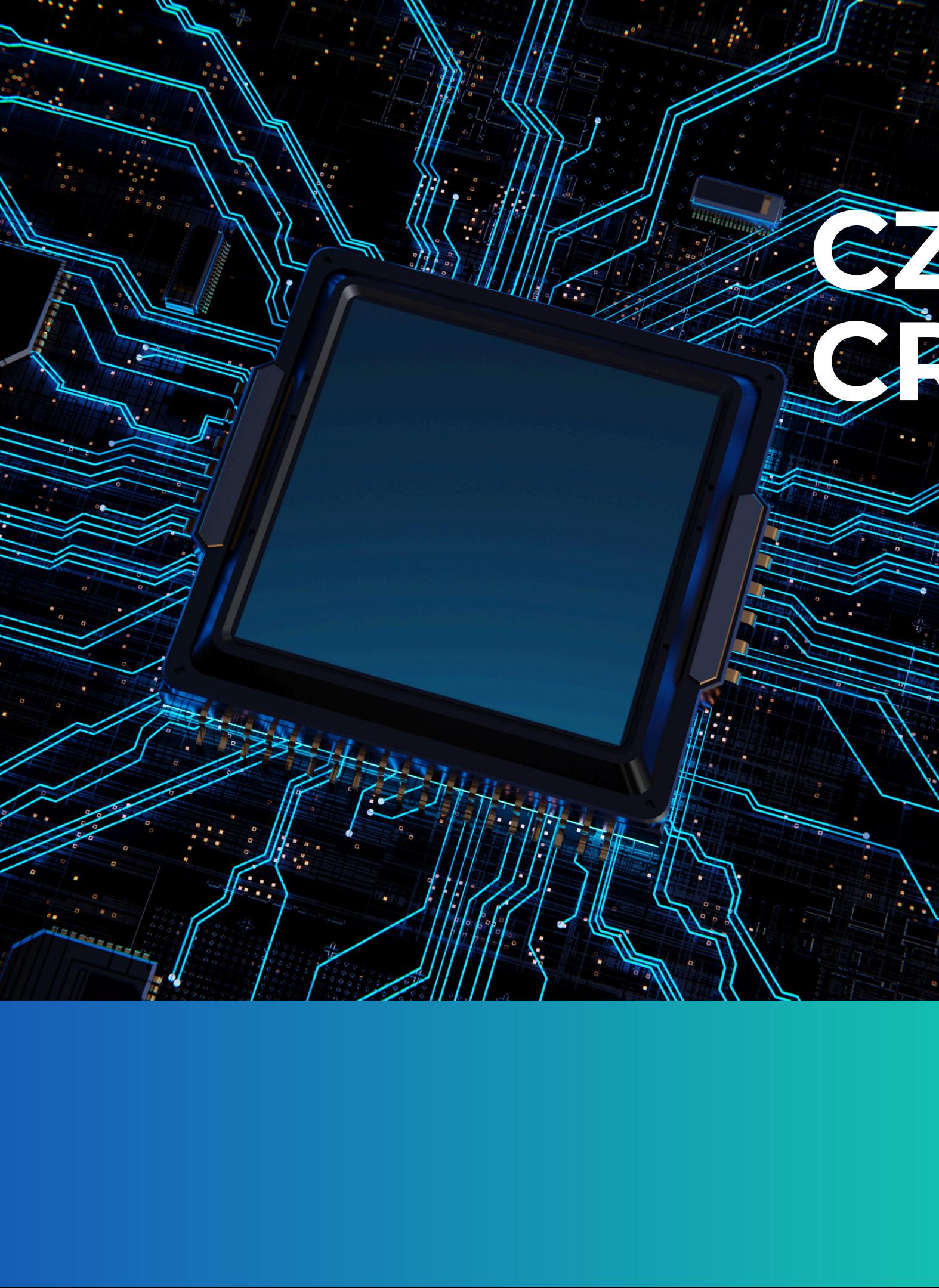


CrowdSec

Efektywna Ochrona Cybernetyczna





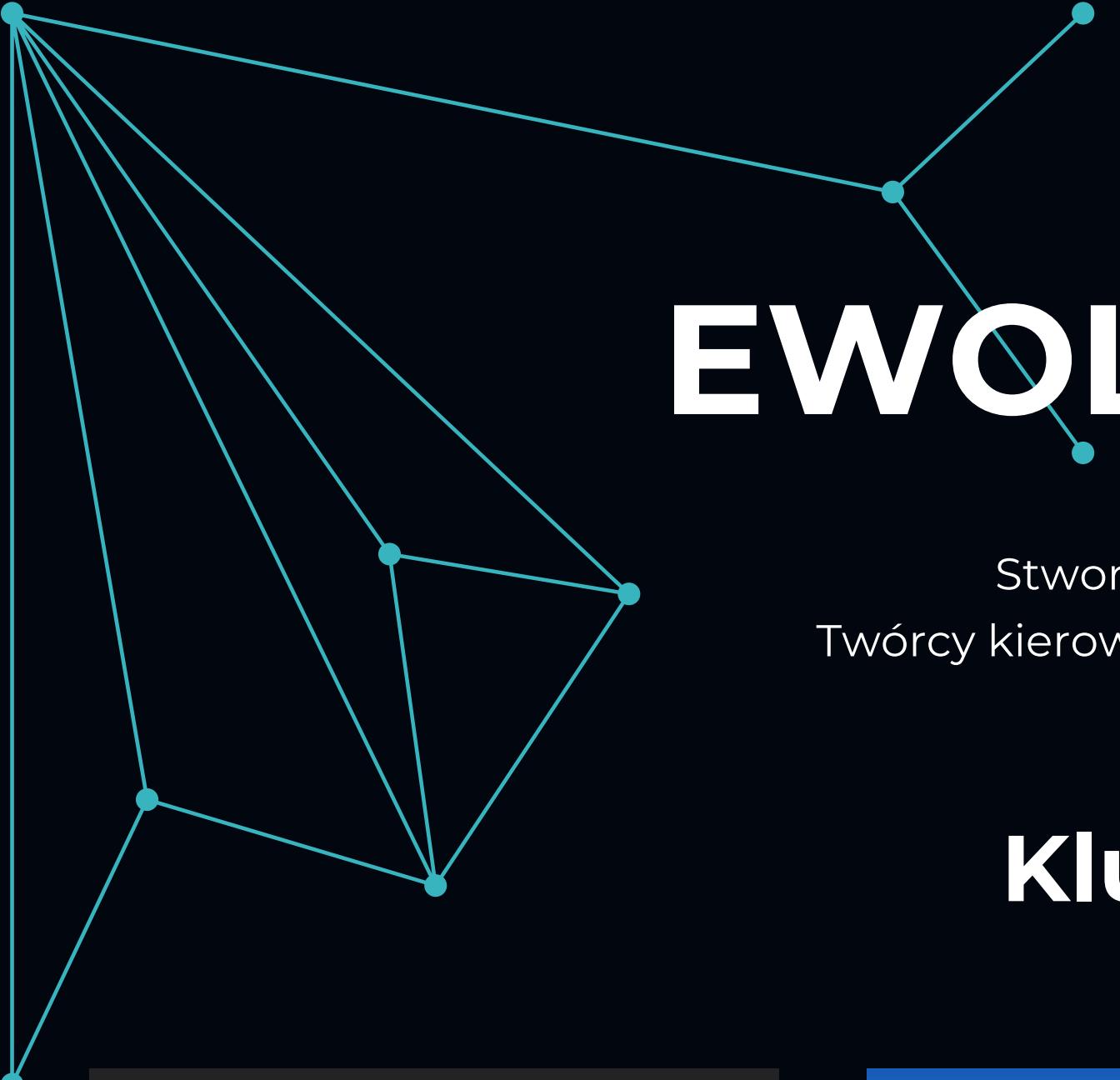
CZYM JEST CROWDSEC?

Definicja: Open-source'owe narzędzie do wykrywania i reagowania na cyberzagrożenia w czasie rzeczywistym

Główne działanie: System wykrywania i zapobiegania atakom (IPS/IDS) wykorzystujący crowdsourcing.

Cel: Blokowanie złośliwego ruchu (skanowanie portów, ataki brute-force, exploitowanie podatności, próby DDoS).

Przewaga: Lekka alternatywa dla Fail2Ban, z szerszą funkcjonalnością i skalowalnością.



