Projekt – Open Source Security Platform wazuh.

Spis treści

1. Infrastruktura sieci

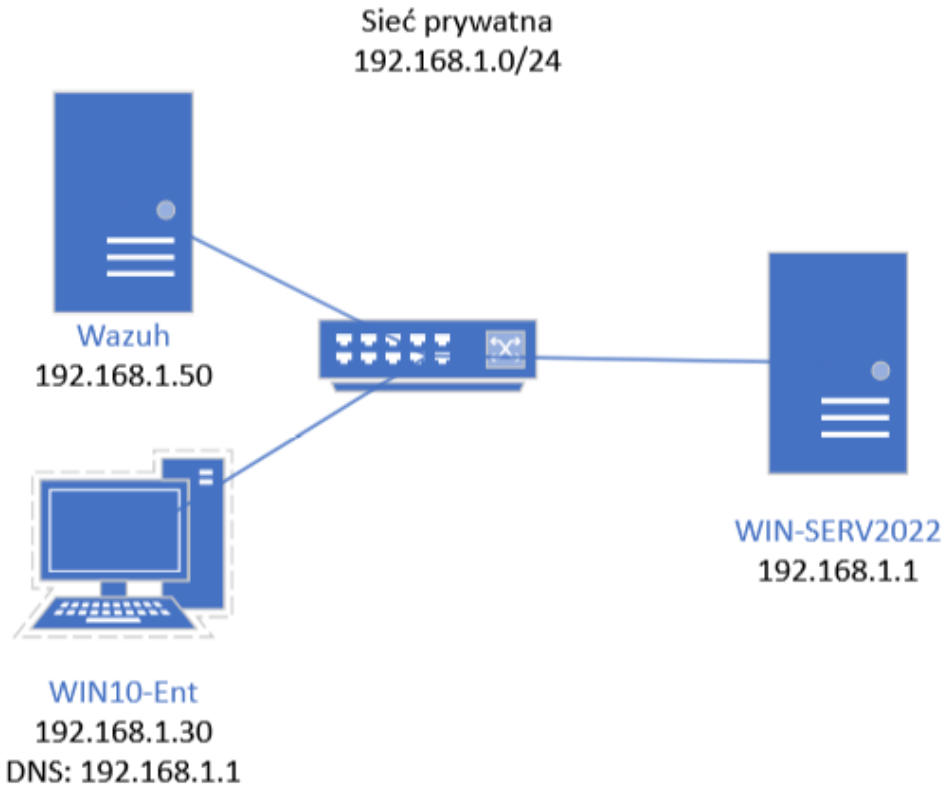
Środowisko sieciowe powinno oparte o 3 maszyny wirtualne w środowisku HyperV z systemami operacyjnymi:

- Debian 12 – pełniący rolę serwera Wazuh,
- Windows Server 2022 – pełniący rolę Active Directory, połączony z internetem,
- Windows 10 Enterprise - pełniący rolę stacji klienckiej połączonej z domeną.

1.1. Adresacja maszyn wirtualnych

l.p	Nazwa hosta	System Operacyjny	Adres IP	Domena	Nazwa agenta Wazuh
1	WIN-SERV2022	Windows Server 2022	192.168.1.1/24 192.168.4.80/24	xxx.internal	WS2022-agent
2	WIN10-Ent	Windows 10 Enterprise	192.168.1.30/24	xxx.internal	Win10E-agent
3	Wazuh	Debian 12 (Bookworm)	192.168.1.50/24	localdomain	Wazuh

1.1.1. Schemat infrastruktury sieciowej



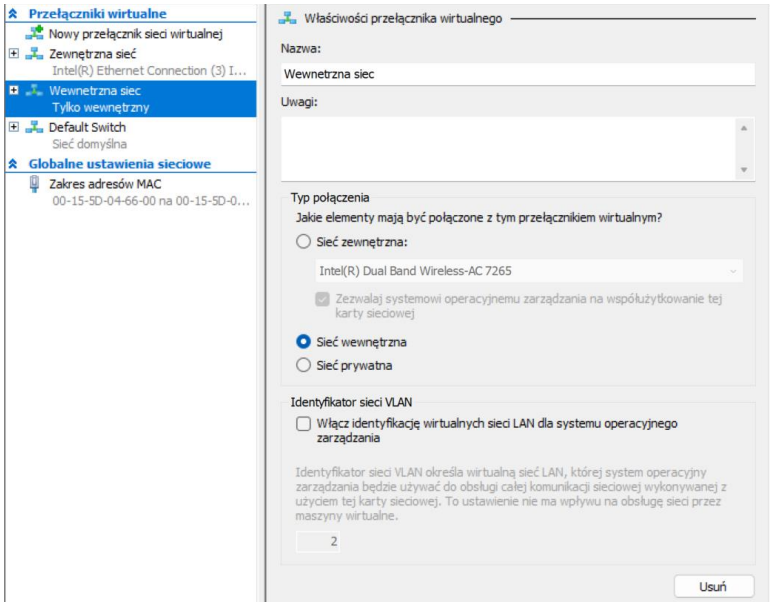
1.2. Konfiguracja maszyn wirtualnych – HyperV

- Debian 12 – CPU - 2 rdzenie, RAM – 4 GB statycznie
- Windows Server 2022 – CPU - 2 rdzenie, RAM – 4 GB dynamicznie przydzielane
- Windows 10 Enterprise - CPU - 2 rdzenie, RAM – 4 GB dynamicznie przydzielane

1.2.1. Przełączniki wirtualne – vSwitch

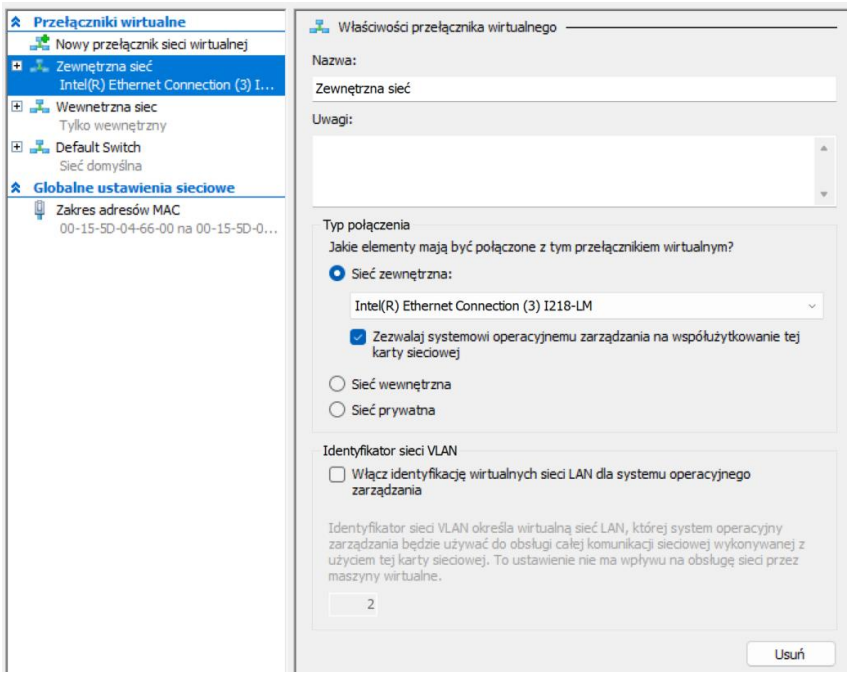
- Sieć wewnętrzna:

