

<p style="text-align: center;">Politechnika Świętokrzyska Wydział Elektrotechniki, Automatyki i Informatyki</p>		
<p style="text-align: center;">Społeczne Aspekty Cyberbezpieczeństwa – Laboratorium</p>		
TEMAT: Opis programu CrowdSec		SKŁAD ZESPOŁU: <ul style="list-style-type: none"> • Przemysław Kałuziński (91271) • Jakub Kuśmierczyk (97504) • Michał Kaczor (91268)
DATA: 15.01.2025	GRUPA: 1IZ22B	

2

1. Spis treści

1.	Spis treści.....	2
2.	Wstęp	3
3.	Historia programu	3
4.	Warianty i wersje programu	4
5.	Architektura programu	5
6.	Identyfikacja i reagowanie na zagrożenia.....	7
7.	Bezpieczeństwo i prywatność.....	8
8.	Integracja i współpraca z innymi środowiskami	9
9.	Opis funkcjonalności	10
9.1.	Wybrane najważniejsze funkcjonalności	16
10.	Automatyzacja działania	17
11.	Krótką instrukcja obsługi.....	18
11.1.	Instalacja CrowdSec	18
11.2.	Wstępna konfiguracja CrowdSec	18
11.3.	Testowanie działania.....	19
12.	Opinie użytkowników	21
13.	Podsumowanie.....	22
14.	Bibliografia	22

3

2. Wstęp

CrowdSec to zaawansowane, open-source'owe narzędzie do wykrywania i reagowania na cyberzagrożenia w czasie rzeczywistym. Działa na zasadzie **systemu wykrywania i zapobiegania atakom (IPS/IDS)** wykorzystującego crowdsourcing, co oznacza, że zbiera dane o zagrożeniach od wielu użytkowników na całym świecie, aby zapewnić lepszą ochronę.

Głównym celem CrowdSec jest **blokowanie złośliwego ruchu**, takiego jak skanowanie portów, ataki brute-force, exploitowanie podatności czy próby DDoS, zanim dotrą one do chronionych systemów. Program działa jako **lekka alternatywa dla narzędzi takich jak Fail2Ban** (które działają głównie lokalnie), ale z szerszą funkcjonalnością, skalowalnością i możliwością współpracy w społeczności

3. Historia programu

CrowdSec został stworzony w 2019 roku przez francuskich specjalistów ds. cyberbezpieczeństwa, którzy dostrzegli potrzebę bardziej skalowalnego i społecznościowego podejścia do wykrywania zagrożeń w porównaniu do tradycyjnych rozwiązań, takich jak Fail2Ban. Inspiracją dla projektu była idea zbiorowej obrony – im więcej użytkowników współpracuje, tym skuteczniejsza staje się ochrona przed atakami.

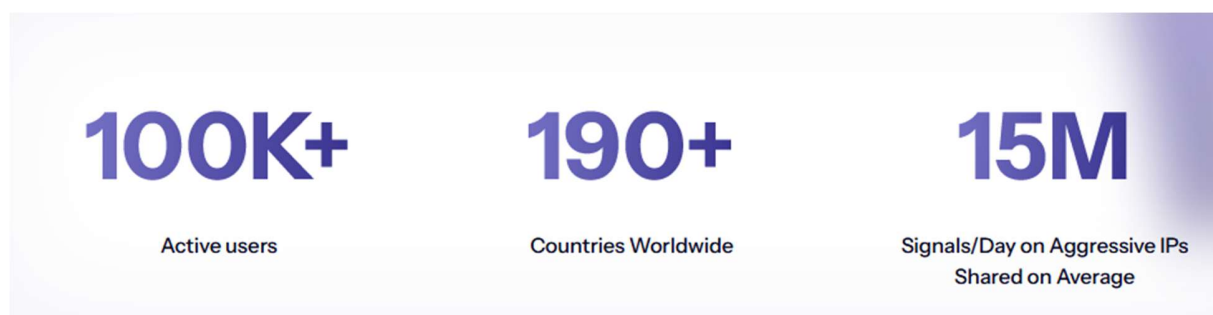
Pierwsza publiczna wersja programu (v1.0) została wydana w 2020 roku i szybko zyskała popularność wśród administratorów systemów oraz entuzjastów bezpieczeństwa IT, oferując rozbudowane możliwości parsowania logów, automatycznej reakcji na zagrożenia oraz współdzielenia informacji o atakujących adresach IP w ramach tzw. **CrowdSec Community Blocklist**.

W kolejnych latach projekt dynamicznie się rozwijał:

- **2021 – Wersja 1.2** przyniosła wsparcie dla wielu agentów w jednym środowisku, co znacznie ułatwiło wdrażanie CrowdSec w środowiskach z wieloma hostami.
- **2022 – Wprowadzenie Console:** uruchomiono *CrowdSec Console* – centralną platformę zarządzania, umożliwiającą wizualizację danych o atakach, kontrolę nad decyzjami blokującymi oraz konfigurację systemu w środowiskach produkcyjnych.
- **2023 – Wersja 1.4** wprowadziła wsparcie dla architektury *multi-machine*, pełniejszą integrację z popularnymi firewallami i narzędziami DevSecOps (m.in. Kubernetes, Cloudflare), a także rozbudowany system metryk i API REST.
- **2024 – Rozszerzenie integracji chmurowych:** CrowdSec zwiększył swoją obecność w środowiskach chmurowych, oferując oficjalne integracje z AWS, Azure i Google Cloud, co pozwoliło użytkownikom łatwiej chronić infrastrukturę rozproszoną.

Dzięki open-source'owemu modelowi rozwoju, wsparciu społeczności i przejrzystości działania, CrowdSec stale ewoluuje, dodając nowe funkcje, ulepszenia oraz lepsze mechanizmy detekcji i korelacji zdarzeń. W ciągu kilku lat projekt przekształcił się w globalną sieć cyberobrony, w której użytkownicy wzajemnie chronią się przed zagrożeniami, współdzieląc reputację adresów IP i informacje o nowych wektorach ataku.

W 2025 roku społeczność CrowdSec liczy już setki tysięcy węzłów na całym świecie, aktywnie zasilających wspólną bazę wiedzy o zagrożeniach – co czyni ten projekt jednym z najbardziej dynamicznie rozwijających się systemów prewencji typu open source.



Statystyki wykorzystania programu prezentowane przez twórców CrowdSec

4. Warianty i wersje programu

CrowdSec jest dostępny w kilku wariantach, dostosowanych do różnych potrzeb użytkowników – od niewielkich środowisk lokalnych po zaawansowane architektury korporacyjne i chmurowe. Podstawową wersją jest **CrowdSec Agent** – darmowy, open-source'owy komponent analizujący logi i podejmujący lokalne decyzje o blokadach. Wersja ta może działać samodzielnie lub jako element większego klastra. Dla użytkowników wymagających centralnego zarządzania i lepszej widoczności, dostępna jest **CrowdSec Console** – dostępna zarówno jako bezpłatna usługa SaaS (dla społeczności), jak i w wersji *Enterprise*, oferującej rozszerzoną analitykę, SLA oraz integrację z korporacyjną infrastrukturą.

