

# **Homelab dla bezpiecznika**

domowy poligon dla pasji, nauki i pracy

**Grzegorz Wróbel**

[adwersarz.pl](http://adwersarz.pl)

# whoami

**Grzegorz Wróbel (@lochtcant)**

## Praca:

- Obecnie Security Engineer w Piwik PRO
- W IT od 12 lat, w tym 8 lat w Security
- Pisałem dla ZaufanaTrzeciaStrona.pl i Niebezpiecznik.pl

## Czas wolny:

- Współrowadzę portal **adwersarz.pl**
- Wałęsam się i śpię po lasach,
- Robię ostre sosy,
- Ostatnio drukuję w 3D,
- Rozwijam homelab



**\* Wyrażone opinie w trakcie prezentacji są wyłącznie moimi prywatnymi**

**\*\* Wspomniane rozwiązania/produkty wynikają z moich osobistych doświadczeń oraz niezależnej opinii.  
Wspominając o nich nie mam w tym żadnego interesu.**

# Agenda

## Wprowadzenie do homelabu

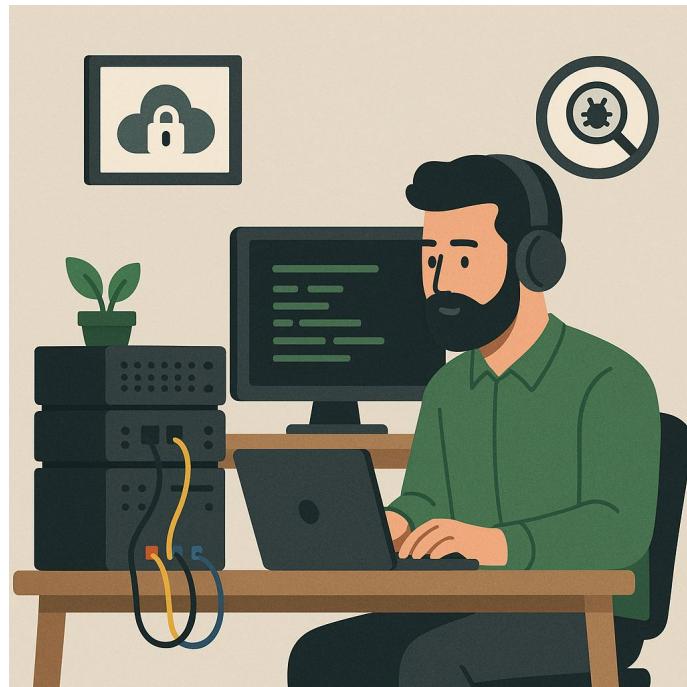
- Co to jest homelab?
- Co możemy osiągnąć?
- Jak zacząć przygodę?

## Budowanie homelabu dla bezpiecznika

- Serce i dupa homelabu
- SIEM i podstawowe usługi
- Darmowe narzędzia security

## Co dalej?

- Kierunki rozwoju
- Gdzie przecierać szlaki w homelabie?



**Kto wie co to jest homelab?**

# Kto ma w domu homelab?

# **Kto ma internet od dwóch dostawców Internetu?\***

**\* nie bierzemy pod uwagę internetu mobilnego z telefonu**

# Homelab to...

- Domowa infrastruktura sprzętowa realizująca konkretne zadania
- Poligon doświadczalny, który wybacza błędy
- Środowisko do nieskończonej zabawy
- Uzależniająca forma rozrywki oraz rozwijania pasji
- Miejsce, gdzie powstają fajne projekty
- Po prostu warsztat.



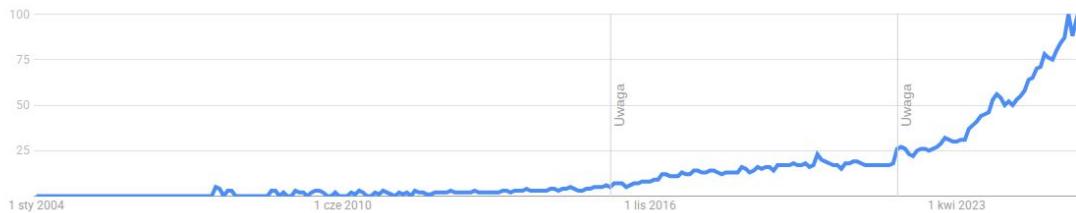
Cały świat

2004 – dziś

Wszystko

Wyszukiwarka Google

Zainteresowanie w ujęciu czasowym ②



## Homelab w Google Trends

Świat: wzrost w okolicy 2016

Polska

2004 – dziś

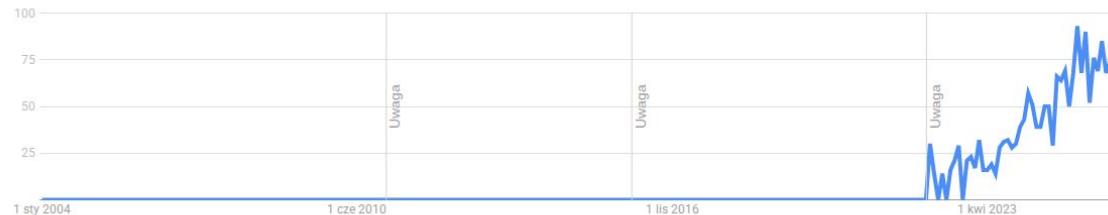
Wszystko

Wyszukiwarka Google

Zainteresowanie w ujęciu czasowym ②



Polska: wzrost z początkiem 2022





#Hackroom

RK146 - Pogaduchy do cyberpoduchy! | Rozmowa Kontrolowana

Zaufana Trzecia Strona  
9,88 tys. subskrybentów



<https://www.youtube.com/watch?v=Rw29KluFSkw>

# Homelab vs. Cloud

- Co jest lepsze? To zależy od Waszych potrzeb.
- Finalnie można mieć hybrydowe rozwiązanie
  - Homelab w domu
  - Dedyki/VPSy u dostawcy
  - Całość połączona VPNem / Tunelami CF/ZeroTier

# Homelab vs. Cloud

	<b>Homelab</b>	<b>Cloud</b>
Koszty	Sprzęt, eksploatacja, prąd, Internet	Koszt subskrypcji usług/serwerów
Rozbudowa	Możliwa tanim kosztem	Najczęściej dodatkowo płatna i limitowana
Dostępność rozwiązań	Mnoga ilość wersji self-hosted	Zależna od dostawcy i wsparcia
Publiczny IP	Zależy od ISP, ale można obejść*	Publicznie dostępne
Limity	Możliwa praca offline	Bez Internetu nie da rady

**Czy Homelab to wyłącznie serwerownia w domu?**

To też zależy :)