EWOLUCJA CROWDSEC

Stworzony w **2019** roku przez francuskich specjalistów.
Twórcy kierowali się **ideą zbiorowej obrony** – im więcej użytkowników
współpracuje, tym skuteczniejsza ochrona.

Kluczowe etapy rozwoju

2020

Pierwsza publiczna wersja
(v1.0) i CrowdSec
Community Blocklist.

2022

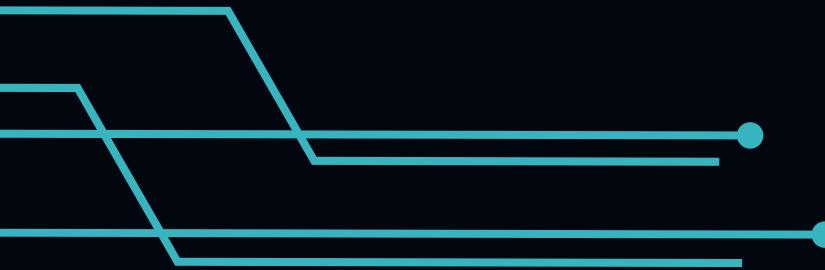
Uruchomienie CrowdSec
Console - centralnej
platformy zarządzania.

2023

Wsparcie dla architektury
multi-machine, integracja z
Kubernetes, Cloudflare, API
REST.

2024

Rozszerzenie integracji
chmurowych (AWS, Azure,
Google Cloud).