Wersja **open-source CrowdSec** skupia się na zapewnieniu skutecznej ochrony dla pojedynczych hostów lub małych środowisk, oferując podstawowe funkcje wykrywania zagrożeń, współdzielenia danych o adresach IP oraz lokalnego reagowania poprzez *bouncery*. Z kolei **CrowdSec Enterprise** jest przeznaczony dla większych organizacji i środowisk produkcyjnych. Zapewnia funkcje klasy korporacyjnej, takie jak: centralne zarządzanie wieloma agentami, rozszerzone API, dedykowane wsparcie techniczne, zgodność z politykami bezpieczeństwa, monitoring stanu komponentów w czasie rzeczywistym, zaawansowane raportowanie oraz wsparcie dla integracji z systemami SIEM, DevSecOps i zarządzaniem tożsamością.

W praktyce, użytkownicy mogą rozpocząć od darmowej wersji open-source i w razie potrzeby łatwo przejść na wariant komercyjny, zachowując dotychczasową infrastrukturę oraz zasady działania. Dzięki takiej strategii CrowdSec zyskał dużą popularność zarówno wśród hobbystów i administratorów małych serwerów, jak i wśród dużych firm oraz dostawców usług chmurowych.



Duże firmy, które zaufały CrowdSec

5. Architektura programu

CrowdSec składa się z trzech głównych komponentów:

1. **Agent** - lekki proces analizujący logi systemowe i aplikacyjne
2. **Local API** - zarządza decyzjami o blokadach na poziomie lokalnym
3. **Bouncers** - moduły wykonawcze implementujące decyzje o blokadach

Program działa jako inteligentny filtr ruchu sieciowego, wykorzystujący zarówno analizę sygnaturową (opartą na znanych wzorcach ataków), jak i behawioralną (wykrywającą anomalie). Jego architektura pozwala na skalowanie od pojedynczego serwera do rozproszonych środowisk chmurowych.

CrowdSec agent odpowiada za analizę logów z różnych źródeł (np. SSH, serwerów WWW, aplikacji webowych) przy pomocy gotowych scenariuszy detekcji (**scenarios**) zapisanych w formacie YAML. Każdy scenariusz określa wzorzec zachowań typowych dla konkretnych zagrożeń, takich jak brute-force, port scanning czy podejrzane logowania. Po wykryciu zagrożenia agent generuje tzw. **decisions** – decyzje o zablokowaniu podejrzanego adresu IP.

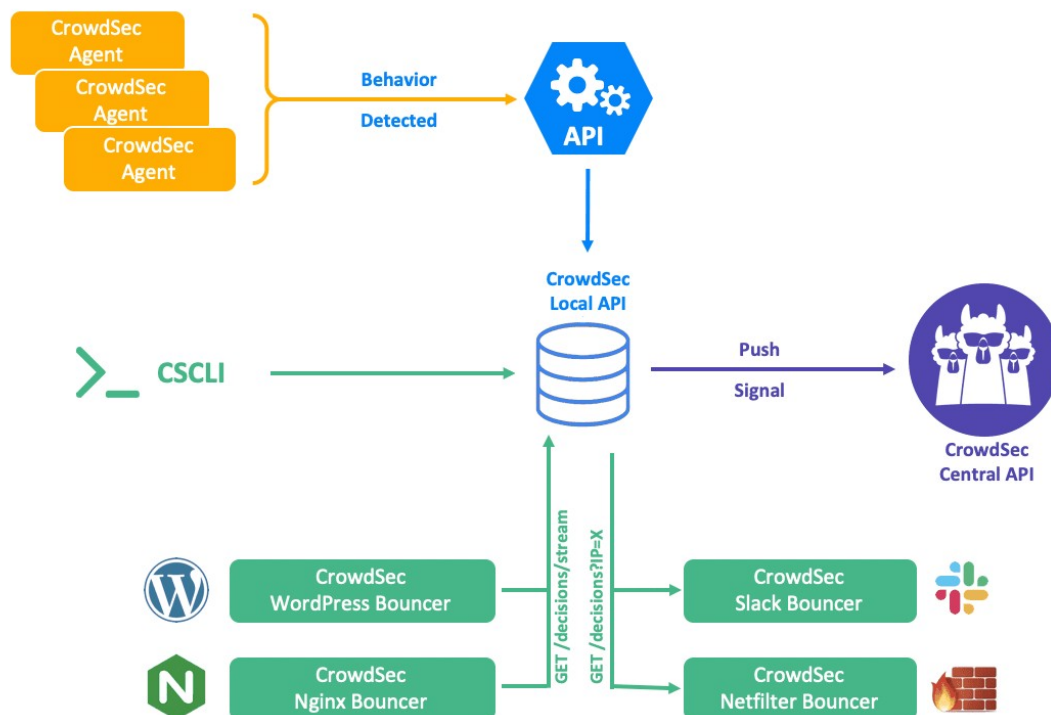
Za wdrożenie tych decyzji odpowiadają **bouncery**, które stanowią kluczowy element wykonawczy architektury CrowdSec — to one realizują decyzje podjęte przez agenta, np. blokując niepożądany ruch. Komunikacja między agentem a bouncerami odbywa się przez **Local API**, najczęściej wystawione jako lokalny serwer REST HTTP (domyślnie na porcie 8080) lub przez socket Unix. Agent publikuje decyzje w formacie JSON, a bouncery cyklicznie odpytują API w celu pobrania aktualnych decyzji.

Istnieje wiele typów bouncerów, dostosowanych do różnych warstw systemu:

- **Sieciowe bouncery**, np. crowdsec-firewall-bouncer, integrują się bezpośrednio z warstwą sieciową systemu operacyjnego, wykorzystując iptables, nftables lub pf (na BSD) do blokowania ruchu na poziomie pakietów.
- **Aplikacyjne bouncery**, jak crowdsec-nginx-bouncer, działają jako moduły w serwerach HTTP i umożliwiają filtrowanie ruchu przychodzącego do aplikacji webowych. Mogą np. zwracać kod HTTP 403 dla adresów IP znajdujących się na czarnej liście.
- **Chmurowe bouncery**, np. crowdsec-cloudflare-bouncer, komunikują się z zewnętrznymi API usług chmurowych (jak Cloudflare) i dynamicznie aktualizują reguły zapory (WAF) dla domen użytkownika.
- **API bouncery**, które integrują się z aplikacjami własnymi, mogą być zaimplementowane w dowolnym języku programowania dzięki udostępnionemu protokołowi REST i SDK (np. Python, Go, PHP).

Taka modularna budowa umożliwia łatwe dostosowanie mechanizmów ochronnych do konkretnej architektury systemu. Dodatkowo bouncery mogą działać niezależnie od siebie, umożliwiając jednoczesną ochronę na wielu poziomach.