  - Debian 12
  - Windows 10 Enterprise
  - Windows Server 2022



- Sieć zewnętrzna:

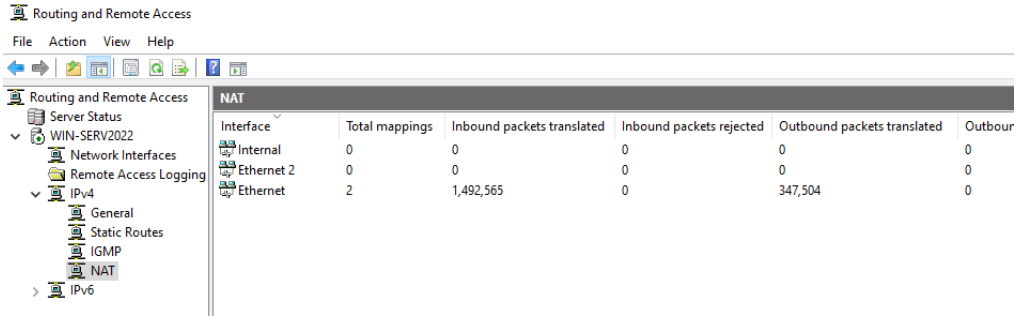
  - Windows Server 2022
  - Zmostkowana karta sieciowa LAN



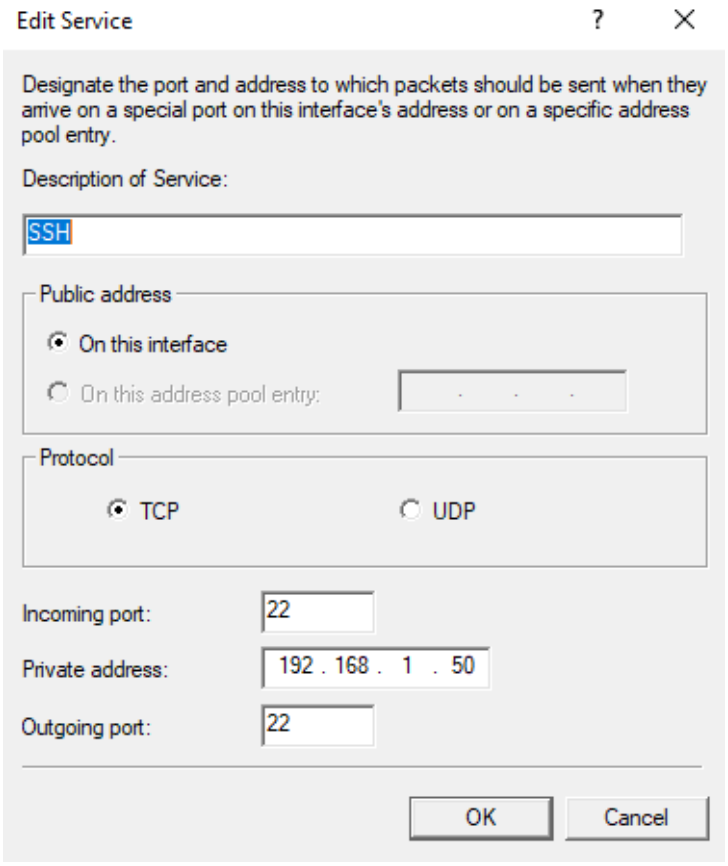
1.2.2. Konfiguracja ustawień Windows Server 2022

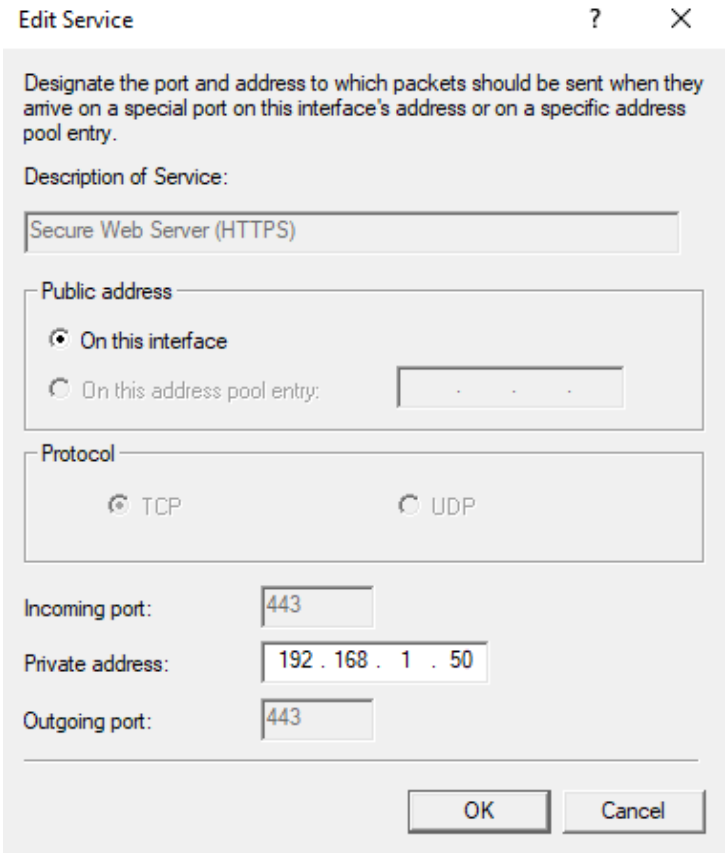
1.2.2.1 NAT

Serwer posiada skonfigurowany NAT na porcie Ethernet, aby sieć wewnętrzna mogła się łączyć z siecią zewnętrzną i internetem.



