	7	550



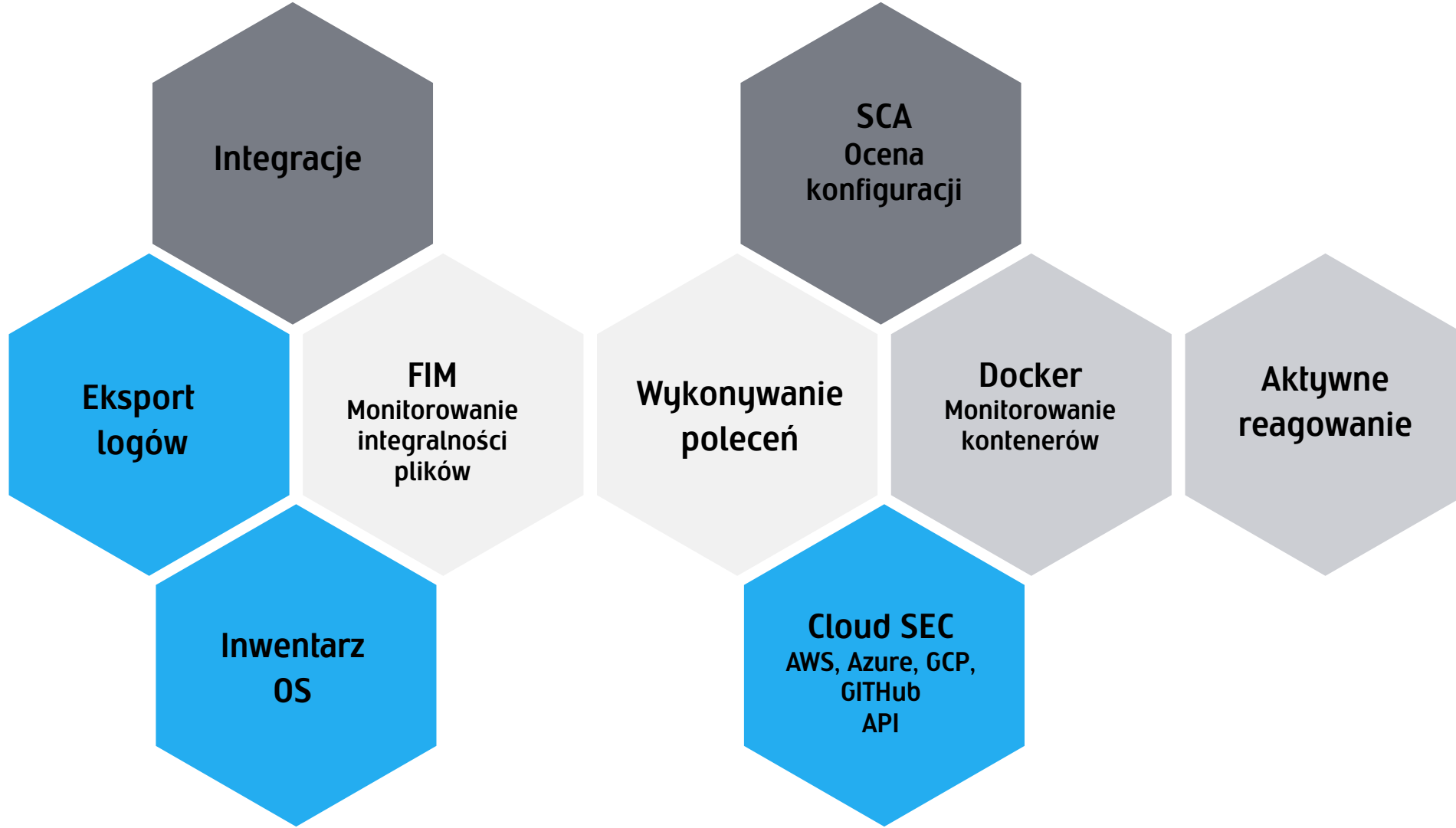
### SCA: Lastest scans

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	39%

< 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



The screenshot displays the Mikrotik WinBox interface for configuring syslog monitoring. The left sidebar shows the navigation menu with 'Logging' selected. The main area is divided into two panels: 'Log Rule <system>' and 'Log Action <remote>'.