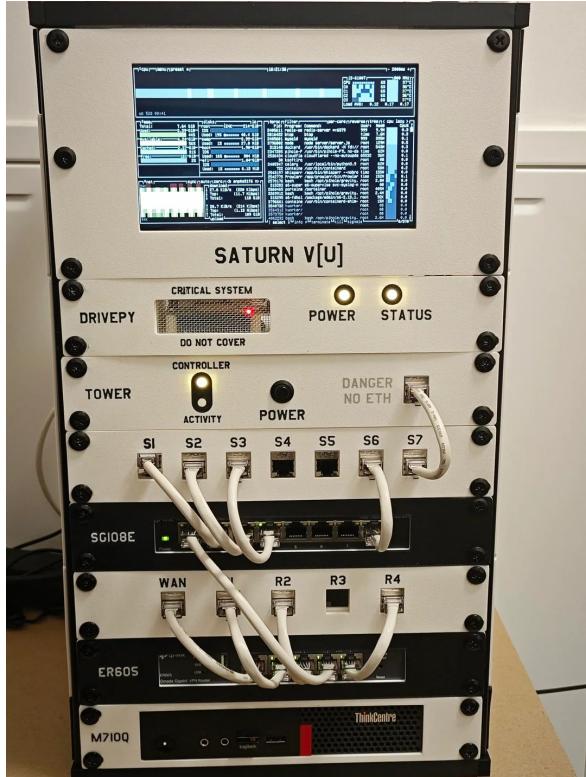
# Homelaby mogą być małe



# Mogą stać przy biurku



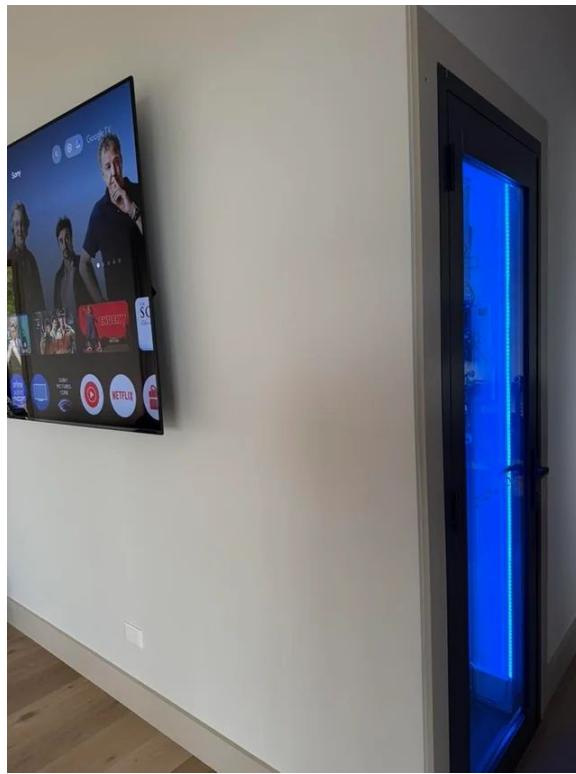
# Mogą być bardziej widoczne



# A mogą być także schowane



# Mogą stać obok salonu



# A mogą i na podwórku



# Mój homelab

Router: Unifi UDM PRO

Switch: Unifi USW-Pro-HD-24

Wi-Fi: Unifi U7-PRO

NAS:

- Synology DS716II (2x 3TB HDD)
- Unifi Pro NAS (6x 6TB HDD)

Serwer:

- Składany PC na Ryzen 7 5700G
- Raspberry Pi 4 8GB

UPS: APC 750W

Pobór mocy na co dzień: ~130-145W



**Czemu realnie może posłużyć homelab?**

# Cele homelabu

## Bezpieczeństwo i prywatność

- Eliminowanie telemetrii
- Kontrola nad domową siecią i danymi (np. własny VPN)
- Chcemy unikać rozwiązań cloudowych
- Ochrona dzieci/rodziny przed zagrożeniami

# Cele homelabu

## Bezpieczeństwo i prywatność

- Eliminowanie telemetrii
- Kontrola nad domową siecią i danymi (np. własny VPN)
- Chcemy unikać rozwiązań cloudowych
- Ochrona dzieci/rodziny przed zagrożeniami

## Rozwój lub przebranżowienie

- Swoboda i niezależność w testowaniu nowych narzędzi
- Bezpieczna możliwość testowania, psucia i naprawiania
- Niezależność od subskrypcji lub limitów dostawcy
- Chcemy zmienić branżę i pójść pracować w security

# Cele homelabu

## Bezpieczeństwo i prywatność

- Eliminowanie telemetrii
- Kontrola nad domową siecią i danymi (np. własny VPN)
- Chcemy unikać rozwiązań cloudowych
- Ochrona dzieci/rodziny przed zagrożeniami

## Rozwój lub przebranżowienie

- Swoboda i niezależność w testowaniu nowych narzędzi
- Bezpieczna możliwość testowania, psucia i naprawiania
- Niezależność od subskrypcji lub limitów dostawcy
- Chcemy zmienić branżę i pójść pracować w security

## Uzupełnianie wiedzy

- Sprzęt sieciowy, elektronika
- Zarządzanie sieciami
- Administracja Linuxem/Windows
- Poznanie rozwiązań devopsowych (np. Ansible, K8S)

# Cele homelabu

<b>Bezpieczeństwo i prywatność</b> <ul style="list-style-type: none"><li>- Eliminowanie telemetrii</li><li>- Kontrola nad domową siecią i danymi (np. własny VPN)</li><li>- Chcemy unikać rozwiązań cloudowych</li><li>- Ochrona dzieci/rodziny przed zagrożeniami</li></ul>	<b>Rozwój lub przebranżowienie</b> <ul style="list-style-type: none"><li>- Swoboda i niezależność w testowaniu nowych narzędzi</li><li>- Bezpieczna możliwość testowania, psucia i naprawiania</li><li>- Niezależność od subskrypcji lub limitów dostawcy</li><li>- Chcemy zmienić branżę i pójść pracować w security</li></ul>
<b>Uzupełnianie wiedzy</b> <ul style="list-style-type: none"><li>- Sprzęt sieciowy, elektronika</li><li>- Zarządzanie sieciami</li><li>- Administracja Linuxem/Windows</li><li>- Poznanie rozwiązań devopsowych (np. Ansible, K8S)</li></ul>	<b>Przygotowanie do certyfikacji</b> <ul style="list-style-type: none"><li>- Łatwe do postawienia środowiska do nauki i testów</li><li>- Szybka adaptacja do materiału do nauki</li><li>- Pentesterskie: OSCP, OSWE, eJPTi itd.</li><li>- Incident Response, Blue Team, Malware</li></ul>

# Cele homelabu

<b>Bezpieczeństwo i prywatność</b> <ul style="list-style-type: none"><li>- Eliminowanie telemetrii</li><li>- Kontrola nad domową siecią i danymi (np. własny VPN)</li><li>- Chcemy unikać rozwiązań cloudowych</li><li>- Ochrona dzieci/rodziny przed zagrożeniami</li></ul>	<b>Rozwój lub przebranżowienie</b> <ul style="list-style-type: none"><li>- Swoboda i niezależność w testowaniu nowych narzędzi</li><li>- Bezpieczna możliwość testowania, psucia i naprawiania</li><li>- Niezależność od subskrypcji lub limitów dostawcy</li><li>- Chcemy zmienić branżę i pójść pracować w security</li></ul>
<b>Uzupełnianie wiedzy</b> <ul style="list-style-type: none"><li>- Sprzęt sieciowy, elektronika</li><li>- Zarządzanie sieciami</li><li>- Administracja Linuxem/Windows</li><li>- Poznanie rozwiązań devopsowych (np. Ansible, K8S)</li></ul>	<b>Przygotowanie do certyfikacji</b> <ul style="list-style-type: none"><li>- Łatwe do postawienia środowiska do nauki i testów</li><li>- Szybka adaptacja do materiału do nauki</li><li>- Pentesterskie: OSCP, OSWE, eJPTi itd.</li><li>- Incident Response, Blue Team, Malware</li></ul>
	<b>Użytek domowy</b> <ul style="list-style-type: none"><li>- Prywatne dane i multimedia</li><li>- Kamery IP lub Home Assistant</li></ul>

# Budowa i rozwój homelabu

- Mając wizję celu łatwiej zacząć
- Opisanie kroków
- Określenie planów minimum per sloty czasowe
- Lista będzie tylko powiększać się

Handwritten notes on a whiteboard detailing a 14-step build and development process for a home lab:

1. Instalacja Hosta
2. Dodanie agentów
3. Rops GH no config
4. Zabbix update
5. Dodanie agentów zabbix
6. Dashboardy
  - WAZUH
  - ZABBIX -> GRAFANA
7. Backup -> Echo
8. RunZero -> Explorar ✓
9. Nessus
10. Syslog -> Unifi -> WAZUH
11. 26x Unifi SNMP
- 12 26x Synology SNMP
- Unifi decoders Wazuh
13. SOAR -> Tracecast
14. PKI -> root ca  
intvuz.net

Notes on the right side of the board:

- VLANY
- PXE VM
- Playbook
- Update
- hardware
- Dashboard
- CPU ✓
- RAM ✓
- Storage ✓
- ETH

# To nie zawsze pięknie wygląda..

- Momentami mozołny postęp prac
  - Metoda prób i błędów
  - Czasem dziwne zdarzenia, restarty, brak komunikacji...