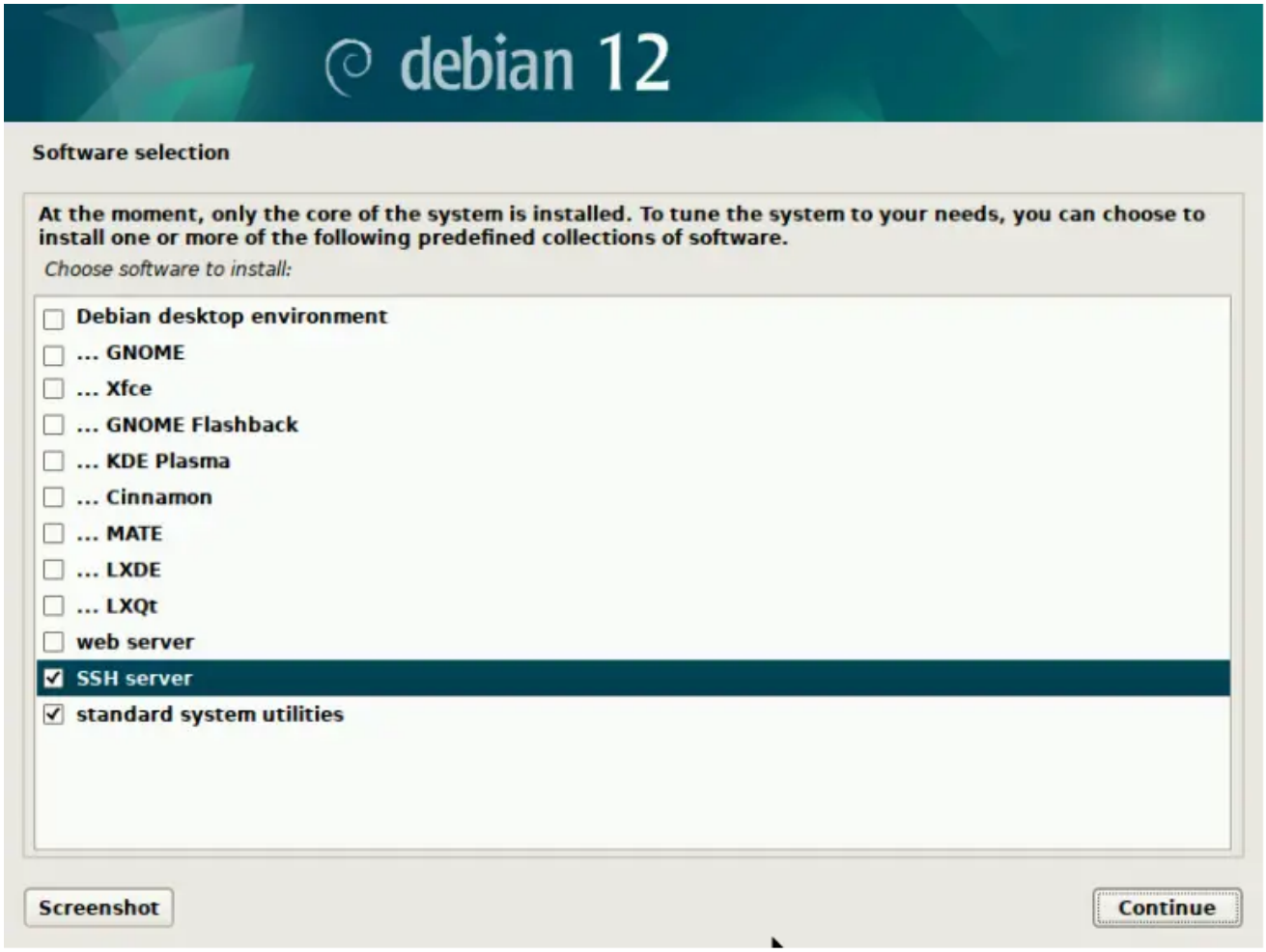
Powinien posiadać również dwa przekierowania kierujące do Wazuha





1.3. Przygotowanie systemu Debian 12 pod instalację Wazuh

Podczas instalacji Debiana należy zaistalować serwer SSH w celu zdalnego łączenia się z serwerem.



Należy się zalogować do systemu jako root wykorzystując polecenie *su-* i wprowadzić wcześniej ustalone hasło.

```
user-wazuh@Wazuh:~$ su -
Password:
root@Wazuh:~#
```

1.3.1. Konfiguracja interfejsu sieciowego

Konfigurujemy interfejsy karty sieciowej na adres statyczny za pomocą polecenia

nano /etc/network/interfaces

```
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
allow-hotplug eth0
iface eth0 inet static
        address 192.168.1.50
        netmask 255.255.255.0
        gateway 192.168.1.1
        dns-nameservers 192.168.1.1 192.168.4.1
```

Następnie zrestatruj usługę sieciową

Systemctl restart networking.service

1.3.2. Łączenie zdalne z Debianem

Możesz połączyć się zdalnie za pomocą SSH korzystając z polecenia

ssh 192.168.4.80 -l user-wazuh

```
C:\Users\Wojti>ssh 192.168.4.80 -l user-wazuh
The authenticity of host '192.168.4.80 (192.168.4.80)' can't be established.
ED25519 key fingerprint is SHA256:MPytJfN7e7Q3mbZXh0qvaZFP66SSydjwuDBcpRAkfgs.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.4.80' (ED25519) to the list of known hosts.
user-wazuh@192.168.4.80's password:
Linux Wazuh 6.1.0-10-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.38-2 (2023-07-27) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Fri Aug  4 08:34:49 2023
```

Zaktualizuj pakiety oraz zainstaluj **curl**

```
root@Wazuh:~# apt upgrade
```

```
root@Wazuh:~# apt update
```

```
root@Wazuh:~# apt-get install curl
```

2. Instalacja Wazuh w wersji 4.4

2.1. Przygotowanie plików

Ze strony wazuh.com pobieramy wymagane pliki do instalacji Wazuh

curl -sO https://packages.wazuh.com/4.4/wazuh-install.sh

curl -sO https://packages.wazuh.com/4.4/config.yml

```
root@Wazuh:~# curl -sO https://packages.wazuh.com/4.4/wazuh-install.sh
root@Wazuh:~# curl -sO https://packages.wazuh.com/4.4/config.yml
root@Wazuh:~# ls
config.yml  wazuh-install.sh
```

Edytujemy plik config.yml wprowadzając nasz adres ip dla każdego z modułu Wazuh

```
root@Wazuh:~# nano config.yml
```

```
nodes:
  # Wazuh indexer nodes
  indexer:
    - name: node-1
      ip: 192.168.1.50
```

```
server:
  - name: wazuh-1
    ip: 192.168.1.50
```

```
dashboard:
  - name: dashboard
    ip: 192.168.1.50
```

2.2. Generowanie certyfikatów

bash wazuh-install.sh --generate-config-files -i

```
root@Wazuh:~# bash wazuh-install.sh --generate-config-files -i
04/08/2023 10:12:12 INFO: Starting Wazuh installation assistant. Wazuh version: 4.4.5
04/08/2023 10:12:12 INFO: Verbose logging redirected to /var/log/wazuh-install.log
04/08/2023 10:12:18 INFO: --- Dependencies ----
04/08/2023 10:12:18 INFO: Installing gawk.
04/08/2023 10:12:21 WARNING: Hardware and system checks ignored.
04/08/2023 10:12:21 INFO: --- Configuration files ---
04/08/2023 10:12:21 INFO: Generating configuration files.
04/08/2023 10:12:23 INFO: Created wazuh-install-files.tar. It contains the Wazuh cluster key, certificates, and password
s necessary for installation.
root@Wazuh:~#
```

(należy skorzystać z argumentu –i, gdyż Debian 12 nie jest rekomendowanym systemem i instalator nie przepuści nas dalej bez jego wykorzystania)