**Log Rule <system> Configuration:**

- Enabled:
- Topics: system
- Prefix: (empty)
- Action: remote

**Log Action <remote> Configuration:**

Name	remote
Type	remote
Remote Address	192.168.56.170
Remote Port	514
Src. Address	(dropdown)
BSD Syslog	<input checked="" type="checkbox"/>
Syslog Facility	daemon
Syslog Severity	emergency

# Monitoring syslog – Mikrotik



wazuh. Modules Ubuntu-latest Security events @ Index pattern wazuh-alerts-\* a

Jan 10, 2024 @ 14:11:05.625 MikroTik router rebooted 5 110002

Table JSON Rule

@timestamp	2024-01-10T13:11:05.625Z
_id	7uB_B4wBMMjWslaQkKfx
agent.id	003
agent.ip	192.168.56.170
agent.name	Ubuntu-latest
data.action	rebooted
data.logtimestamp	Jan 10 13:11:04
decoder.name	mikrotik
full_log	RouterOS7.1-logs: Jan 10 13:11:04 MikroTik router rebooted
id	1704892265.101768
input.type	log
location	/var/log/mikrotik.log
manager.name	centos
rule.description	MikroTik router rebooted
rule.firetimes	1
rule.groups	Mikrotik
rule.id	110002
rule.level	5

wazuh. Modules Ubuntu-latest Security events @ Index pattern wazuh-alerts-\* a

Top 5 alerts

Top 5 rule groups

Top 5 PCI DSS Requirements

Security Alerts

Time ↓	Technique(s)	Tactic(s)	Description	Level	Rule ID
> Jan 10, 2024 @ 14:11:05.625			MikroTik router rebooted	5	110002
> 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



# 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).</description>
  </rule>
</group>
  
```

wazuh. Modules Abdullahs-Mac.I... Security events

Top 5 alerts

Top 5 rule groups

Top 5 PCI DSS Requirements

wazuh. Modules Abdullahs-Mac.I... Security events

Jan 10, 2024 @ 14:05:02.264 macOS: Unauthorized USB drive RTL8152 Fast Ethernet Adapter was connected.

Table	JSON	Rule
@timestamp	2024-01-10T08:05:02.264Z	
_id	RCxn8owBrjf1OAKpSAKg	
agent.id	001	
agent.ip	172.28.8.192	
agent.name	Abdullahs-Mac.local	
data.aws.accountId		
data.aws.region		
data.deviceInfo.idProduct	8152	
data.deviceInfo.idVendor	0bda	
data.deviceInfo.kUSBSerialNumberString	00E04C365880	
data.deviceInfo.productName	RTL8152 Fast Ethernet Adapter	
data.deviceInfo.vendorName	Realtek Semiconductor Corp.	
data.eventType	USBConnected	
data.timestamp	2024-01-10T00:05:00.211-08:00	
decoder.name	json	
full_log	{"timestamp":"2024-01-10T00:05:00.211-08:00","deviceInfo":{"kUSBSerialNumberString":"00E04C365880","pr Corp.,"idProduct":"8152","idVendor":"0bda"},"eventType":"USBConnected"}	
id	1704873902.31510	

Security Alerts

Time ↓	Description	Level	Rule ID
Jan 10, 2024 @ 14:07:08.066	macOS: Unauthorized USB drive RTL8152 Fast Ethernet Adapter was disconnected.	8	111063
Jan 10, 2024 @ 14:06:51.783	Successful sudo to ROOT executed.	3	5402
Jan 10, 2024 @ 14:06:41.753	sshd: authentication success.	3	5715
Jan 10, 2024 @ 14:05:02.264	macOS: Unauthorized USB drive RTL8152 Fast Ethernet Adapter was connected.	8	111061
Jan 10, 2024 @ 14:03:59.388	Screen unlocked with userID:501.	3	89602

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-IEFP03BFT0D	ADATA USB Flash Drive USB Device	1

14

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

Export: Raw Formatted

# Monitorowanie zmian konfiguracji FIM



wazuh. Modules ubuntu\_server Integrity monitoring

Inventory Dashboard Events (9) ubuntu\_server (003)

Search DQL Last 24 hours Show dates Refresh

manager.name: ubuntu rule.groups: syscheck agent.id: 003 + Add filter

14 hits

Aug 7, 2023 @ 10:09:35.158 - Aug 8, 2023 @ 10:09:35.158 Auto

Time	syscheck.path	syscheck.event	rule.description	rule.level	rule.id	
>	Aug 8, 2023 @ 10:09:07.129	/etc/app.conf	modified	Integrity checksum changed.	7	550