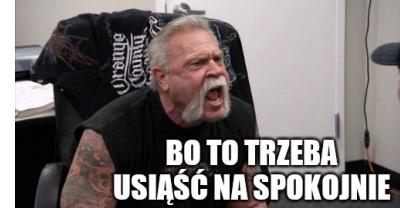
# To nie zawsze pięknie wygląda..

- Momentami mozołny postęp prac
  - Metoda prób i błędów
  - Czasem dziwne zdarzenia, restarty, brak komunikacji... **Wystarczy spóźnić się z kolacją :)**



# To nie zawsze pięknie wygląda..

- Zasada “więcej sprzętu niż talentu” :D
- Nie zawsze przemyślane zakupy
- Regularnie overkill
  - Ale do tego trzeba się przyzwyczaić/pokochać
- Doba ma (niestety) tylko 24h...
- Kaprysy wdrażanych usług (lub już działających)

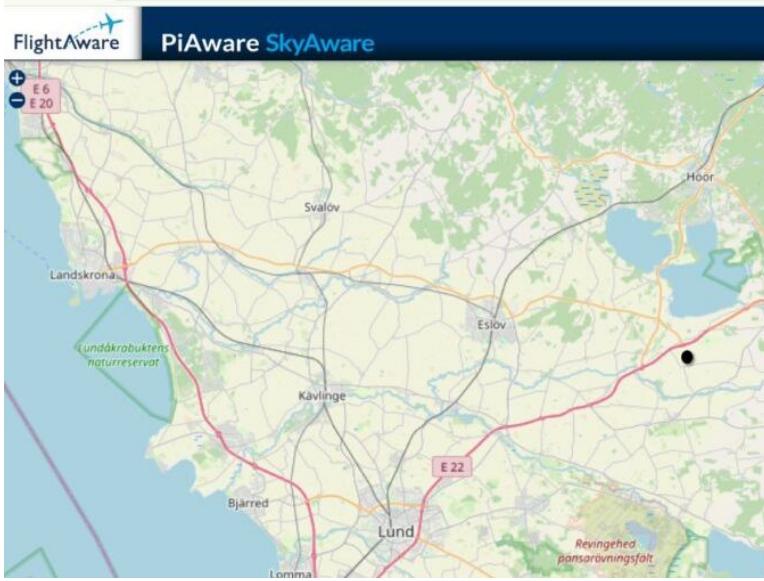




It works, but: I'm a homelabber. I love overkill!

# Na co uważać, czego nie robić?

- Właściwe podłączenie i konserwacja sprzętu
- Ochrona przed zwierzakami
- Gaśnicę (wskażana śniegowa/CO2)
- Dbać o bezpieczeństwo styku między homelabem, a Internetem
  - Ekspozycję na świat można monitorować np. przez [moje.cert.pl](https://moje.cert.pl), runZero lub Shodana



## Hans Kloss

Member since: 8 years ago

Language: English (UK)

ADS-B feeder since: March 28, 2017

Highest User Ranking Achieved in Last 30

Days: X,XXX

NOTE: Hourly data is reported in the site's local time. Daily data is reported in UTC time.

These statistics reflect ADS-B feeder sites for [epkfrc4](#) | [View all FlightAware ADS-B Statistics](#) | [View ADS-B Coverage Map](#)

### SITE XXX – ESMS

#### WEB INTERFACES

Local Web Interfaces (Local Network Connection Required)

Remote Web Interfaces

#### SITE INFORMATION

Data Feed: September 4, 2025

Nearest Airport: Malmö (Malmö) (ESMS)

Joined: July 16, 2019

Location: (XX.4, XX.3)



# Na co uważać, czego nie robić?

- Homelab niekoniecznie jest dobry do zarabiania
  - A na pewno stawia tu sporo wyzwań
  - [grumpy.systems/2023/please-dont-sell-space-in-your-homelab](https://grumpy.systems/2023/please-dont-sell-space-in-your-homelab)
- Rozdzielać pracę od homelaba i nie wpaść w pracoholizm
- I nie przeginać, praca siedząca nie jest zdrowa :)

**Budujemy homelab.**

# Gdy już jesteśmy zdecydowani

- **Potrzebujemy na początek:**
  - Mieć na czym odpalić środowisko (Proxmox, KVM)
  - Mieć gdzie przechowywać backupy (NAS np. TrueNAS, Synology, QNAP)
- **Z biegiem czasu dojdą:**
  - Zasilacz awaryjny UPS
  - Bardziej zaawansowany router + firewall (np. OPSense, PFSense, Mikrotik, Unifi, etc.)
  - Switch 2.5Gb/10Gb
  - Dodatkowe urządzenia (np. miniPC, Raspberry-Pi, etc.)
  - Szafa RACK 10"/19"
  - Kolejne serwery? :D

# Skąd pozyskać sprzęt?

- Kupić nowy albo poleasingowy

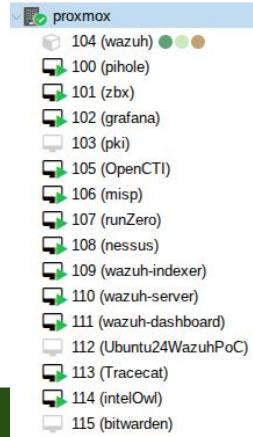
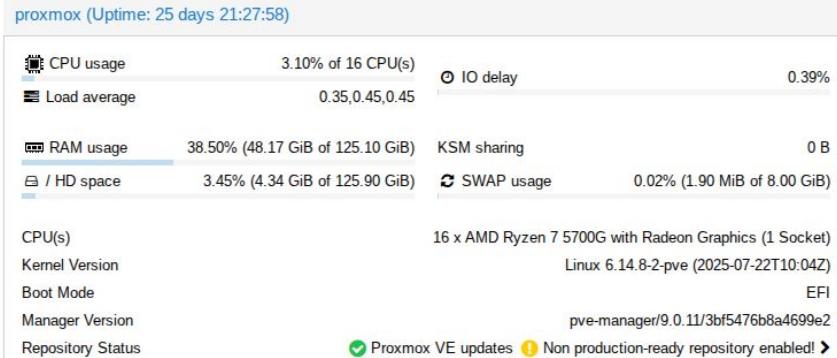


Okazyjna cena! To dokupię RAMu żeby mieć 64GB i będzie gitara.

Szkoda tylko, że wspiera max 16 GB RAM... Po fakcie.