2.3. Instalacja modułu - Wazuh Indexer

Gdy posiadamy już certyfikaty, należy zainstalować pierwszy moduł o nazwie Wazuh Indexer

bash wazuh-install.sh --wazuh-indexer node-1 –i

```
root@Wazuh:~# bash wazuh-install.sh --wazuh-indexer node-1 -i
04/08/2023 10:16:31 INFO: Starting Wazuh installation assistant. Wazuh version: 4.4.5
04/08/2023 10:16:31 INFO: Verbose logging redirected to /var/log/wazuh-install.log
04/08/2023 10:16:37 WARNING: Hardware and system checks ignored.
04/08/2023 10:16:40 INFO: --- Dependencies ----
04/08/2023 10:16:40 INFO: Installing apt-transport-https.
04/08/2023 10:16:42 INFO: Installing software-properties-common.
04/08/2023 10:17:10 INFO: Installing gnupg.
04/08/2023 10:17:20 INFO: Wazuh repository added.
04/08/2023 10:17:20 INFO: --- Wazuh indexer ---
04/08/2023 10:17:20 INFO: Starting Wazuh indexer installation.
04/08/2023 10:19:00 INFO: Wazuh indexer installation finished.
04/08/2023 10:19:00 INFO: Wazuh indexer post-install configuration finished.
04/08/2023 10:19:00 INFO: Starting service wazuh-indexer.
04/08/2023 10:19:29 INFO: wazuh-indexer service started.
04/08/2023 10:19:29 INFO: Initializing Wazuh indexer cluster security settings.
04/08/2023 10:19:31 INFO: Wazuh indexer cluster initialized.
04/08/2023 10:19:31 INFO: Installation finished.
root@Wazuh:~#
```

2.3.1. Inicjacja i uruchamianie klastra

Po wykonaniu instalacji Indexera należy zainicjalizować klaster

bash wazuh-install.sh --start-cluster –i

```
root@Wazuh:~# bash wazuh-install.sh --start-cluster -i
04/08/2023 10:23:22 INFO: Starting Wazuh installation assistant. Wazuh version: 4.4.5
04/08/2023 10:23:22 INFO: Verbose logging redirected to /var/log/wazuh-install.log
04/08/2023 10:23:29 WARNING: Hardware and system checks ignored.
04/08/2023 10:23:37 INFO: Wazuh indexer cluster security configuration initialized.
04/08/2023 10:24:05 INFO: Wazuh indexer cluster started.
root@Wazuh:~#
```

2.3.2. Wyodrębnianie hasła

Po uruchomieniu klastra, należy wyodrębnić z archiwum wazuh-install-files.tar hasło z pliku wazuh-passwords.txt dla admina

tar -axf wazuh-install-files.tar wazuh-install-files/wazuh-passwords.txt -O | grep -P "\'admin\'" -A 1

```
root@Wazuh:~# tar -axf wazuh-install-files.tar wazuh-install-files/wazuh-passwords.txt -O | grep -P "\'admin\'" -A 1
  indexer_username: 'admin'
  indexer_password: 'GHE+PePk?66+LKPN9YLToSWfhEXRhv4g'
```

2.3.3. Weryfikacja instalacji Wazuh Indexer

Po wyodrębnieniu hasła weryfikujemy poprawność instalacji Indexera

curl -k -u admin:<ADMIN_PASSWORD> https://<WAZUH_INDEXER_IP>:9200

W miejscu <ADMIN_PASSWORD> wprowadzamy wyodrębnione hasło, a w <WAZUH_INDEXER_IP> wprowadzamy adres Indexera

```
root@Wazuh:~# curl -k -u admin:GHE+PePk?66+LKPN9YLToSWfhEXRhv4g https://192.168.1.50:9200
{
  "name" : "node-1",
  "cluster_name" : "wazuh-indexer-cluster",
  "cluster_uuid" : "iPcG0gRyS12y_xNEBU2K3A",
  "version" : {
    "number" : "7.10.2",
    "build_type" : "rpm",
    "build_hash" : "7203a5af21a8a009aece1474446b437a3c674db6",
    "build_date" : "2023-02-24T18:57:04.388618985Z",
    "build_snapshot" : false,
    "lucene_version" : "9.5.0",
    "minimum_wire_compatibility_version" : "7.10.0",
    "minimum_index_compatibility_version" : "7.0.0"
  },
  "tagline" : "The OpenSearch Project: https://opensearch.org/"
}
root@Wazuh:~#
```

1.1. Instalacja serwera Wazuh

bash wazuh-install.sh --wazuh-server wazuh-1 –i

```
root@Wazuh:~# bash wazuh-install.sh --wazuh-server wazuh-1 -i
04/08/2023 10:33:55 INFO: Starting Wazuh installation assistant. Wazuh version: 4.4.5
04/08/2023 10:33:55 INFO: Verbose logging redirected to /var/log/wazuh-install.log
04/08/2023 10:34:02 WARNING: Hardware and system checks ignored.
04/08/2023 10:34:05 INFO: Wazuh repository added.
04/08/2023 10:34:06 INFO: --- Wazuh server ---
04/08/2023 10:34:06 INFO: Starting the Wazuh manager installation.
04/08/2023 10:35:31 INFO: Wazuh manager installation finished.
04/08/2023 10:35:31 INFO: Starting service wazuh-manager.
04/08/2023 10:35:57 INFO: wazuh-manager service started.
04/08/2023 10:35:57 INFO: Starting Filebeat installation.
04/08/2023 10:36:06 INFO: Filebeat installation finished.
04/08/2023 10:36:07 INFO: Filebeat post-install configuration finished.
04/08/2023 10:36:14 INFO: Starting service filebeat.
04/08/2023 10:36:17 INFO: filebeat service started.
04/08/2023 10:36:17 INFO: Installation finished.
root@Wazuh:~#
```

2.4. Instalacja panelu Wazuh

Ostatnim modułem które zainstalujemy jest Wazuh dashboard

bash wazuh-install.sh --wazuh-dashboard dashboard –i

```
root@Wazuh:~# bash wazuh-install.sh --wazuh-dashboard dashboard -i
04/08/2023 10:38:17 INFO: Starting Wazuh installation assistant. Wazuh version: 4.4.5
04/08/2023 10:38:17 INFO: Verbose logging redirected to /var/log/wazuh-install.log
04/08/2023 10:38:25 WARNING: Hardware and system checks ignored.
04/08/2023 10:38:28 INFO: Wazuh repository added.
dashboard
04/08/2023 10:38:28 INFO: --- Wazuh dashboard ----
04/08/2023 10:38:28 INFO: Starting Wazuh dashboard installation.
04/08/2023 10:39:55 INFO: Wazuh dashboard installation finished.
04/08/2023 10:39:55 INFO: Wazuh dashboard post-install configuration finished.
04/08/2023 10:39:55 INFO: Starting service wazuh-dashboard.
04/08/2023 10:39:56 INFO: wazuh-dashboard service started.
04/08/2023 10:40:21 INFO: Initializing Wazuh dashboard web application.
04/08/2023 10:40:22 INFO: Wazuh dashboard web application initialized.
04/08/2023 10:40:22 INFO: --- Summary ---
04/08/2023 10:40:22 INFO: You can access the web interface https://192.168.1.50
    User: admin
    Password: GHE+PePk?66+LKPN9YLToSWfhEXRhv4g
04/08/2023 10:40:22 INFO: Installation finished.
root@Wazuh:~#
```

Jesteśmy gotowi do przejścia na stronę panelu głównego Wazuh.