CrowdSec umożliwia także współdzielenie anonimowych danych o zagrożeniach z **Community Threat Intelligence** (CTI). Użytkownicy mogą dobrowolnie przysyłać informacje o zidentyfikowanych adresach IP, które są agregowane, analizowane i redystrybuowane w postaci globalnych list zagrożeń (**blocklists**). Dzięki temu system działa nie tylko reaktywnie, ale też proaktywnie, wykorzystując zbiorową wiedzę do obrony przed nowymi wektorami ataku.



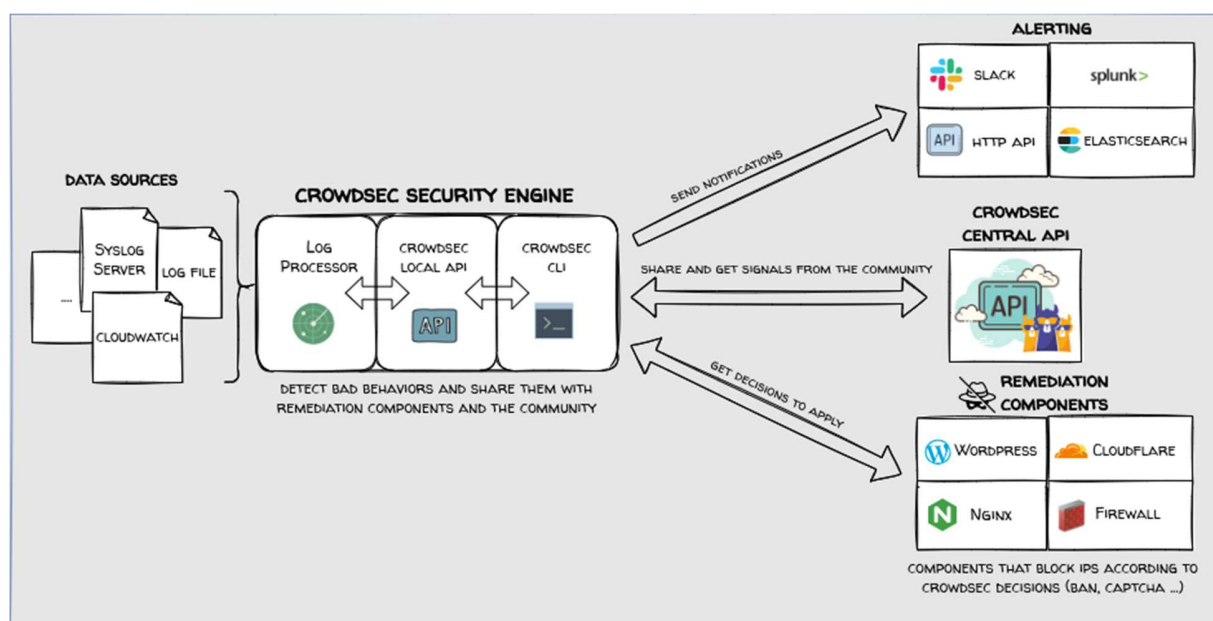
Architektura działania CrowdSec

6. Identyfikacja i reagowanie na zagrożenia

CrowdSec wykorzystuje zaawansowany mechanizm analizy logów oparty na **parserach** i **scenariuszach detekcji**, aby w czasie rzeczywistym identyfikować potencjalne zagrożenia. Podstawą działania systemu jest tzw. **silnik decyzyjny** (*Decision Engine*), który analizuje zachowania użytkowników i ruch sieciowy na podstawie wcześniej zdefiniowanych reguł. Logi pochodzące z systemów operacyjnych, serwerów aplikacyjnych, zapór sieciowych czy usług chmurowych są przetwarzane przez **agenta** CrowdSec, który za pomocą parserów dopasowuje dane do znanych **wzorców ataków**, takich jak brute-force, próby logowania SSH z wielu adresów, skanowanie portów, exploitowanie popularnych luk w aplikacjach (np. SQLi, RCE, LFI), a także nienaturalne częstotliwości zapytań HTTP wskazujące na potencjalny DDoS.

Wykryte incydenty są oceniane na podstawie tzw. scenariuszy (**scenarios**) – czyli reguł opisanych w języku YAML, które zawierają warunki i progi reakcji. Jeśli warunki są spełnione, silnik podejmuje decyzję o zagrożeniu i wydaje tzw. decyzję blokującą (**decision**), która jest następnie realizowana przez lokalnego **bouncera** (np. poprzez zablokowanie IP, przekierowanie ruchu, odrzucenie żądania). Każde podejrzane IP może być również zgłoszone do globalnej bazy **CrowdSec Community Blocklist**, gdzie podlega dalszej weryfikacji przez algorytmy reputacyjne, analizujące m.in. częstotliwość zgłoszeń, źródła, oraz korelację z innymi zdarzeniami w ekosystemie.

CrowdSec klasyfikuje zagrożenia według ich charakteru i intensywności, co pozwala różnicować reakcję – od tymczasowej blokady IP po trwałe odrzucenie ruchu. Dodatkowo, użytkownicy mają możliwość dostosowania poziomów czułości detekcji, edycji scenariuszy oraz ręcznego zatwierdzania lub odrzucania decyzji. Dzięki temu CrowdSec nie tylko skutecznie wykrywa i eliminuje znane ataki, ale też umożliwia adaptację do indywidualnych potrzeb zabezpieczanego środowiska. W połączeniu z mechanizmami uczenia zbiorowego i szybkiej dystrybucji informacji o nowych wektorach ataku, program zapewnia dynamiczną i proaktywną ochronę.



Silnik decyzyjny CrowdSec – podstawa działania programu

7. Bezpieczeństwo i prywatność

CrowdSec został zaprojektowany z myślą o zachowaniu równowagi pomiędzy efektywną ochroną a poszanowaniem prywatności użytkowników. Kluczową kwestią jest sposób przetwarzania i przesyłania danych telemetrycznych, jak również ochrona przed nadużyciami w rozproszonej sieci detekcyjnej.

Szyfrowanie i anonimizacja danych

Dane telemetryczne, które użytkownicy dobrowolnie udostępniają do bazy Threat Intelligence (CTI), są anonimizowane – zawierają jedynie adresy IP uznane za złośliwe, znacznik czasu, typ wykrycia oraz kraj pochodzenia. Informacje te są przesyłane za pomocą połączeń HTTPS z użyciem aktualnych protokołów TLS. Żadne dane osobowe ani logi źródłowe nie są udostępniane zewnętrznie bez zgody użytkownika.

Ochrona przed fałszywymi zgłoszeniami

Aby zapobiec nadużyciom i celowemu zgłaszaniu fałszywych zagrożeń (tzw. false positives), CrowdSec stosuje system reputacji i walidacji zgłoszeń. Informacje pochodzące od wielu agentów są korelowane – tylko adresy IP wskazywane przez wielu niezależnych uczestników społeczności trafiają na globalne listy zagrożeń. Dodatkowo, każde zgłoszenie musi być zgodne z wcześniej zdefiniowanym scenariuszem detekcyjnym, co minimalizuje ryzyko błędów wynikających z błędnej konfiguracji.