# Skąd pozyskać sprzęt?

- Kupić nowy albo poleasingowy
  - Złożyć samemu komputer
- 
- CPU: Ryzen 7 5700G 8 rdzeni, 16 wątków
  - RAM: 128GB DDR4
  - Dyski:
    - 1TB M2
    - 2TB M2
    - 480GB SSD
  - Zasilacz: Corsair 550W
  - Proxmox 9.0.11, 11 VM pracujących 24/7
  - Pobór mocy: ~65W





# Skąd pozyskać sprzęt?

- Kupić nowy albo poleasingowy
- Złożyć samemu komputer
- Przejrzeć oferty z ogłoszeniami na portalach aukcyjnych lub lokalnymi
  - Lub oferty wyprzedaży w firmach
  - Grupa FB: DevOps/SysOps: Bazarek

To tylko szafa serwerowa 72U (~210cm wysokości)

Koszt? 200 zł

W 55m<sup>2</sup> mieszkaniu wytrzymała... 2 miesiące :)



# Platformy miniPC

- Używane “Mini-PC” przeżywają drugą młodość w homelabach
  - Świecznie nadają się pod OPNsense, Proxmoxa lub TrueNAS
- 
- Przykładowy HP ProDesk G3 600
  - CPU i5-7500T + 8GB RAM + 256 GB SSD
  - Dwie karty sieciowe 1Gb
  - Cena: 550 zł.

Oczywiście można taniej!





Intel NUC energooszczędny miniPC HDn-5i5MYBE  
i5-5300u Nvme 120GB Win10

350 zł

Używane

36750 zł z Pakietem Ochronnym

Ormontowice - 23 listopada 2025



Intel Nuc d34010wyk 2 sztuki

350 zł

do negocjacji

Używane

Tczew - 17 listopada 2025



Komputer Intel NUC NUC5i7RYH i7/8GB  
RAM/128GB SSD/512 HDD/WIN10 PRO

350 zł

Używane

Radzymin - 15 listopada 2025



GMKtec G3 Mini PC Intel Alder Lake N100 8gb ram 256 dysk

459 zł

Nowe

Warszawa, Mokotów - 16 listopada 2025



MiniPC Gmktc G3 Mini Intel N100 8Gb/16Gb 2.5Gb ethernet - nowy  
folia

495 zł

Nowe

Ryki - 16 listopada 2025



Minikomputer gmktc nucbox g3 8gb/256gb - kompletny zestaw

500 zł

Nowe

Wrocław, Stare Miasto - 14 listopada 2025



Zanim kupisz  
**Raspberry Pi 5**



POS5000: WYPAS NAS  
po taniości

22:00



NAJLEPSZY TERMINAL\*  
\*możesz wybrać sam :)

54:16



HP T630  
brać i  
uitekać\*

14:20



Wszystko co chciałbyś wiedzieć o Raspberry  
Pi 5 ale nie masz kogo zapytać

109 tys. wyświetleń • 1 rok temu



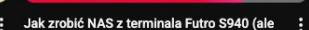
DELL WYSE  
**5070**

Światło mówią  
że warto !!!



Jak zrobić NAS z terminala Futro S940 (ale  
takie szybkie, oszczędnego i ciche)

82 tys. wyświetleń • 9 miesięcy temu



Odroid H4 Plus - twój nowy serwer domowy

69 tys. wyświetleń • 1 rok temu



Pi-hole i Unbound - Zadbaj o swoje  
bezpieczeństwo !!

60 tys. wyświetleń • 3 lata temu



**tata.geek.**

@tatageek • 23 tys. subskrybentów • 119 filmów

Pokazuję ciekawe rzeczy z świata IT, dostępnego

instagram.com/tata.geek

# Tylko co postawić?

- Spora ilość rozwiązań self-hosted w modelu Open-Source
  - [github.com/ccbikai/awesome-homelab](https://github.com/ccbikai/awesome-homelab)
  - [github.com/awesome-selfhosted/awesome-selfhosted](https://github.com/awesome-selfhosted/awesome-selfhosted)
- Wirtualizacja / Konteneryzacja - warto zacząć od Proxmoxa
- Na początek przydatne, praktyczne rozwiązania:
  - Pi-Hole jako serwer DNS do wycinania niechcianego ruchu
  - TrueNAS do backupów
  - Bitwarden do zarządzania hasłami/dostępami
  - TLS wewnątrz sieci (własne PKI lub Let's Encrypt)
  - Własne projekty - np. radar lotniczy

# Domowe projekty?

# Radar lotniczy

- Dystrybucja Pi-Aware dla Raspberry-Pi
- Agreguje dane z komunikacji ADS-B z samolotami

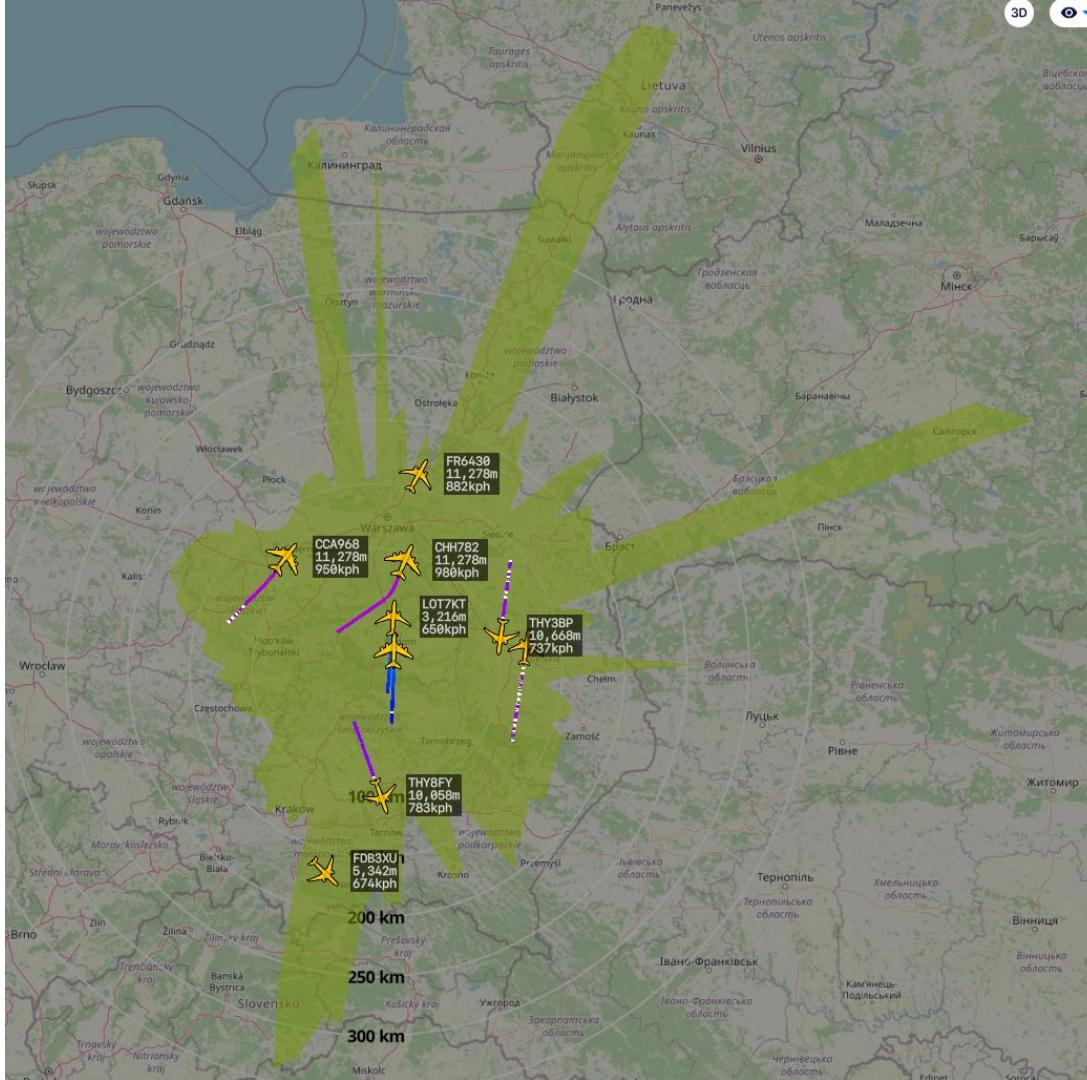
## Korzyści:

- Dostęp enterprise do np. Flightradar24 za darmo
- Dużo losowych danych (np. do programowania)
- Wyzwania OSINT (historia lotów 3 lata wstecz)
  - Dedykowany kanał na DC Bellingcat



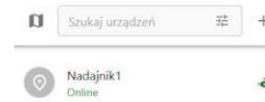
# aviation

This channel is for discussing flight tracking and aviation topics



# Monitoring GPS (w planach)

- Rozwiązanie oparte o opensource-owy Traccar ([traccar.org](http://traccar.org))
- Własny system monitoringu GPS
- Nie płacimy za subskrypcje
- Logi zostają u nas



# Homelab dla bezpiecznika od podstaw

# Proxmox - serce homelabu

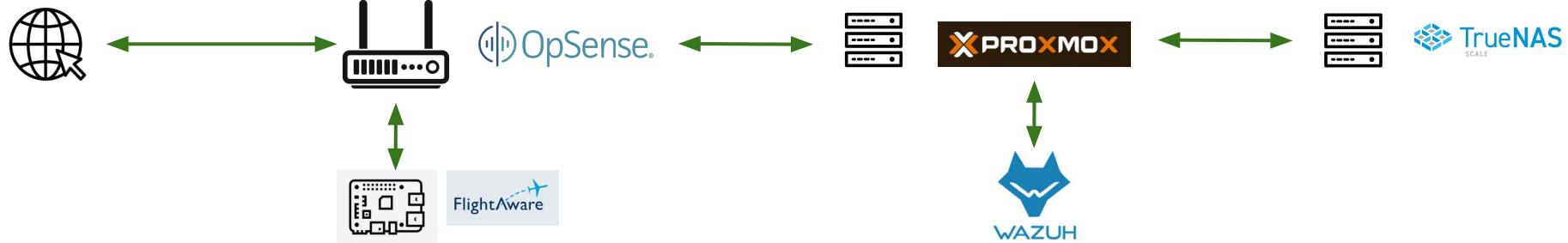
- Niski próg wejścia i darmowy
- Spore community i dużo przetartych ścieżek
- Łatwa implementacja rozwiązań
  - [community-scripts.github.io/ProxmoxVE/scripts](https://community-scripts.github.io/ProxmoxVE/scripts)
- Mało awaryjny
- Możliwość pracy z maszynami wirtualnymi lub kontenerami LXD
- Wbudowane usługi (firewall, backup, monitoring, etc.)

# NAS - dupa homelabu

- Ratuje i pozwala miękko wylądować
- Wyrabiamy nawyk
- Automatyzujemy backup
- Backup na tym samym sprzęcie jest zły
- Homelab to poligon prób i błędów
- TrueNAS, Synology lub QNAP?
  - Łatwa instalacja i wdrożenie
  - Sporo wbudowanych aplikacji
  - Dużo usług sieciowych by default
  - <https://blog.briancmoses.com/2025/11/diy-nas-2026-edition.html> <- bardzo fajny guideline jak budować NAS samodzielnie pod TrueNASa

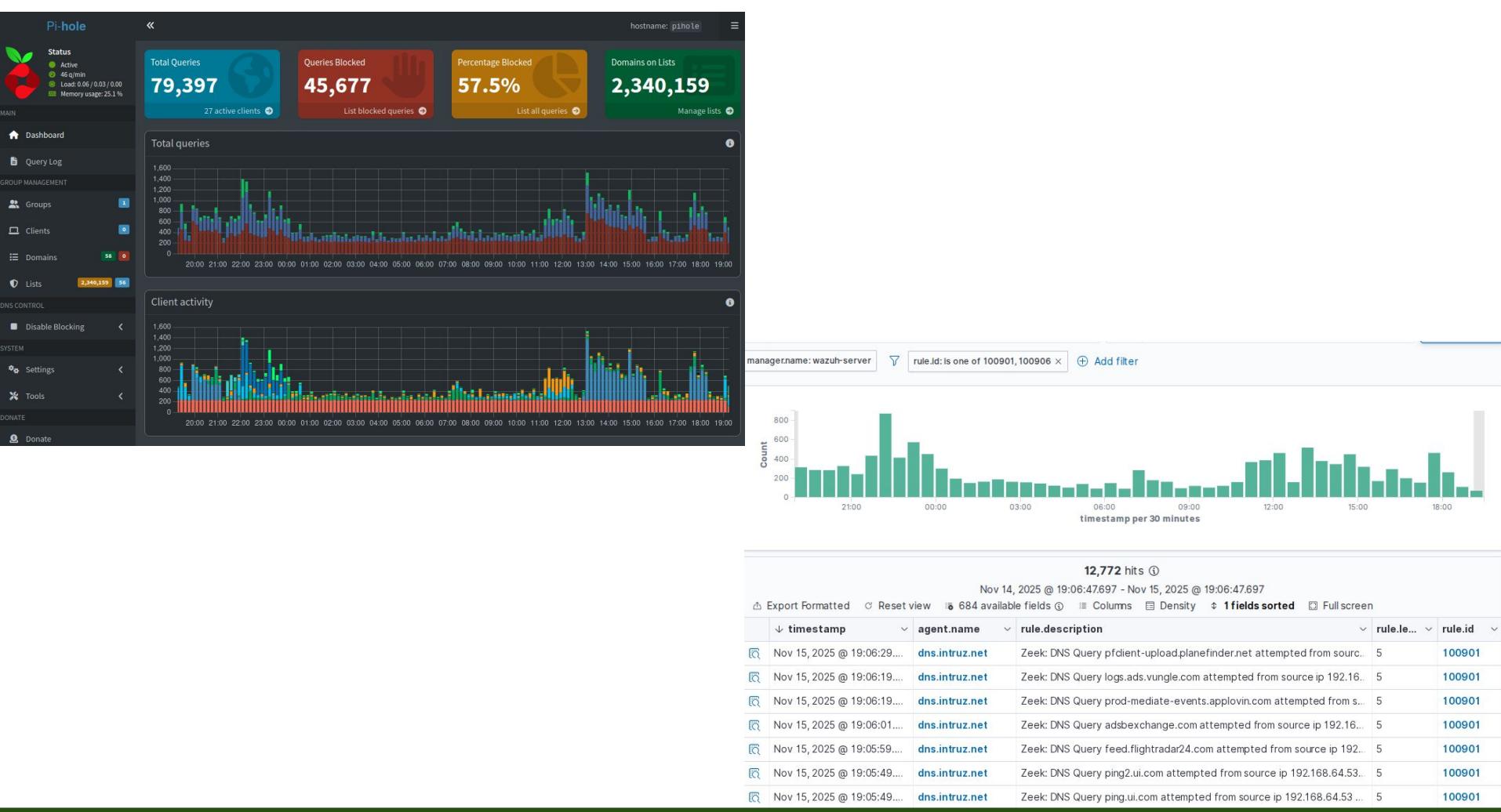
# SIEM w homelabie

- Świeetnie sprawdzi się Wazuh
  - Open Source
  - Sporo możliwych integracji
  - Coraz lepsza reputacja + rosnąca popularność
- Świeetne narzędzie do nauki i rozwijania kompetencji w obszarze IT Sec
  - Implementacja reguł wykrywania anomalii np. na Linux/Windows/MacOS
  - Lepsze zrozumienie technik ataków
  - Praktyczna zabawa z sysmon czy auditd
  - [wazuh.com/blog/](http://wazuh.com/blog/) - kopalnia wiedzy jak można integrować Wazuh
  - Wazuh już w domyślnej konfiguracji identyfikuje zagrożenia (np. podatności, braki w hardeningu, etc.)