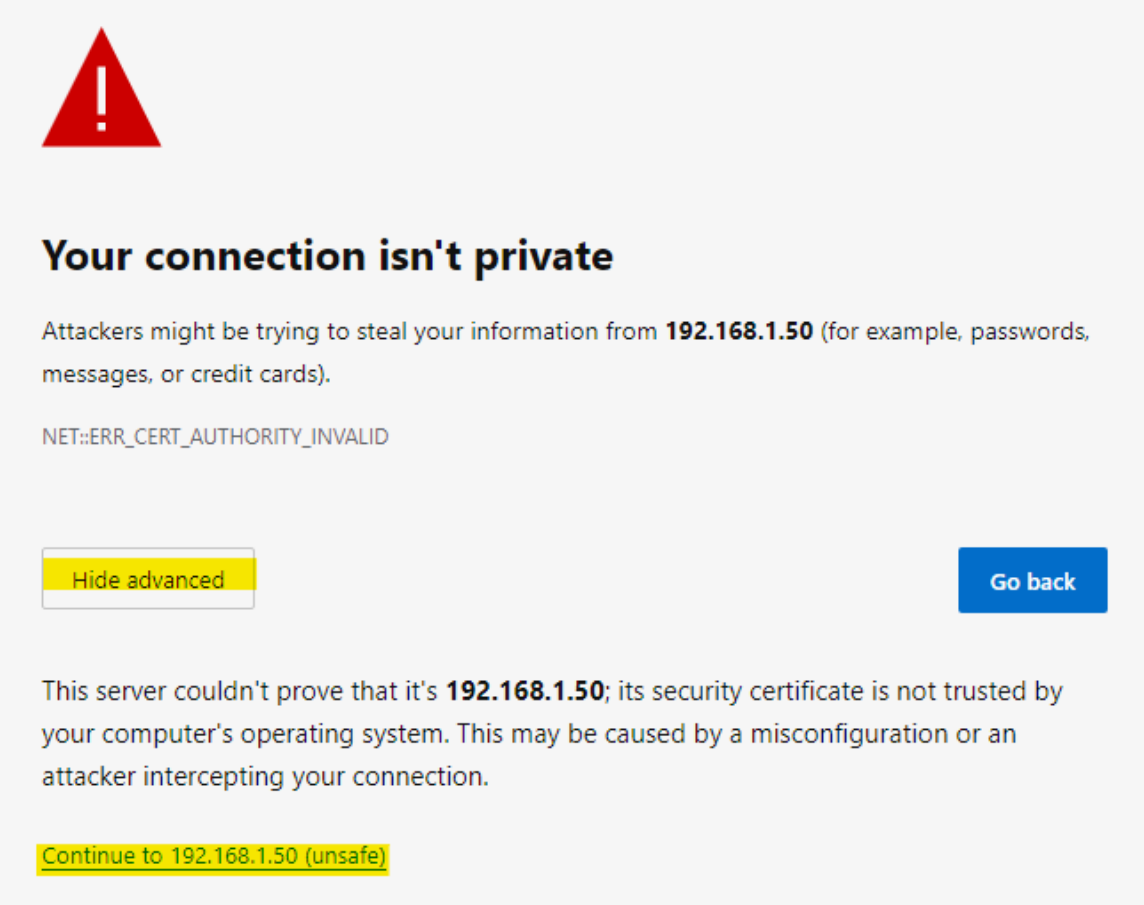
3. Wazuh Dashboard

Aby połączyć się z głównym panelem Wazuh należy połączyć się z wcześniej zdefiniowanym adresem wpisując w okno przeglądarki adres:

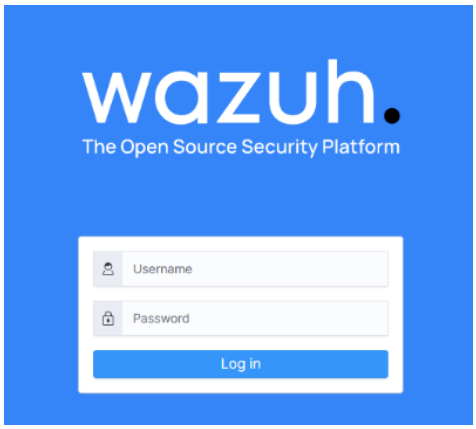
https://192.168.1.50

3.1. Pierwsze logowanie

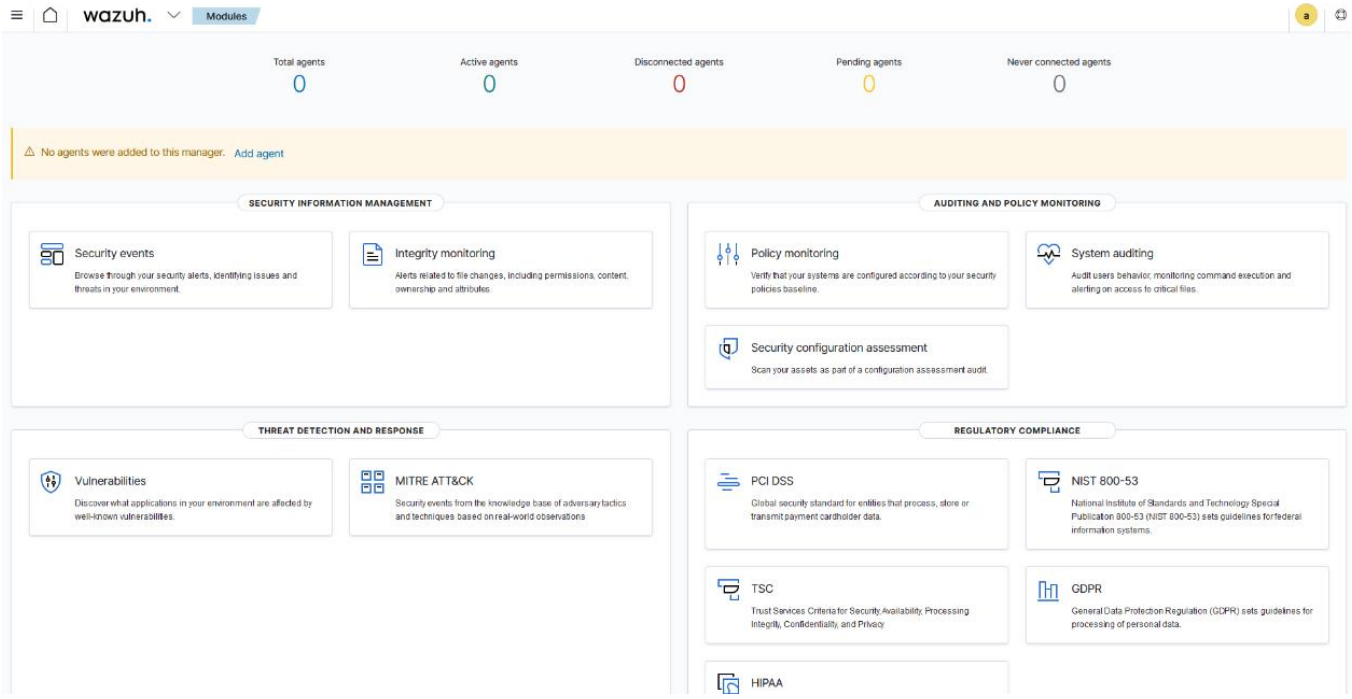
Podczas pierwszej próby połączenia się z panelem głównym pojawi się monit o nieautoryzowanym certyfikacie, należy się nie przejmować tym komunikatem i przejść dalej.