```
<!-- 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



wazuh. Modules ArchLinux Vulnerabilities

Inventory Events ArchLinux (004)

**SEVERITY**

- Critical (2)
- High (8)
- Medium (3)
- Low (0)

**DETAILS**

Critical: 2 High: 8 Medium: 3 Low: 0

Last full scan: Apr 2, 2024 @ 15:53:31.000  
Last partial scan: Apr 2, 2024 @ 17:32:48.000

**SUMMARY**

- grub (8)
- perl (2)
- openssl (1)
- wget (1)

Vulnerabilities (1)

cve=CVE-2024-3094

Name	Version	Architecture	Severity
xz	5.6.0-1	x86_64	Critical

Rows per page: 10

**CVE-2024-3094**

Details

- Title: CVE-2024-3094 affects xz
- Version: 5.6.0-1
- Architecture: x86\_64
- Condition: Package less than 5.6.1-2
- Published: -
- References: View external references

Recent events (1 hits)

Time	Description	Level	Rule ID	Status
Apr 2, 2024 @ 16:14:02.196	CVE-2024-3094 affects xz	13	23506	Active

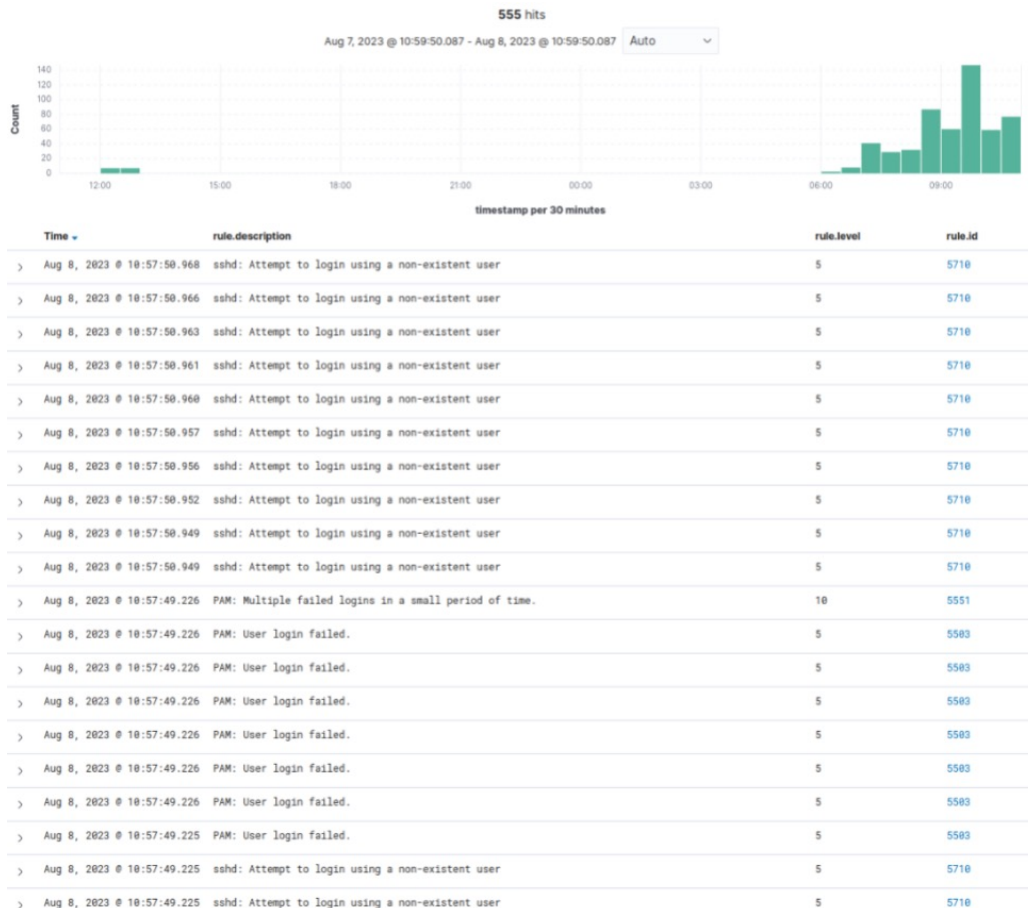
Rows per page: 10

```
<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>
```