Potencjalne wektory ataku

Jak każdy system ochrony, CrowdSec może być celem ataku. Do potencjalnych wektorów należą m.in.:

- **Atak na Local API** – nieprawidłowo zabezpieczone API może umożliwić nieautoryzowany dostęp do decyzji o blokadzie.
- **Przejęcie bouncera** – atakujący mogą próbować modyfikować lub dezaktywować komponenty wykonawcze, by obejść blokadę.
- **Spoofing zgłoszeń** – próba masowego wysyłania fałszywych zgłoszeń do sieci CTI w celu zdyskredytowania legalnych adresów IP.

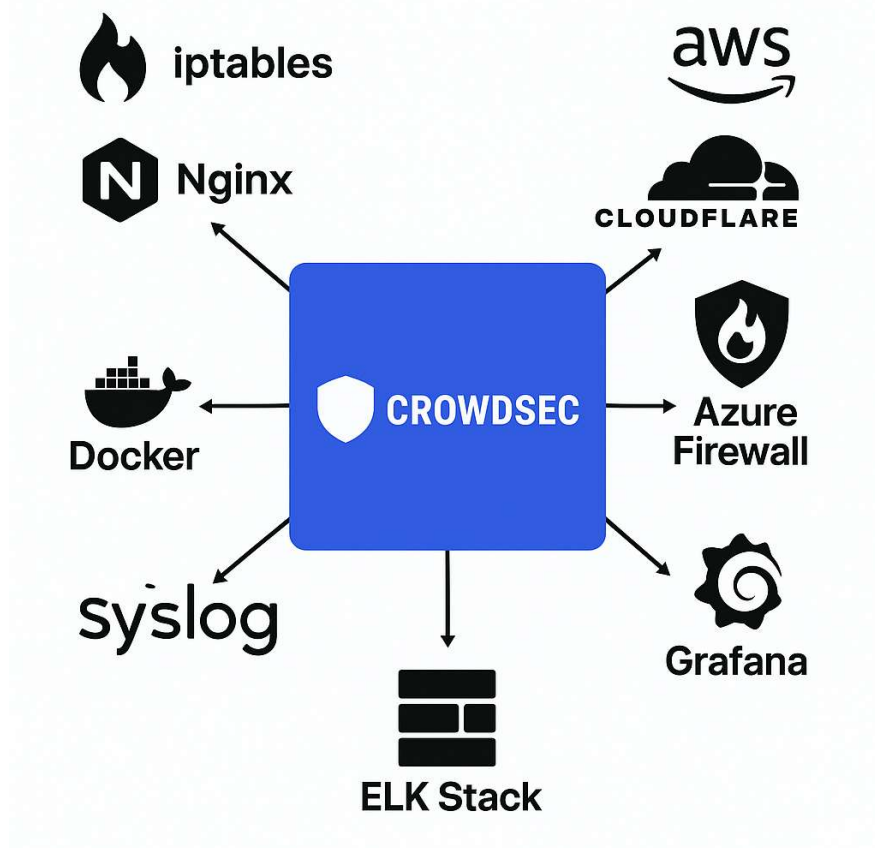
W odpowiedzi na te zagrożenia CrowdSec umożliwia konfigurację uwierzytelniania tokenowego, stosowanie lokalnych list wyjątków (*whitelist*), jak również korzystanie z mechanizmów kontroli integralności i logowania zdarzeń bezpieczeństwa.

8. Integracja i współpraca z innymi środowiskami

CrowdSec został zaprojektowany z myślą o elastycznej integracji z różnorodnymi środowiskami, co czyni go wszechstronnym narzędziem zarówno w klasycznych, jak i nowoczesnych architekturach IT. Program jest przede wszystkim dostępny na systemy **Linux** (w tym na popularne dystrybucje takie jak Ubuntu, Debian, CentOS, Fedora, RHEL czy Alpine), gdzie działa jako usługa analizująca logi i podejmująca działania obronne. Wspiera zarówno środowiska serwerowe, jak i lokalne maszyny developerskie. Dzięki modularnej budowie i systemowi *bouncerów*, może być z łatwością zintegrowany z popularnymi **zaporami sieciowymi** (np. iptables, nftables, PF, firewalld), **serwerami WWW** (takimi jak Nginx, Apache), a także z **usługami dostarczanyymi przez dostawców chmurowych**, m.in. AWS WAF, Cloudflare czy Azure Firewall.

CrowdSec oferuje również wsparcie dla **środowisk konteneryzowanych** (Docker) i **orkiestracji** (Kubernetes), umożliwiając ochronę mikroserwisów i infrastruktury typu cloud-native. Ponadto, integracja z **systemami logowania i monitorowania** – takimi jak Syslog, Prometheus, Grafana czy ELK Stack – pozwala na skuteczne śledzenie zagrożeń i ich wizualizację w czasie rzeczywistym.

CrowdSec udostępnia **REST API**, które ułatwia włączenie go w istniejące przepływy **DevOps** i **systemy SIEM** (np. Splunk, Graylog), umożliwiając automatyzację reakcji na incydenty oraz lepszą korelację danych z innymi źródłami informacji. Tak szeroki zakres kompatybilności sprawia, że CrowdSec może pełnić rolę centralnego komponentu ochrony w złożonych i zróżnicowanych środowiskach IT.



Przykładowe integracje programu CrowdSec w rozwiązaniach firm trzecich

9. Opis funkcjonalności

1. Analiza logów i wykrywanie zagrożeń

CrowdSec przetwarza logi generowane przez różne systemy (serwery WWW, serwery SSH, aplikacje, urządzenia sieciowe) i identyfikuje podejrzane aktywności, wykorzystując reguły (scenariusze) oparte na sygnaturach i analizie behawioralnej. Działa podobnie do SIEM (Security Information and Event Management), ale jest lżejszy i bardziej skoncentrowany na automatycznym reagowaniu.

Zastosowania:

- Monitorowanie ruchu na serwerach,
- Wykrywanie ataków brute-force na SSH,
- Analizowanie prób SQL Injection na stronach internetowych.

Przykład:

Jeśli system wykryje wielokrotne nieudane próby logowania do SSH z tego samego adresu IP, oznacza to potencjalny atak brute-force i może podjąć odpowiednie działania.

```
admin@Ubuntu-Server-24:~$ sudo cscli alerts list
```

ID	value	reason	country	as	decisions	created_at
37	Ip:192.168.143.132	crowdsecurity/ssh-bf			ban:1	2025-04-05 08:07:44.030809167 +0000 UTC

Przykładowe ostrzeżenia o ataku bruteforce na SSH zgłaszane przez CrowdSec

```
admin@Ubuntu-Server-24: /etc/crowdsec/scenarios × ssh-bf.yaml
GNU nano 7.2
# ssh bruteforce
type: leaky
name: crowdsecurity/ssh-bf
description: "Detect ssh bruteforce"
filter: "evt.Meta.log_type == 'ssh_failed-auth'"
leakspeed: "10s"
references:
- http://wikipedia.com/ssh-bf-is-bad
capacity: 5
groupby: evt.Meta.source_ip
blackhole: 1m
reprocess: true
labels:
  service: ssh
  confidence: 3
  spoofable: 0
  classification:
    - attack.T1110
  label: "SSH Bruteforce"
  behavior: "ssh:bruteforce"
remediation: true
---
# ssh user-enum
type: leaky
name: crowdsecurity/ssh-bf_user-enum
description: "Detect ssh user enum bruteforce"
filter: evt.Meta.log_type == 'ssh_failed-auth'
groupby: evt.Meta.source_ip
```

Fragment pliku konfiguracyjnego scenariusza YAML dla ataku bruteforce na SSH

2. Mechanizm społecznościowego Threat Intelligence

CrowdSec wykorzystuje model crowdsourcingowy, w którym użytkownicy raportują złośliwe adresy IP do centralnej bazy danych. Dzięki temu system jest stale aktualizowany o nowe zagrożenia, co zwiększa skuteczność ochrony.