Następnie przywita nas strona logowania.

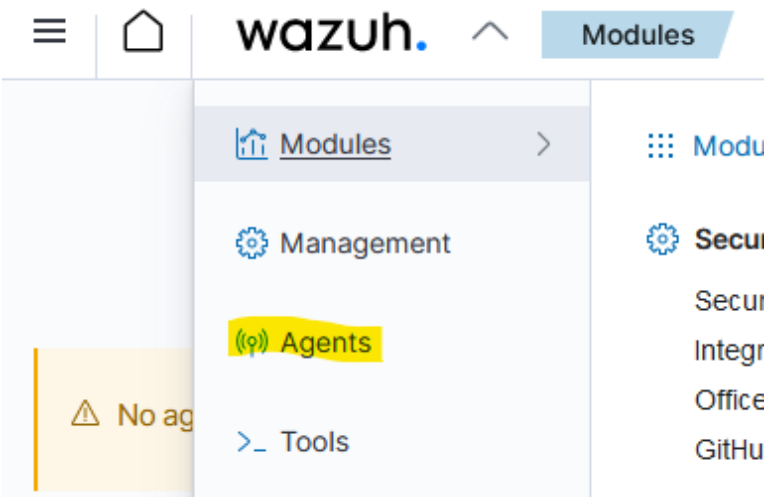


Tak powinna wyglądać strona po pierwszym zalogowaniu



3.2. Dodawanie agentów

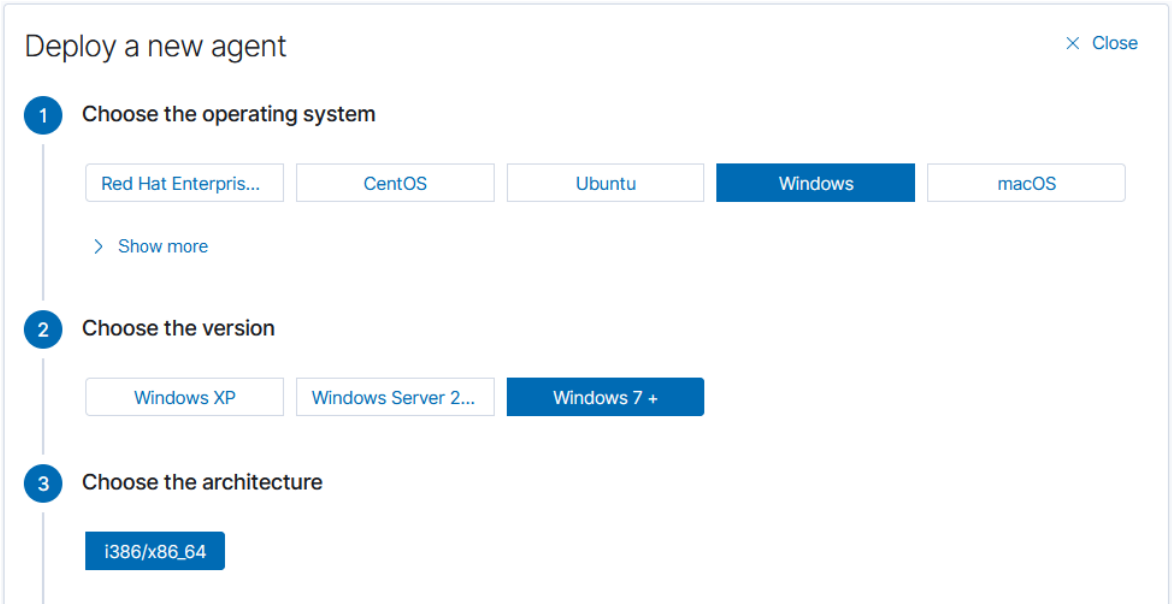
Z rozwijanego menu obok loga Wazuh wybieramy zakładkę Agents.



3.2.1. Określanie systemu docelowego

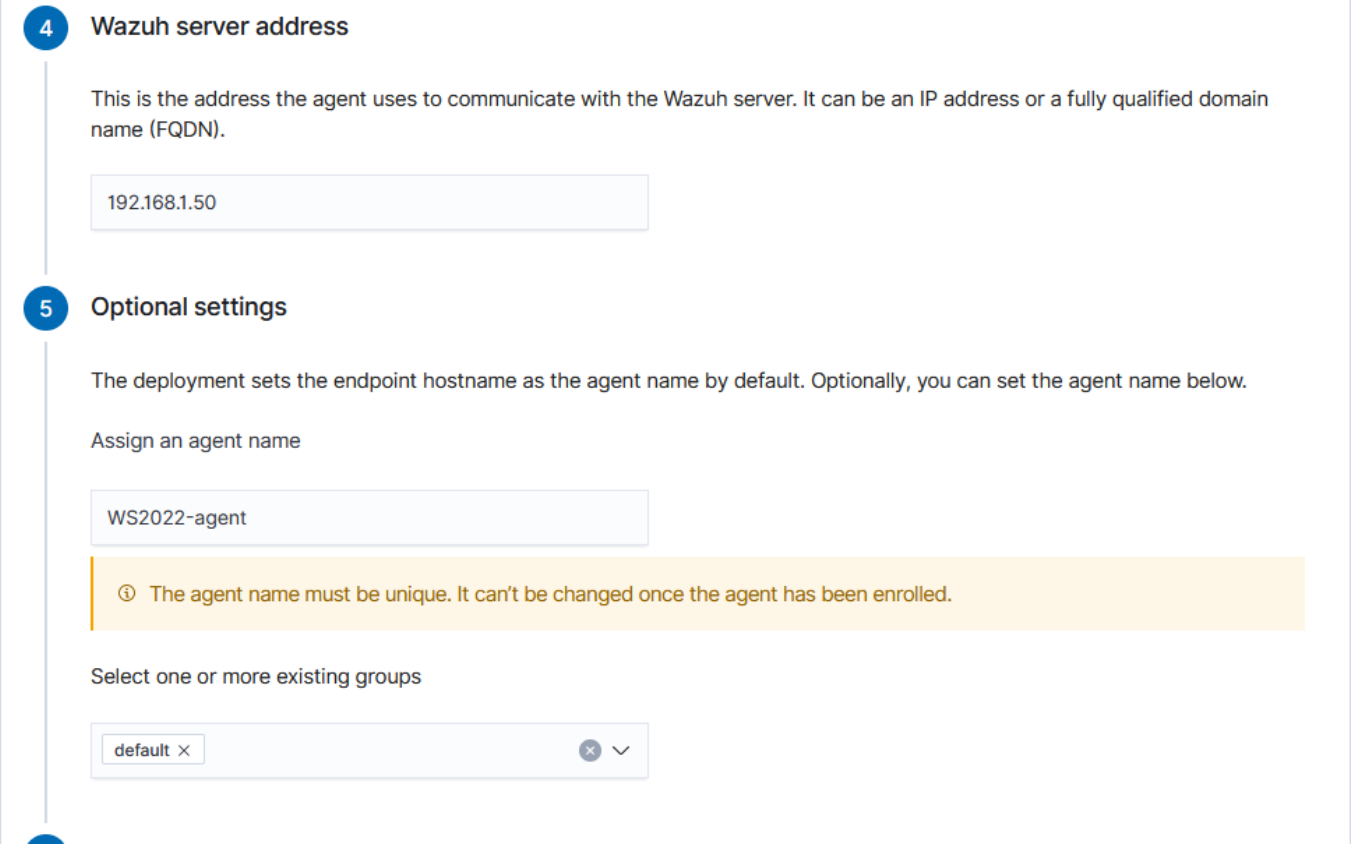
Wypełniamy formularz wybierając system operacyjny.