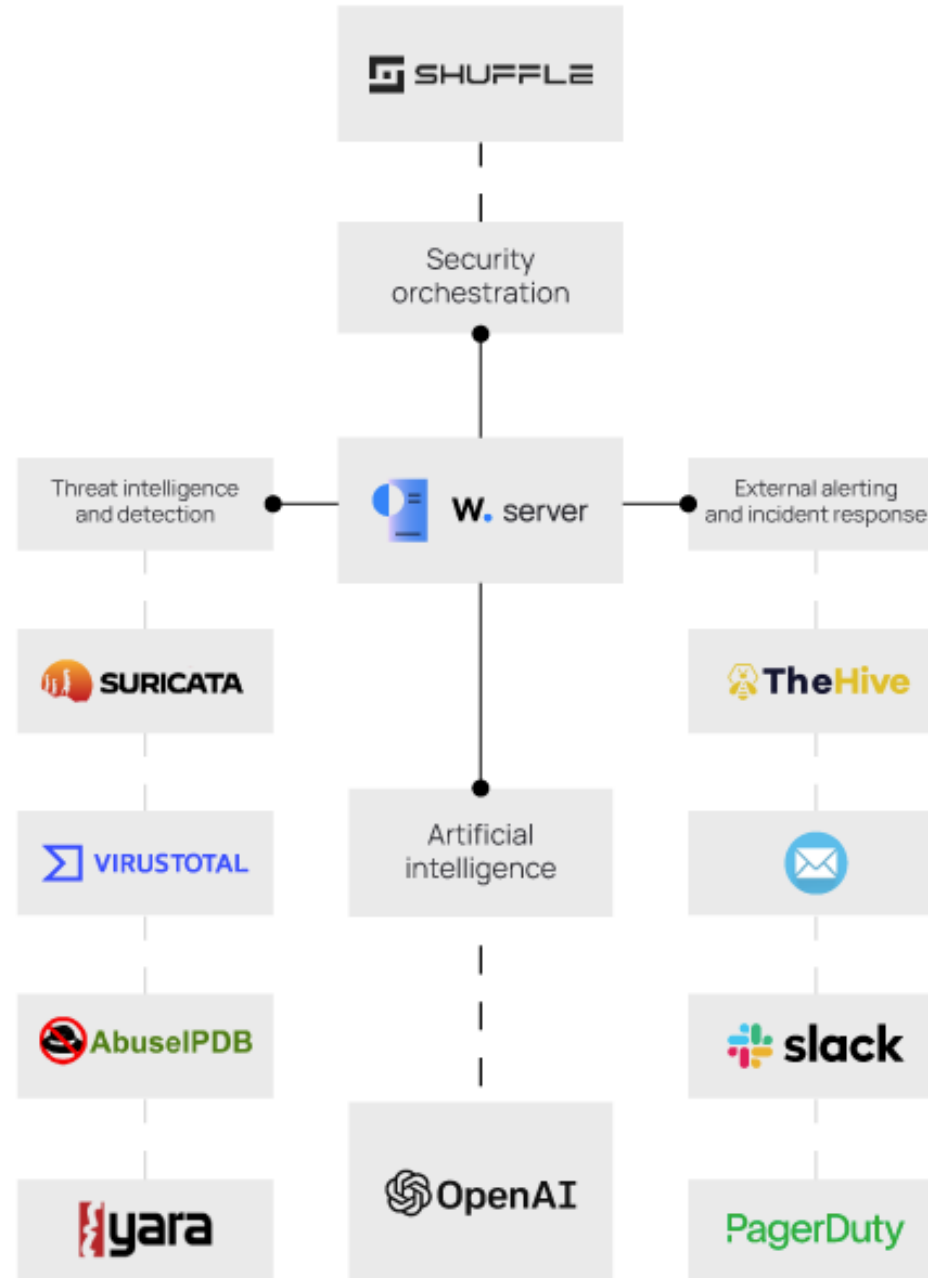
```
<ossec_config>  
  <active-response>  
    <command>firewall-drop</command>  
    <location>local</location>  
    <rules_id>5763</rules_id>  
    <timeout>180</timeout>  
  </active-response>  
</ossec_config>
```