Zastosowania:

- Automatyczna aktualizacja listy złośliwych adresów IP,
- Ochrona systemów bez konieczności ręcznego zarządzania blokadami.


Przykład:

Jeśli jeden użytkownik wykryje atak z konkretnego adresu IP, inni użytkownicy CrowdSec na całym świecie automatycznie otrzymają informację o tym zagrożeniu.

Zalety:

- ✓ Szybsza reakcja na nowe zagrożenia,
- ✓ Mniejsza liczba fałszywych alarmów (weryfikacja przez społeczność),
- ✓ Ochrona przed atakami zero-day, zanim pojawią się w oficjalnych bazach CVE.

```
admin@Ubuntu-Server-24:~$ sudo cscli collections list
```

COLLECTIONS					Your personal collection
					DATA
Name		Status	Version	Local Path	Browse data
crowdsecurity/apache2	✓	enabled	0.1	/etc/crowdsec/collections/apache2.yaml	
crowdsecurity/apiscp	✓	enabled	0.1	/etc/crowdsec/collections/apiscp.yaml	
crowdsecurity/base-http-scenarios	✓	enabled	1.0	/etc/crowdsec/collections/base-http-scenarios.yaml	
crowdsecurity/dovecot	✓	enabled	0.1	/etc/crowdsec/collections/dovecot.yaml	
crowdsecurity/haproxy	✓	enabled	0.1	/etc/crowdsec/collections/haproxy.yaml	
crowdsecurity/http-cve	✓	enabled	2.9	/etc/crowdsec/collections/http-cve.yaml	
crowdsecurity/http-dos	✓	enabled	0.2	/etc/crowdsec/collections/http-dos.yaml	
crowdsecurity/linux	✓	enabled	0.2	/etc/crowdsec/collections/linux.yaml	
crowdsecurity/mysql	✓	enabled	0.1	/etc/crowdsec/collections/mysql.yaml	
crowdsecurity/nextcloud	✓	enabled	0.3	/etc/crowdsec/collections/nextcloud.yaml	
crowdsecurity/nginx	✓	enabled	0.2	/etc/crowdsec/collections/nginx.yaml	
crowdsecurity/pgsql	✓	enabled	0.1	/etc/crowdsec/collections/pgsql.yaml	
crowdsecurity/postfix	✓	enabled	0.4	/etc/crowdsec/collections/postfix.yaml	
crowdsecurity/sshd	✓	enabled	0.5	/etc/crowdsec/collections/sshd.yaml	
crowdsecurity/vsftpd	✓	enabled	0.1	/etc/crowdsec/collections/vsftpd.yaml	

Przykładowe kolekcje z publicznej bazy „crowdsecurity”

3. Automatyczne blokowanie zagrożeń (Bouncers)

Bouncers to moduły odpowiedzialne za egzekwowanie decyzji CrowdSec poprzez blokowanie zagrożeń. W zależności od infrastruktury mogą one działać na różnych poziomach zabezpieczeń.

Dostępne Bouncers:

Typ	Opis	Przykłady zastosowań
Firewall (iptables/nftables)	Blokowanie IP na poziomie sieci	Ochrona przed atakami DDoS
Cloudflare Bouncer	Dodawanie IP do czarnej listy w Cloudflare	Zabezpieczenie stron WWW przed botami
Nginx/Apache Bouncer	Blokowanie ruchu na poziomie serwera WWW	Ochrona przed brute-force i SQL Injection
CSFirewall (dedykowany firewall CrowdSec)	Zaawansowane filtrowanie ruchu	Kompleksowa ochrona serwerów

Zastosowania:

- Po wykryciu skanowania portów, CrowdSec może zablokować ruch z danego IP za pomocą iptables/nftables,
- W przypadku ataku botnetu na stronę internetową, moduł Cloudflare Bouncer może automatycznie dodać IP atakujących do czarnej listy Cloudflare,
- Możliwość wysyłania powiadomień o zagrożeniach do administratora poprzez e-mail lub Slack.

```
admin@Ubuntu-Server-24:~$ sudo cscli bouncers list
```

Name	IP Address	Valid	Last API pull	Type	Version	Auth Type
FirewallBouncer-gX0p0qzK6mFzC8yoyF9mgxLdzzB8DqgD	127.0.0.1	✓	2025-05-08T16:11:28Z	crowdsec-firewall-bouncer	2.1.0	api-key
crowdsec-nginx-bouncer-1746720435		✓		crowdsec-nginx-bouncer	1.0.0	api-key

Przykładowa lista zainstalowanych bouncerów

```
admin@Ubuntu-Server-24:~$ sudo cscli decisions list
```

ID	Source	Scope:Value	Reason	Action	Country	AS	Events	expiration	Alert ID
543394	crowdsec	Ip:192.168.0.177	crowdsecurity/ssh-bf	ban			6	3h59m59s	63

24 duplicated entries skipped

Lista decyzji podjętych przez bouncery

4. Modularność i integracja z innymi systemami

CrowdSec może zostać wdrożony w różnych środowiskach i integrować się z popularnymi technologiami używanymi w administracji systemami i DevOps.

Środowisko	Możliwości integracji
Serwery Linux	Debian, Ubuntu, CentOS, RHEL
Kontenery	Docker, Kubernetes, Podman
Chmura	AWS, Azure, Google Cloud
Web Serwery	Nginx, Apache, Traefik
SIEM & Logowanie	Splunk, ELK Stack, Grafana, Prometheus

Zastosowania:

- Wdrożenie CrowdSec na serwerze VPS do ochrony przed skanowaniem portów,
- Integracja z Kubernetes do monitorowania i blokowania ataków na mikrousługi,
- Współpraca z Cloudflare w celu blokowania botów na stronach internetowych.

5. Niski wpływ na wydajność systemu

CrowdSec został zaprojektowany w taki sposób, aby działać wydajnie i nie obciążać systemu, w przeciwieństwie do klasycznych systemów IPS.

Zastosowania:

- Zabezpieczenie dużych środowisk produkcyjnych,
- Ochrona systemów IoT i aplikacji chmurowych.