WARIANTY I ZASIĘG GLOBALNY

WARIANTY PROGRAMU I SPOŁECZNOŚĆ



CROWDSEC AGENT

Darmowy, open-source'owy komponent do lokalnej analizy logów i blokad



CROWDSEC CONSOLE

Centralne zarządzanie, dostępne w wersji SaaS (dla społeczności) i Enterprise.



CROWDSEC ENTERPRISE

Funkcje korporacyjne (centralne zarządzanie agentami, rozszerzone API, dedykowane wsparcie)

GLOBALNY ZASIĘG

STATYSTYKI TWÓRCÓW

100K+

Aktywnych użytkowników

190+

Krajów na świecie

15M

Sygnałów/dzień o
agresywnych IP



JAK DZIAŁA CROWDSEC?

KLUCZOWE KOMPONENTY

Działanie

Inteligentny filtr ruchu sieciowego wykorzystujący analizę sygnaturową i behawioralną

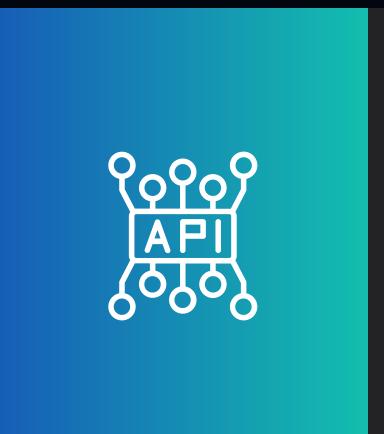
Skalowalność

Od pojedynczego serwera do rozproszonych środowisk chmurowych.



Agent

Lekki proces analizujący logi systemowe i aplikacyjne.



Local API

Zarządza decyzjami o blokadach na poziomie lokalnym.



Bouncers

Moduły wykonawcze implementujące decyzje o blokadach.

BOUNCERY

PODEJMOWANIE DECYZJI O BLOKADACH

Rola bouncerów

Bouncery odpowiadają za realizację decyzji podjęte przez agenta (np. blokują niepożądany ruch)



Sieciowe

Integracja z zaporami
(iptables, nftables, pf).



Aplikacyjne

Moduły w serwerach HTTP
(np. Nginx, Apache).



Chmurowe

Komunikacja z API usług chmurowych (np.
Cloudflare)



API Bouncery

Integracja z własnymi
aplikacjami przez REST
API.



SILNIK DECYZYJNY CROWDSEC



WSZECHSTRONNA INTEGRACJA CROWDSEC

Systemy operacyjne: Linux (Ubuntu, Debian, CentOS, Fedora, RHEL, Alpine)

Zapory sieciowe: iptables, nftables, PF, firewalld.

Serwery WWW: Nginx, Apache, Traefik.

Środowiska chmurowe: AWS WAF, Cloudflare, Azure Firewall, Google Cloud.

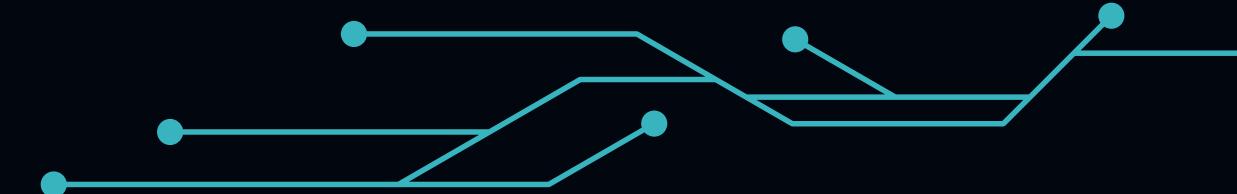
Konteneryzacja: Docker, Kubernetes.

Logowanie i monitorowanie: Syslog, Prometheus, Grafana, ELK Stack, Splunk, Graylog

API REST: Ułatwia integrację z DevOps i SIEM

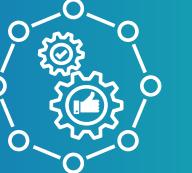


KLUCZOWE FUNKCJONALNOŚCI



Analiza logów i wykrywanie zagrożeń:

Podstawa działania, identyfikacja ataków brute-force, skanowania portów, SQL Injection.



Mechанизm społecznościowego Threat Intelligence:

Wyróżnik CrowdSec, dzielenie się informacjami o złośliwych IP, szybka reakcja na nowe zagrożenia, ochrona przed zero-day.



Automatyczne blokowanie zagrożeń (Bouncers):

Dynamiczne blokowanie atakujących IP na różnych poziomach (firewall, serwery WWW, usługi chmurowe), natychmiastowa reakcja bez interwencji człowieka.



PODSUMOWANIE

Kluczowe zalety CrowdSec

- Zaawansowane wykrywanie zagrożeń.
- Siła społeczności (Threat Intelligence)
- Automatyczne i elastyczne reagowanie (Bouncers).
- Modularność i szeroka integracja.
- Niski wpływ na wydajność.





DZIĘKUJEMY ZA UWAGĘ

PRZYGOTOWALI:

Przemysław Kałuziński

Michał kaczor

Jakub kuśmierczyk