wazuh. Modules ubuntu\_server Security events

> Aug 8, 2023 @ 11:34:11.881	Host Blocked by firewall-drop Active Response	3	651
> Aug 8, 2023 @ 11:34:11.861	Host Blocked by firewall-drop Active Response	3	651
> Aug 8, 2023 @ 11:34:11.845	Host Blocked by firewall-drop Active Response	3	651
> Aug 8, 2023 @ 11:34:11.830	Host Blocked by firewall-drop Active Response	3	651
> Aug 8, 2023 @ 11:34:11.814	Host Blocked by firewall-drop Active Response	3	651
> Aug 8, 2023 @ 11:34:11.783	Host Blocked by firewall-drop Active Response	3	651
> Aug 8, 2023 @ 11:34:11.775	Host Blocked by firewall-drop Active Response	3	651
> Aug 8, 2023 @ 11:34:11.756	Host Blocked by firewall-drop Active Response	3	651
> Aug 8, 2023 @ 11:34:09.872	sshd: Attempt to login using a non-existent user	5	5710
> Aug 8, 2023 @ 11:34:09.844	sshd: Attempt to login using a non-existent user	5	5710
> Aug 8, 2023 @ 11:34:09.844	sshd: Attempt to login using a non-existent user	5	5710
> Aug 8, 2023 @ 11:34:09.844	sshd: Attempt to login using a non-existent user	5	5710
> Aug 8, 2023 @ 11:34:09.844	sshd: Attempt to login using a non-existent user	5	5710
> Aug 8, 2023 @ 11:34:09.844	sshd: Attempt to login using a non-existent user	5	5710
> Aug 8, 2023 @ 11:34:09.844	sshd: Attempt to login using a non-existent user	5	5710
> Aug 8, 2023 @ 11:34:09.844	sshd: Attempt to login using a non-existent user	5	5710
> Aug 8, 2023 @ 11:34:09.844	sshd: Attempt to login using a non-existent user	5	5710
> Aug 8, 2023 @ 11:34:09.844	sshd: Attempt to login using a non-existent user	5	5710



# Integracje





# Podsumowanie Wazuh i obserwacje

- OpenSource + Społeczność (Google Groups, Slack, Discord, Github)
- Edycja reguł/ dekoderek/ 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](mailto:a.pielak@beyond.pl)

[www.beyond.pl](http://www.beyond.pl)