Przykład:

Serwer obsługujący setki połączeń na sekundę nie odczuje znaczącego spadku wydajności, ponieważ analiza logów odbywa się w sposób zoptymalizowany.

```
adnln@Ubuntu-Server-24:~$ ps aux | grep crowdsec
root      2897   4.3   0.3 2042624 12492 ?        Ssl  17:07   3:02 /usr/bin/crowdsec-firewall-
root      8743   1.7   3.9 2858480 156912 ?        Ssl  17:16   1:05 /usr/bin/crowdsec -c /etc/c
admin    19032   0.0   0.0   6544   2304 pts/0    S+   18:17   0:00 grep --color=auto crowdsec
```

Wykorzystanie zasobów maszyny przez procesy CrowdSec (kolumny 3 i 4 to CPU i RAM)

6. Obsługa polityk bezpieczeństwa

CrowdSec umożliwia dostosowanie reakcji na zagrożenia poprzez definiowanie polityk bezpieczeństwa.

Zastosowania:

- Personalizacja reguł dla różnych typów ruchu (np. ostrzeżenie zamiast natychmiastowej blokady).

Przykład:

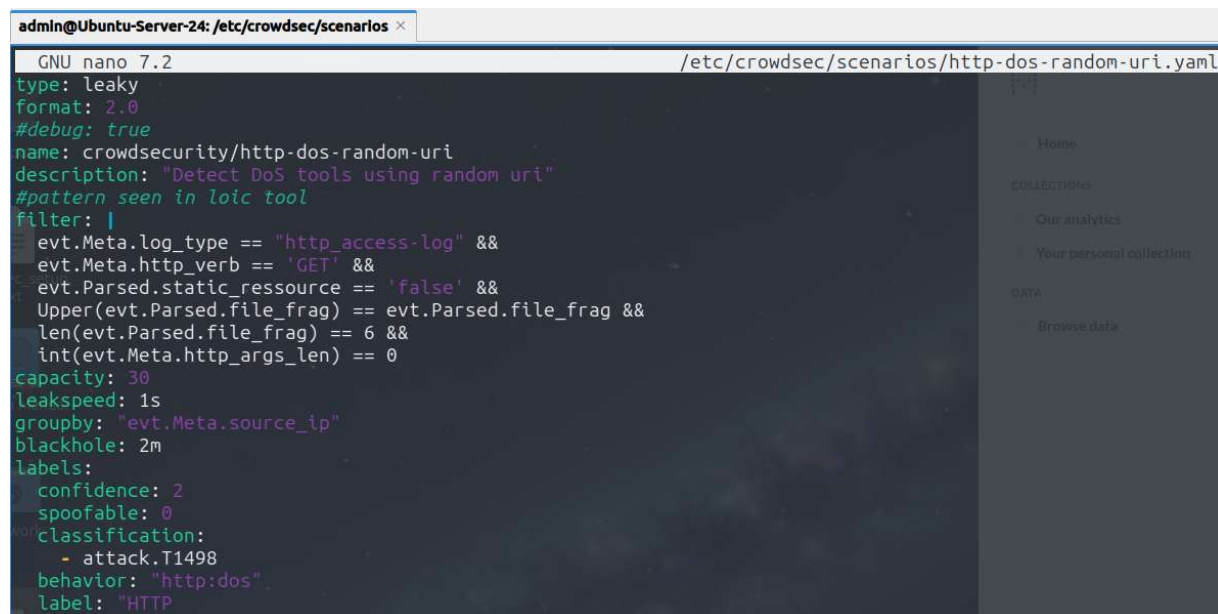
Administrator może skonfigurować CrowdSec tak, aby podejrzane adresy IP najpierw były oznaczane jako "potencjalnie szkodliwe" i dopiero po kolejnych wykrytych anomaliach – blokowane.

7. Analiza behawioralna (Behavioral Detection)

CrowdSec nie opiera się wyłącznie na statycznych regułach, lecz wykorzystuje także analizę behawioralną i uczenie maszynowe.

Zastosowania:

- Wykrywanie botów analizujących stronę poprzez nietypowe odstępy czasowe między zadaniami,
- Identyfikacja anomalii w ruchu HTTP (np. nagły wzrost żądań do jednego endpointu może wskazywać na atak DDoS),
- Detekcja ataków na API (np. wielokrotne próby logowania za pomocą różnych danych w żądaniach POST /login).



```
admin@Ubuntu-Server-24: /etc/crowdsec/scenarios x
GNU nano 7.2 /etc/crowdsec/scenarios/http-dos-random-uri.yaml
type: leaky
format: 2.0
#debug: true
name: crowdsecurity/http-dos-random-uri
description: "Detect DoS tools using random uri"
#pattern seen in loic tool
filter: |
  evt.Meta.log_type == "http_access-log" &&
  evt.Meta.http_verb == 'GET' &&
  evt.Parsed.static_resource == 'false' &&
  Upper(evt.Parsed.file_frag) == evt.Parsed.file_frag &&
  len(evt.Parsed.file_frag) == 6 &&
  int(evt.Meta.http_args_len) == 0
capacity: 30
leakspeed: 1s
groupby: "evt.Meta.source_ip"
blackhole: 2m
labels:
  confidence: 2
  spoofable: 0
  classification:
    - attack.T1498
  behavior: "http:dos"
  label: "HTTP"
```

Fragment scenariusza behawioralnego

8. Tryb nauki i testowania (Loki Mode)

Przed pełnym wdrożeniem, CrowdSec może działać w trybie monitorowania (Loki Mode), aby uniknąć przypadkowych blokad.

Funkcje trybu nauki:

- **Symulacja blokad** – system pokazuje, co zostałyby zablokowane, ale nie podejmuje faktycznych działań,
- **Raporty statystyczne** – administrator może sprawdzić, ile ataków wykryto, ale nie zablokowano,
- **Dostosowywanie czułości** – możliwość regulowania poziomu agresywności reguł.

9. Monitorowanie i raportowanie

CrowdSec oferuje zaawansowane narzędzia do wizualizacji danych, umożliwiające administratorom śledzenie zagrożeń w czasie rzeczywistym.

Funkcje:

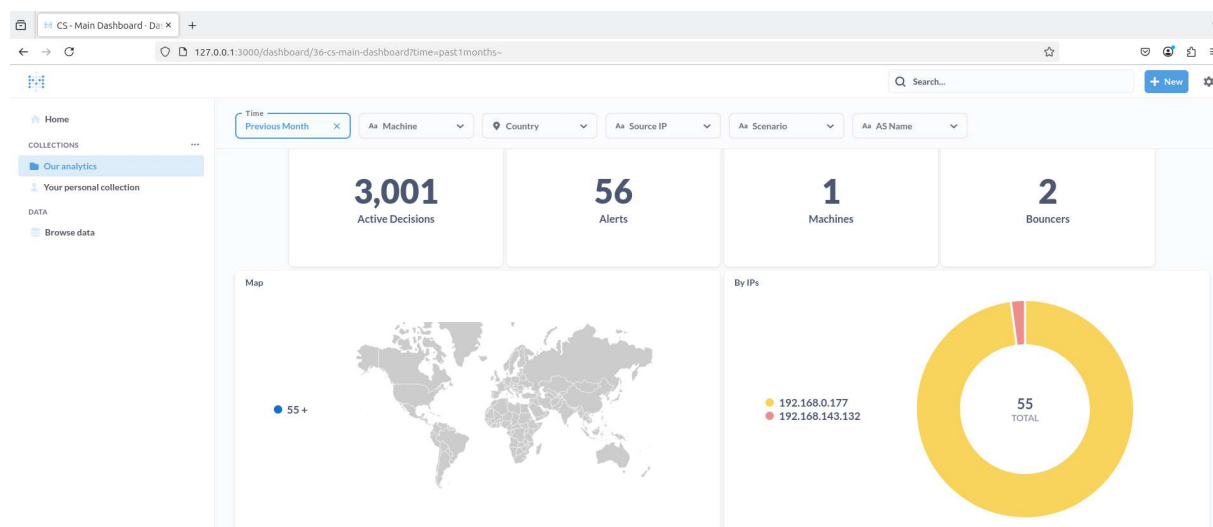
- ✓ Interfejs Metabase – graficzny panel do przeglądania zablokowanych adresów IP,
- ✓ REST API – integracja z innymi systemami i automatyzacja działań,
- ✓ Możliwość ręcznego dodawania wyjątków – administrator może zezwolić na dostęp określonym adresom IP,
- ✓ Eksport danych do SIEM – kompatybilność ze Splunk, ELK Stack i innymi narzędziami.

Zastosowania:

- Analiza ataków, wykrywanie trendów, raportowanie do zespołów ds. bezpieczeństwa.

Przykład:

Panel monitorowania pokazuje, ile adresów IP zostało zablokowanych w danym okresie oraz jakie były najczęstsze typy ataków.



Graficzny interfejs CrowdSec zawierający wszystkie dane dotyczące działania CrowdSec

ID	Created At	Updated At	Until	Scenario	Type	Start IP	End IP	Scope	Start Suffix	End Suffix	Value	IP Size	Origin	Simulated
540369	2025-5-8, 15:28:40	2025-5-8, 15:28:40	April 5, 2025, 12:07 PM	crowdsecurity/ssh-bf	ban	-9223372033622503000	-9223372033622503000	ip	-9223372033622503000	-9223372033622503000	192.168.143.132	4	crowdsec	0
540370	2025-5-8, 15:36:24	2025-5-8, 15:36:24	May 15, 2025, 2:36 PM	httpbruteforce	ban	-9223372033736547000	-9223372033736547000	ip	-9223372033736547000	-9223372033736547000	185.220.101.0	4	CAPi	0
540371	2025-5-8, 15:36:24	2025-5-8, 15:36:24	May 15, 2025, 12:36 PM	httpbruteforce	ban	-92233720335835808000	-92233720335835808000	ip	-92233720335835808000	-92233720335835808000	60.188.57.0	4	CAPi	0
540372	2025-5-8, 15:36:24	2025-5-8, 15:36:24	May 13, 2025, 6:36 PM	httpbruteforce	ban	-92233720335415325000	-92233720335415325000	ip	-92233720335415325000	-92233720335415325000	85.204.70.100	4	CAPi	0
540373	2025-5-8, 15:36:24	2025-5-8, 15:36:24	May 15, 2025, 2:36 PM	httpbruteforce	ban	-9223372033736547000	-9223372033736547000	ip	-9223372033736547000	-9223372033736547000	185.220.101.100	4	CAPi	0
540374	2025-5-8, 15:36:24	2025-5-8, 15:36:24	May 15, 2025, 11:36 AM	httpbruteforce	ban	-9223372034119738000	-9223372034119738000	ip	-9223372034119738000	-9223372034119738000	163.5.91.100	4	CAPi	0
540375	2025-5-8, 15:36:24	2025-5-8, 15:36:24	May 15, 2025, 10:36 AM	httpbruteforce	ban	-9223372034544236000	-9223372034544236000	ip	-9223372034544236000	-9223372034544236000	137.184.13.100	4	CAPi	0
540376	2025-5-8, 15:36:24	2025-5-8, 15:36:24	May 15, 2025, 3:36 PM	httpbruteforce	ban	-9223372035095533000	-9223372035095533000	ip	-9223372035095533000	-9223372035095533000	104.219.236.100	4	CAPi	0
540377	2025-5-8, 15:36:24	2025-5-8, 15:36:24	May 15, 2025, 1:36 PM	httpbruteforce	ban	-9223372036029338000	-9223372036029338000	ip	-9223372036029338000	-9223372036029338000	49.51.47.100	4	CAPi	0
540378	2025-5-8, 15:36:24	2025-5-8, 15:36:24	May 15, 2025, 1:36 PM	httpbruteforce	ban	-9223372034759736000	-9223372034759736000	ip	-9223372034759736000	-9223372034759736000	124.223.197.100	4	CAPi	0
540379	2025-5-8, 15:36:24	2025-5-8, 15:36:24	May 13, 2025, 12:36 PM	httpbruteforce	ban	-9223372036459858000	-9223372036459858000	ip	-9223372036459858000	-9223372036459858000	23.137.248.100	4	CAPi	0
540380	2025-5-8, 15:36:24	2025-5-8, 15:36:24	May 15, 2025, 2:36 PM	httpbruteforce	ban	-9223372033604361000	-9223372033604361000	ip	-9223372033604361000	-9223372033604361000	193.189.100.200	4	CAPi	0
540381	2025-5-8, 15:36:24	2025-5-8, 15:36:24	May 15, 2025, 1:36 PM	httpbruteforce	ban	-9223372034348250000	-9223372034348250000	ip	-9223372034348250000	-9223372034348250000	149.102.141.200	4	CAPi	0
540382	2025-5-8, 15:36:24	2025-5-8, 15:36:24	May 14, 2025, 9:36 PM	httpbruteforce	ban	-9223372034120660000	-9223372034120660000	ip	-9223372034120660000	-9223372034120660000	162.247.74.200	4	CAPi	0
540383	2025-5-8, 15:36:24	2025-5-8, 15:36:24	May 15, 2025, 2:36 PM	httpbruteforce	ban	-9223372033630768000	-9223372033630768000	ip	-9223372033630768000	-9223372033630768000	192.42.156.200	4	CAPi	0
540384	2025-5-8, 15:36:24	2025-5-8, 15:36:24	May 15, 2025, 3:36 PM	httpbruteforce	ban	-9223372033214889000	-9223372033214889000	ip	-9223372033214889000	-9223372033214889000	216.244.66.200	4	CAPi	0

Lista wszystkich decyzji bouncerów zaprezentowana graficznie (uwzględniająca też te z bazy crowdsecurity)

9.1. Wybrane najważniejsze funkcjonalności

Wybraliśmy trzy kluczowe funkcjonalności CrowdSec, które naszym zdaniem mają największe znaczenie dla skutecznej ochrony systemów i infrastruktury IT:

1. Analiza logów i wykrywanie zagrożeń

Funkcja ta stanowi podstawę działania CrowdSec. Bez skutecznego monitorowania logów i identyfikacji zagrożeń, dalsze działania ochronne, takie jak blokowanie atakujących adresów IP, byłyby niemożliwe. Dzięki analizie logów z różnych źródeł (serwery, aplikacje, urządzenia sieciowe), CrowdSec może wykrywać podejrzane aktywności, takie jak ataki brute-force, skanowanie portów czy próby SQL Injection. Jest to kluczowe dla zapewnienia bezpieczeństwa zarówno dla pojedynczych serwerów, jak i rozproszonych środowisk.