# DNS, monitoring zasobów

- Centralny DNS w homelabie
  - Wycina złośliwe domeny, telemetrie, reklamy
  - Łatwiejsza komunikacja w homelabie
- Zabbix - monitorowanie parametrów serwerów
  - wyłapujemy brakujące zasoby na hostach
- Grafana - ładniejsze wykresy
- Rośnie liczba danych do analizy dla Wazuhu

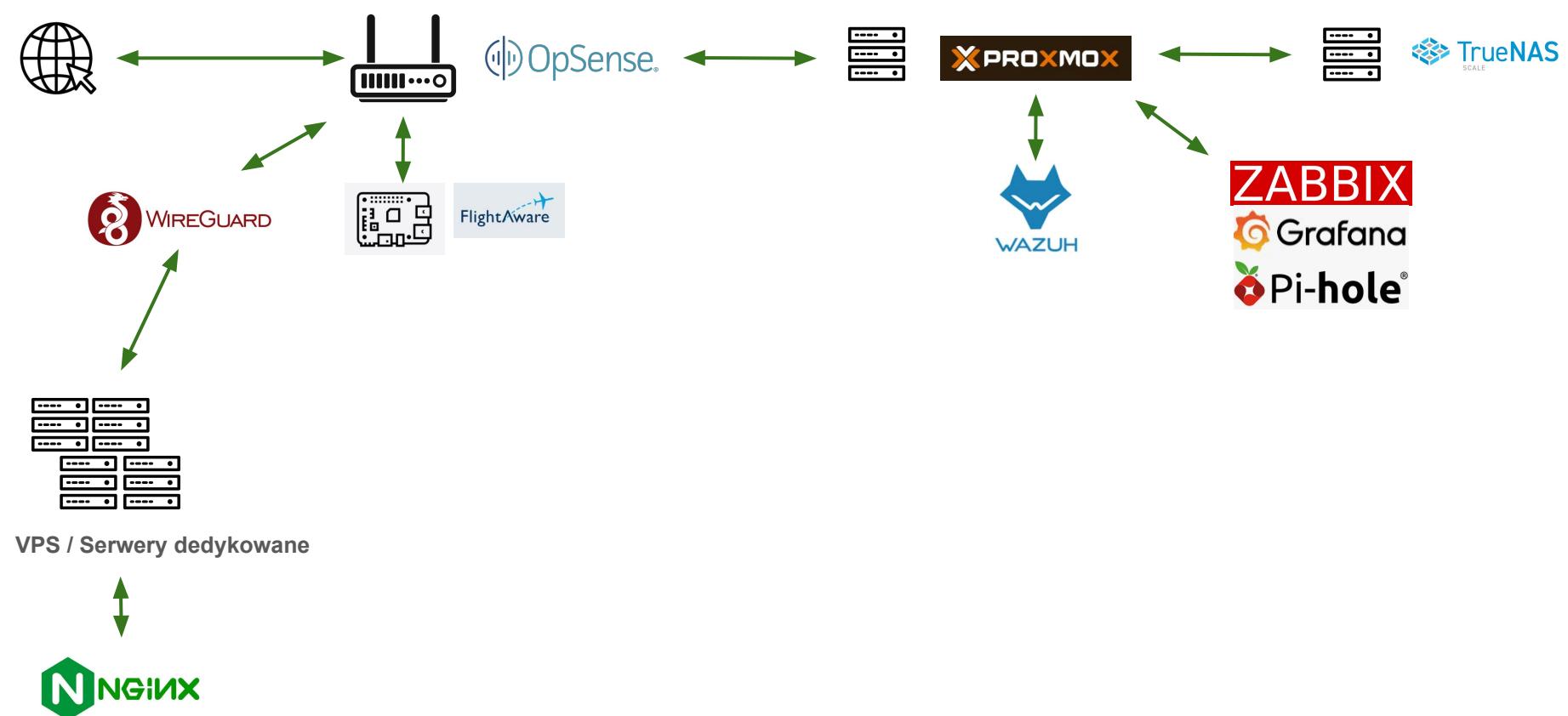


# VPN

- Dobra alternatywa od dostępnych obecnie usług VPN
- Pełna kontrola i wpływ na bezpieczeństwo
  - Logi zostają u nas
- Niestety ekspozycja usługi na świat
- Przydatne w podróży lub na wyjazdach
- Wykorzystanie usług w routerze
- Można też postawić własny serwer

# Hybrydowy homelab

- VPS/Serwer dedykowany (warto polować w okolicach Black Friday!)
- Wymaga stworzenia sieci VPN z homelabem (kolejne dobre doświadczenia)
- Dostarcza realistyczne zdarzenia i scenariusze
- Warto pomyśleć o honeypotach
- Ale wybacza mniejszą ilość błędów



VPS / Serwery dedykowane



# Więcej usług, więcej utrzymania

- Podatności do latania
- Utrzymanie i hardening
- Logowanie danych
- Monitorowanie zdarzeń
  
- Nie musimy ograniczać się tylko do Wazuha

# RunZero

- Platforma stworzona przez HD Moore'a (twórca Metasploita)
- Dostępny w wersji Community z szerokimi możliwościami
- Skany z wykorzystaniem agenta (tzw. "explorera") w sieci lokalnej
- Skanuje także publicznie IP/domeny
- Cykliczne skanowanie i agregowanie informacji o sieci
- Integracje z usługami/platformami cloudowymi (np. Shodan, Azure, AWS, etc.)
- Limit to "tylko" 100 assetów

Our free Community Edition is great for  
small businesses & security nerds.

					OS	Type	Hardware	
I.1+1			Low	Unset		Ubiquiti UDM Pro		Network Appliance
I.2+1			Low	Unset		Ubiquiti Linux 4.4.4		Ubiquiti UNAS Pro
I.20+1			Low	Unset		Ubuntu Linux 24.04		Proxmox VM
I.21+1			None	Unset		Ubuntu Linux 24.04		Proxmox VM
I.22+1			Low	Unset		Ubuntu Linux 24.04		Proxmox VM
I.23			None	Unset				
I.24+1			None	Unset		Ubuntu Linux 24.04		Proxmox VM
I.30			None	Unset				
I.31+1			None	Unset		Apple iOS 26.0.1		Apple iPhone 15 Pro
I.40			Low	Unset		Synology DSM		Synology DiskStation DS716+II
I.53+1			Low	Unset		Ubuntu Linux 24.04		Proxmox VM
I.81+1			None	Unset		Ubiquiti Linux		Ubiquiti Device
I.93+1			None	Unset		Ubuntu Linux 24.04		Proxmox VM
I.99+1			Low	Unset		Proxmox PVE 9.0.11		
I.104			None	Unset		Ubuntu Linux 24.04		Proxmox VM
I.111+1			None	Unset		Ubiquiti Linux		Ubiquiti Device
I.112+1			None	Unset				Proxmox VM
I.138			Info	Unset		Debian Linux 12		Proxmox VM
I.189			None	Unset				
I.192+1			Info	Unset		Ubuntu Linux 24.04		Proxmox VM