Dla systemów nowszych niż Windows 7, będzie tak jak poniżej.



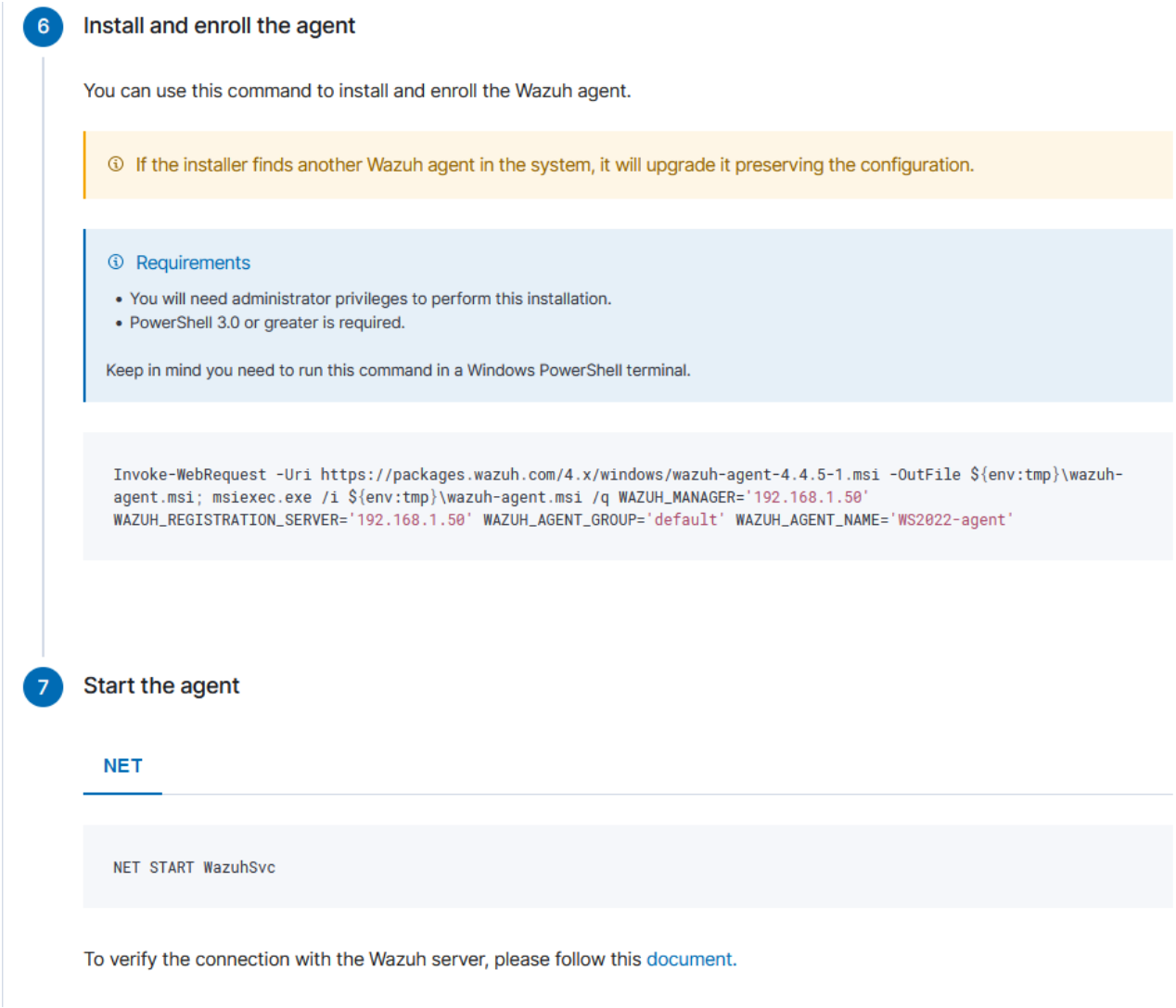
3.2.2. Określanie docelowego serwera Wazuh

Wprowadzamy adres serwera Wazuh oraz wpisujemy unikalną nazwę dla wdrażanego agenta i dodajemy do grupy default.



3.2.3. Instalacja agentów Wazuh

Ostatnim etapem jest skopiowanie wskazanych poleceń w programie Powershell na maszynie docelowej.



Na Serwerze Windows 2022 uruchamiamy aplikację PowerShell i wklejamy polecenia.

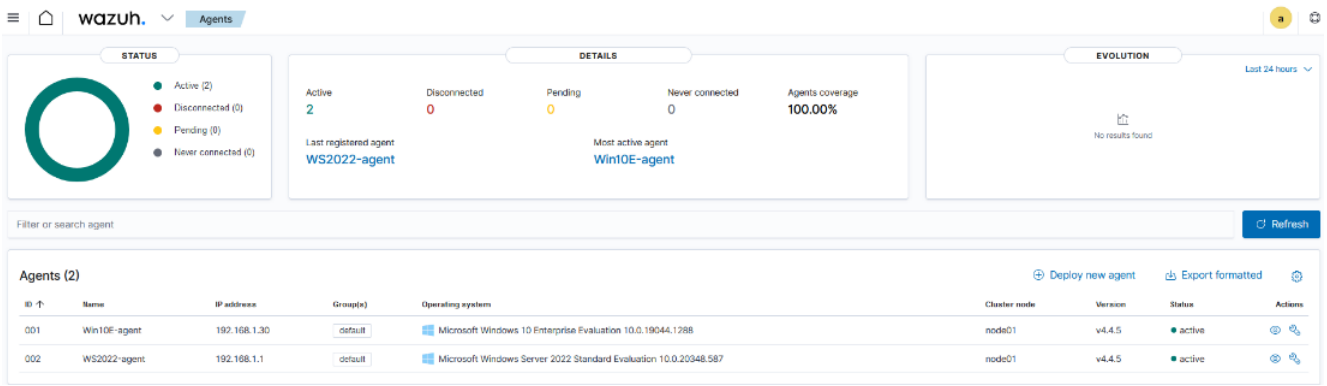
```
PS C:\Users\Administrator> Invoke-WebRequest -Uri https://packages.wazuh.com/4.x/windows/wazuh-agent-4.4.5-1.msi -OutFil
e ${env:tmp}\wazuh-agent.msi; msiexec.exe /i ${env:tmp}\wazuh-agent.msi /q WAZUH_MANAGER='192.168.1.50' WAZUH_REGISTRATI
ON_SERVER='192.168.1.50' WAZUH_AGENT_GROUP='default' WAZUH_AGENT_NAME='WS2022-agent'
PS C:\Users\Administrator> NET START WazuhSvc

The Wazuh service was started successfully.

PS C:\Users\Administrator>
```