Attrs	Address	↓   Transport	Port	Protocol	VHost	Service response	Hostname	OS	Type
✓	192.168.1.100:80	TCP	80	http	↗	HTTP/1.1 200 OK Content-Type: text/html ETag: "843414280" Last-Modified: Thu, 13 Nov 2014 11:42:00 GMT Date: Thu, 13 Nov 2014 11:42:00 GMT Server: nginx	VM1	Linux	Server
✓	192.168.1.100:123	UDP	123	ntp			VM1	Linux	Server
✓	192.168.1.100:5353	UDP	5353	mdns			VM1	Linux	Server
✓	192.168.1.100:10050	TCP	10050				VM1	Linux	Server
✓	192.168.1.100:1	ICMP					VM1	Linux	Server
✓	192.168.1.100:1	NDP					VM1	Linux	Server
✓	192.168.1.100:1	ICMP					VM1	Ubiquiti Linux	Device
✓	192.168.1.100:1	NDP					VM1	Ubiquiti Linux	Device
✓	192.168.1.100:1	NDP					VM1	Ubiquiti Linux	Device
✓	192.168.1.100:1	ICMP					VM1	Ubiquiti Linux	Device
✓	192.168.1.100:22	TCP	22	ssh	↗	SSH-2.0-OpenSSH_9.2p1-2+deb12u7	VM1	Linux	Server
✓	192.168.1.100:80	TCP	80	http	↗	HTTP/1.1 200 OK Content-Type: text/html ETag: "843414280" Last-Modified: Thu, 13 Nov 2014 11:42:00 GMT Date: Thu, 13 Nov 2014 11:42:00 GMT Server: nginx	VM1	Linux	Server
✓	192.168.1.100:123	UDP	123	ntp			VM1	Linux	Server
✓	192.168.1.100:5353	UDP	5353	mdns			VM1	Linux	Server
✓	192.168.1.100:10050	TCP	10050				VM1	Linux	Server
✓	192.168.1.100:1	NDP					VM1	Linux	Server
✓	192.168.1.100:1	ICMP					VM1	Linux	Server
✗	192.168.1.100:22	TCP	22	ssh	↗	SSH-2.0-OpenSSH_10.0p2 Debian-7	PROXMOX	Proxmox PVE 9.0.11	Hypervisor
✗	192.168.1.100:111	TCP	111	sunrpc			PROXMOX	Proxmox PVE 9.0.11	Hypervisor
✗	192.168.1.100:111	UDP	111	sunrpc			PROXMOX	Proxmox PVE 9.0.11	Hypervisor
✗	192.168.1.100:3128	TCP	3128	http	↗	HTTP/1.1 501 method 'GET' not available Cache-Control: max-age=0 Content-Type: text/html; charset=iso-8859-1	PROXMOX	Proxmox PVE 9.0.11	Hypervisor
✗	192.168.1.100:8006	TCP	8006	http,tls	↗	HTTP/1.1 301 Moved Permanently Cache-Control: max-age=0 Content-Type: text/html; charset=iso-8859-1	PROXMOX	Proxmox PVE 9.0.11	Hypervisor
✗	192.168.1.100:10050	TCP	10050				PROXMOX	Proxmox PVE 9.0.11	Hypervisor
✗	192.168.1.100:1	NDP					PROXMOX	Proxmox PVE 9.0.11	Hypervisor
✗	192.168.1.100:1	ICMP					PROXMOX	Proxmox PVE 9.0.11	Hypervisor
✗	192.168.1.100:80	TCP	80	http	↗	HTTP/1.1 301 Moved Permanently Server: nginx Date: Thu, 13 Nov 2014 11:42:00 GMT Location: /index.html Content-Type: text/html; charset=iso-8859-1	192.168.1.100	Ubiquiti Linux 4.4.4	NAS
✗	192.168.1.100:111	TCP	111	sunrpc			192.168.1.100	Ubiquiti Linux 4.4.4	NAS

# Nessus Essentials

- Dozwolony do prywatnego użytku
- Max 16 IP per skanowanie
- Bogata oferta skanowania (od podstawowych po bardziej zaawansowane)
- Możliwość skanowania sieci lub web aplikacje
- Doświadczenia z Nessusem
- Cyklicznie dostarcza informacje o bezpieczeństwie w homelabie

## Scanner

### DISCOVERY

 Host Discovery  
A simple scan to discover live hosts and open ports.

 Ping-Only Discovery  
A simple scan to discover live hosts with minimal network traffic.

### VULNERABILITIES

 Basic Network Scan  
A full system scan suitable for any host.

 Credential Validation  
Verify that host credential pairs for Windows & Unix successfully authenticate to scan targets.

 Advanced Scan  
Configure a scan without using any recommendations.

 Advanced Dynamic Scan  
Configure a dynamic plugin scan without recommendations.

 Malware Scan  
Scan for malware on Windows and Unix systems.



Nessus 10.8.0 / 10.8.1 Agent Reset

Scan to find, reset, and update Nessus 10.8.0 / 10.8.1 Agents.

 Mobile Device Scan  
Assess mobile devices via Microsoft Exchange or an MDM.

 Web Application Tests  
Scan for published and unknown web vulnerabilities using Nessus Scanner.

 Credentialed Patch Audit  
Authenticate to hosts and enumerate missing updates.

 Active Directory Starter Scan  
Look for misconfigurations in Active Directory.

 Find AI  
AI, LLM, ML related detections and vulnerabilities

### COMPLIANCE

 Audit Cloud Infrastructure  
Audit the configuration of third-party cloud services.

 Internal PCI Network Scan  
Perform an internal PCI DSS (11.2.1) vulnerability scan.

 MDM Config Audit  
Audit the configuration of mobile device managers.

 Offline Config Audit  
Audit the configuration of network devices.

 PCI Quarterly External Scan  
Approved for quarterly external scanning as required by PCI.



Policy Compliance Auditing

Audit system configurations against a known baseline.

 SCAP and OVAL Auditing  
Audit systems using SCAP and OVAL definitions.

## ADS scan part 1

[Back to My Scans](#)

Hosts 9 Vulnerabilities 8 Notes 1 History 2

Filter ▾ Search Vulnerabilities 8 Vulnerabilities

Sev ▾	CVSS ▾	VPR ▾	EPSS ▾	Name ▾
MEDIUM	6.5	4.0	0.0596	IP Forwarding Enabled
MEDIUM	6.5			HSTS Missing From HTTPS Server (RFC 6797)
MEDIUM	5.3			SMB Signing not required
MEDIUM	...	...	...	SSL (Multiple Issues)
LOW	3.3 *			DHCP Server Detection
LOW	2.1 *	2.2	0.0037	ICMP Timestamp Request Remote Date Disclosure
INFO				Nessus TCP scanner
INFO				Nessus Scan Information

# MISP

- *Threat Intelligence Sharing Platform* ([github.com/MISP](https://github.com/MISP))
- Darmowe narzędzie do agregowania danych o IoC (*Indicator of Compromise*)
- Whitelistowanie ruchu do wycinania false positive-ów
- Posiada masę “feedów” dostępnych za darmo do integracji
- Można go zintegrować z innymi narzędziami
- Przykładowe użycie w Wazuhu
  - monitorowane hashe filesystemie
  - wyłapywanie IP/domen w połączeniach na hostach

# Tracecat

- *All-in-one AI automation platform* ([tracecat.com](https://tracecat.com))
- Orkiestracja i automatyzacja
  - reagowanie na konkretne zdarzenia/incydenty
  - Przykłady:
    - wykryto zdarzenie na Wazuhu -> wyślij notyfikację na Slacka/E-mail
    - sprawdź hash z Wazuha na VirusTotal
- W wersji self-hosted to nielimitowany open-source
- Podobny do n8n

# Intel Owl

- Opensource-wa platforma do analizy IoC (hash, domena, URL, IP)
- Integracja m. in. z
  - VirusTotal, Shodan, AbuseIPDB, URLHaus, etc.
  - DNSy Cloudflare, Mullvad, Quad9, Google
  - Phishing army, Twitter
  - Lokalnym MISP
- Upraszczca analizę podejrzanych plików/hostów w wielu źródłach
- Oszczędza czas
- Sporo usług udostępnia darmowy API Key (z limitami)

# Scan Observables

Month: 7

Total: 7



observable (domain, IP, URL, HASH, etc...)  file

Observable Value(s) \*

http://125.43.XX.X54:38626



Add new value

Playbooks  Analyzers/Connectors

Select Analyzers

BBOT CloudFlare\_Malicious\_Detector PhishingArmy

Quad9\_Malicious\_Detector Thug\_URL\_Info TweetFeed URLhaus



7 / 61

Select Connectors

Select...

0 / 6



TLP

CLEAR  GREEN  AMBER  RED

disable analyzers that could impact privacy and limit access to my organization

Advanced settings

Start Scan

Similar Investigations:  
0



Analyzers Report 6/6

Connectors Report 0/0

Pivots Report 0/0

Visualizers Report 0/0

Full Report

Visualizer

Raw

	Actions	Status	Name	Process Time (s)	Running Time
1		All	URLhaus	0.41	10:28:25 PM - 10:28:25 PM (GMT+1)

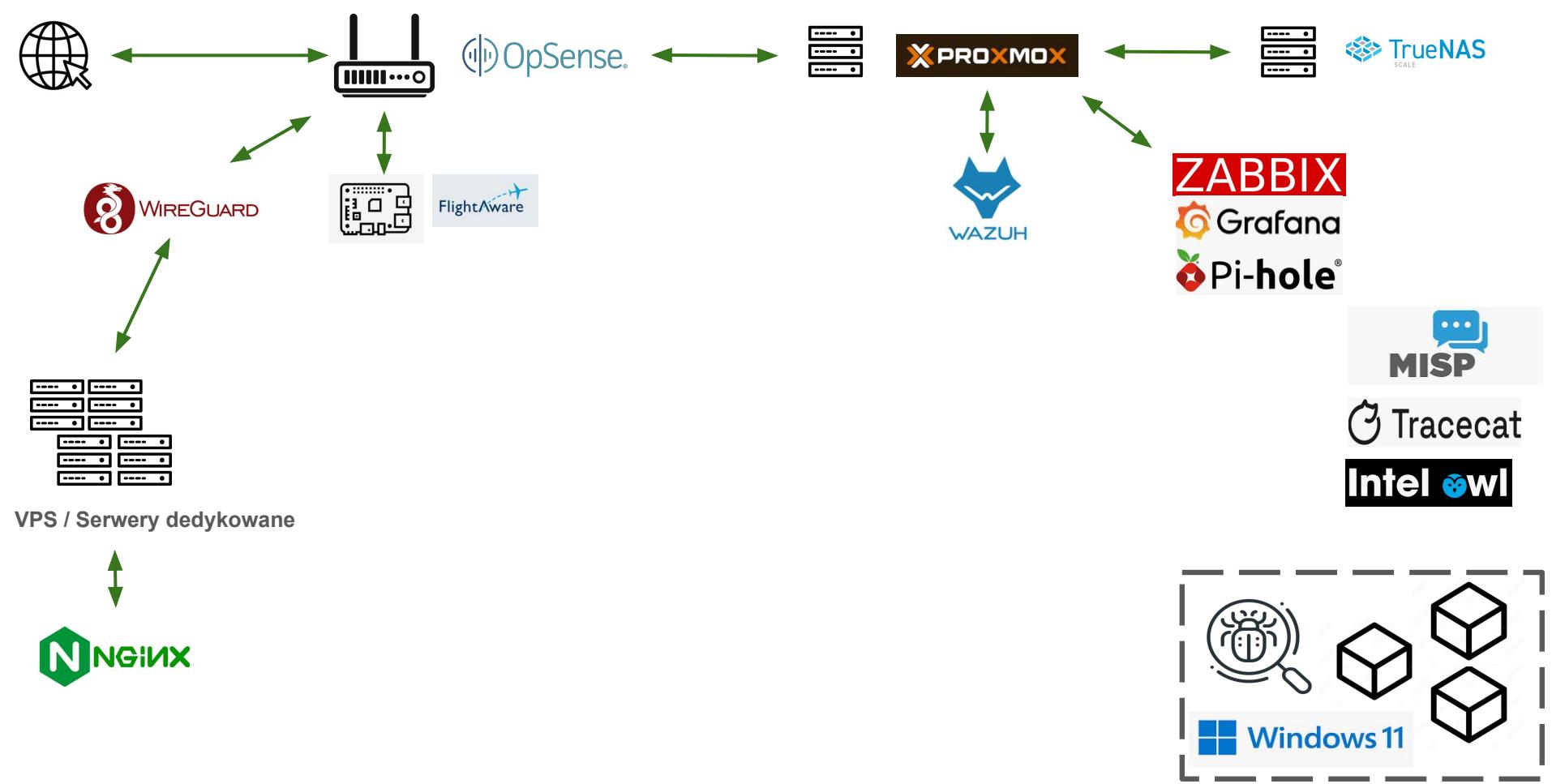
```
1  {
2    "report": [ ],
3    "id": "3716563",
4    "url": "https://wp2.unairdedemo.com",
5    "host": "wp2.unairdedemo.com",
6    "tags": [ ],
7    "larted": "true",
8    "threat": "malware_download",
9    "payloads": [ ],
10   "reporter": "threatquery",
11   "blacklists": { },
12   "date_added": "2025-11-25 15:02:08 UTC",
13   "url_status": "offline",
14   "last_online": "2025-11-25 17:XX:XX UTC",
15   "query_status": "ok",
16   "urlhaus_reference": "https://urlhaus.abuse.ch/url/3716563/",
17   "takedown_time_seconds": "8300"
18 },
19 "data_model": { },
20 "errors": [ ],
21 "parameters": { }
```

1		SUCCESS	Phishtank	0.59	10:28:25 PM - 10:28:26 PM (GMT+1)
2		SUCCESS	PhishingArmy	0.06	10:28:25 PM - 10:28:25 PM (GMT+1)

# Ścieżki rozwoju homelaba

- **Sandbox i analiza malware'u**
  - Przydatna do bezpiecznej analizy podejrzanych/złośliwych danych
  - Praktyczna nauka izolacji w sieci
  - I przygotowania systemów/usług do separacji
  - Lab na KVM: <https://c3rb3ru5d3d53c.github.io/2022/06/kvm-malware-lab/>
  - Lab na Hyper-V (@Lasq): [https://www.youtube.com/watch?v=fLJifLf\\_fRE](https://www.youtube.com/watch?v=fLJifLf_fRE)
- **Suricata jako IDS na Raspberry-Pi**
- **Cloudflare Tunnel / Zero Tier / Tailscale**
- **Honeypoty**
- **Lokalne LLMy**





# Gdzie szukać wiedzy?

- **reddit/r/homelab** - największa społeczność homelabowa
  - Jest też serwer na Discordzie
- Mnóstwo rozwiązań i inspiracji
  - [github.com/aboutsecurity/blueteam\\_homelabs](https://github.com/aboutsecurity/blueteam_homelabs)
  - <https://github.com/Uttamydv/Cybersecurity-Homelab-and-Penetration-Testing-Project>
  - <https://ergaster.org/posts/2025/08/04-overengineering-homelab/>
  - HomeLab Services Tour 2024 ([youtube.com/watch?v=MpaAu3HVDYE](https://youtube.com/watch?v=MpaAu3HVDYE))
- Youtube
  - @JeffGeerling
  - @HardwareHaven
  - @jeffsponaugle6339 (Jeff's CTO Laboratory)



**Pytania?  
Serdecznie dziękuję!  
Zapraszam do oceny w Eventory!**

X: [x.com/adwersarz\\_pl](https://x.com/adwersarz_pl)

Mastodon: [infosec.exchange/@adwersarz\\_pl](https://infosec.exchange/@adwersarz_pl)

Kontakt: [redakcja@adwersarz.pl](mailto:redakcja@adwersarz.pl)