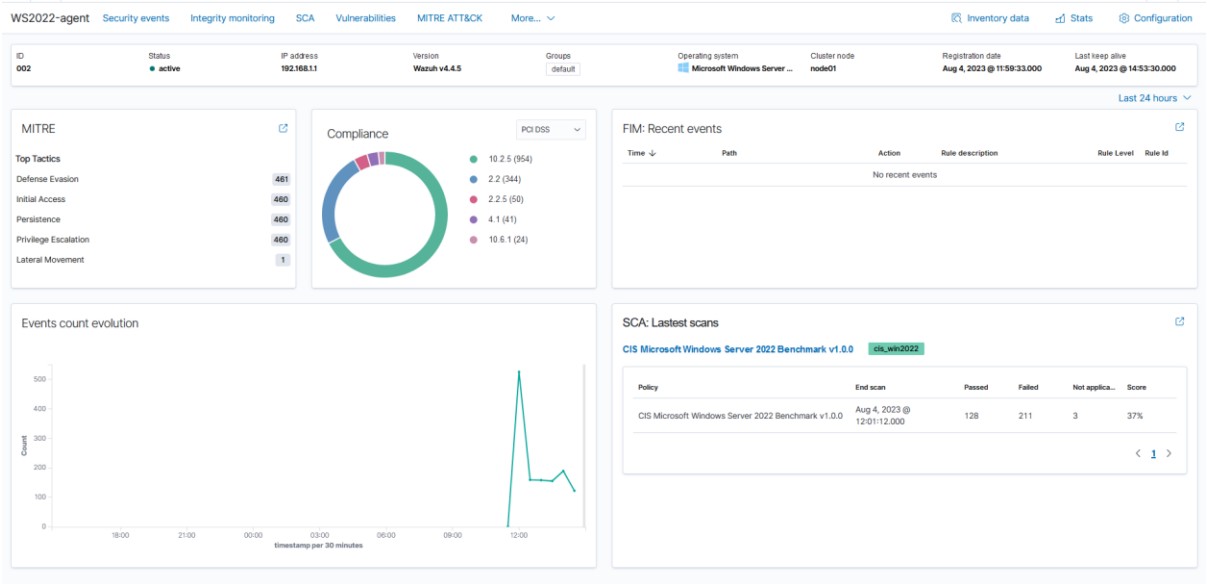
3.2.4. Weryfikacja Agentów Wazuh

Po pomyślnym wdrożeniu agentów, powinniśmy zobaczyć nowych aktywnych Agentów



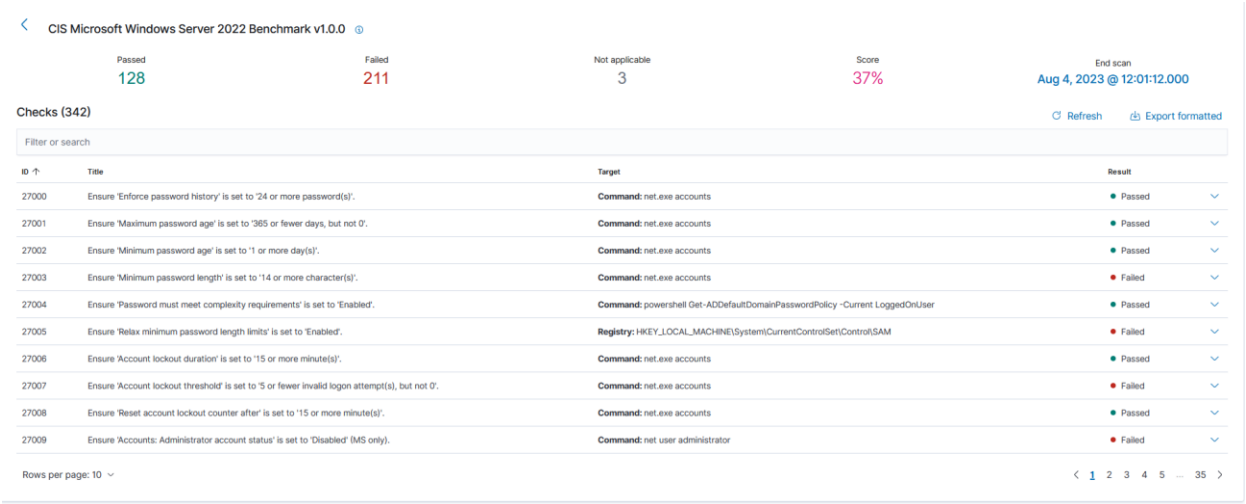
4. Analizowanie systemów za pomocą Agentów

Po wybraniu dowolnego Agenta można analizować różne zdarzenia w systemie

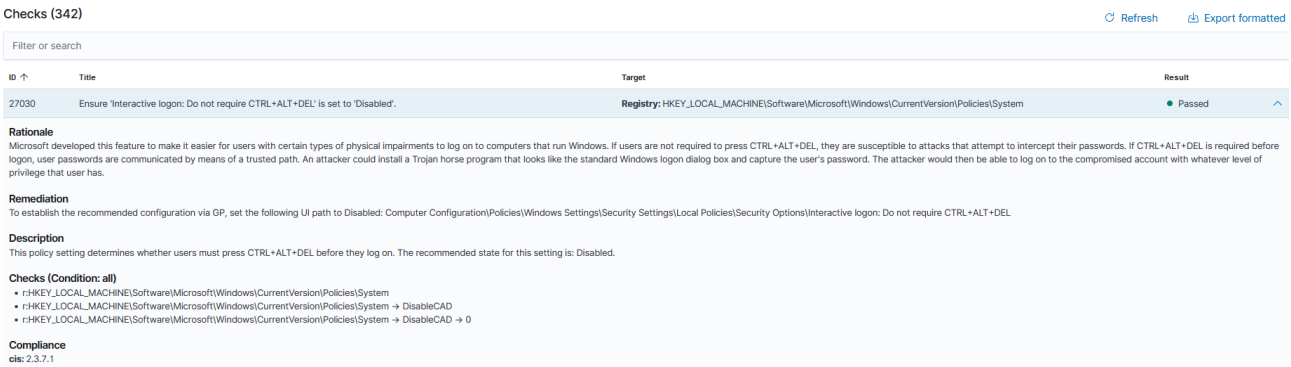


4.1. SCA – Security Configuration Assessment

Jest to moduł badający na ile jest bezpieczny system i bada go pod względem podatności



Po wybraniu danej kontroli możemy obejrzeć szczegóły uzasadniające dlaczego warto stosować dane zasady w polityce systemu bądź całej domeny



5. Materiały dodatkowe

https://www.youtube.com/watch?v=3CaG2GI1kn0 – NetworkChuck