2. Mechanizm społecznościowego Threat Intelligence

Funkcja jest jednym z głównych czynników wyróżniających CrowdSec na tle innych systemów ochrony. Mechanizm ten pozwala użytkownikom na dzielenie się informacjami o złośliwych adresach IP, co znacząco przyspiesza reakcję na nowe zagrożenia i zmniejsza liczbę fałszywych alarmów. Dzięki temu społeczność CrowdSec działa jak globalny system ostrzegania, w którym każdy użytkownik przyczynia się do poprawy bezpieczeństwa całej sieci. To podejście pozwala również lepiej chronić przed atakami zero-day, zanim zostaną one oficjalnie udokumentowane.

3. Automatyczne blokowanie zagrożeń (Bouncers)

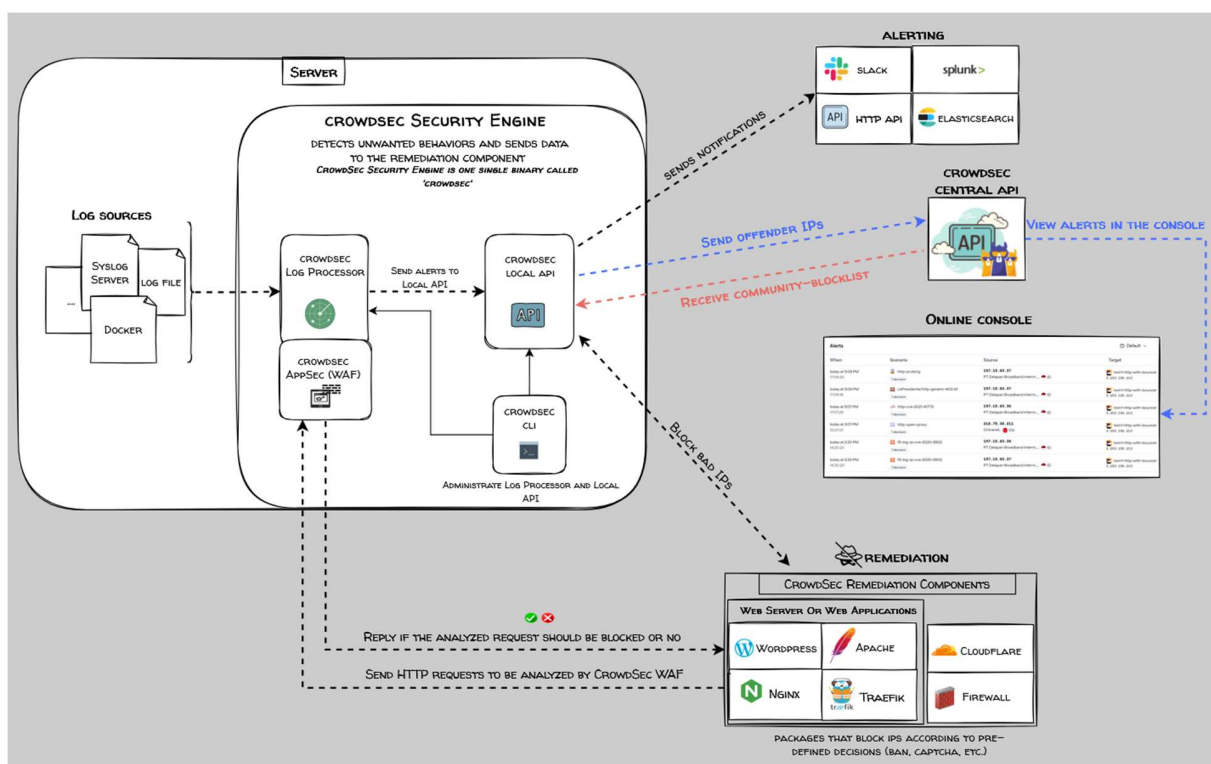
Wykrywanie zagrożeń to jedno, ale bez automatycznej reakcji na nie, ochrona nie byłaby w pełni skuteczna. Moduły Bouncers umożliwiają dynamiczne blokowanie atakujących IP na różnych poziomach – od firewalla, przez serwery WWW, aż po integrację z usługami chmurowymi, takimi jak Cloudflare. Automatyzacja tego procesu pozwala na natychmiastowe odcinanie zagrożeń bez konieczności ręcznej interwencji administratora, co jest kluczowe w przypadku ataków rozproszonych i dużej liczby incydentów.

10. Automatyzacja działania

CrowdSec oferuje zaawansowaną automatyzację mechanizmów obronnych, dzięki której użytkownik nie musi ręcznie analizować logów ani reagować na incydenty bezpieczeństwa. System działa w sposób ciągły, monitorując logi w czasie rzeczywistym, identyfikując podejrzane zachowania i natychmiast podejmując działania zapobiegawcze.

Automatyzacja obejmuje m.in. **wykrywanie wzorców ataków** (takich jak brute-force, skanowanie portów, próby włamań) na podstawie zdefiniowanych scenariuszy (tzw. "**scenarios**") oraz podejmowanie decyzji blokujących poprzez lokalny silnik decyzyjny (**Decision Engine**). Po zidentyfikowaniu zagrożenia, program automatycznie przekazuje decyzję do tzw. **bouncerów** – modułów odpowiedzialnych za wykonanie reakcji, np. blokadę IP na zaporze sieciowej, odcięcie sesji SSH, czy odrzucenie ruchu HTTP.

Ponadto, CrowdSec może integrować się z popularnymi firewallami, serwerami aplikacji, systemami SIEM i środowiskami chmurowymi, co pozwala na automatyczne egzekwowanie polityk bezpieczeństwa w różnych warstwach infrastruktury. Dzięki tej automatyzacji użytkownik zyskuje system, który nie tylko identyfikuje zagrożenia, ale również natychmiast je neutralizuje bez konieczności interwencji człowieka, minimalizując czas reakcji i ryzyko eskalacji ataku.



Schemat automatyzacji działania programu CrowdSec

11. Krótka instrukcja obsługi

11.1. Instalacja CrowdSec

Instalacja i konfiguracja programu CrowdSec na świeżym serwerze Ubuntu jest stosunkowo prosta i dobrze udokumentowana, co sprawia, że nawet mniej doświadczeni administratorzy mogą bez większych problemów rozpocząć korzystanie z tego systemu ochrony. Proces zaczyna się od dodania oficjalnego repozytorium CrowdSec do systemu za pomocą polecenia:

```
curl -s  
https://packagecloud.io/install/repositories/crowdsec/crowdsec/script.  
deb.sh | sudo bash
```

To polecenie automatycznie konfiguruje źródła pakietów dla systemu Ubuntu. Następnie instaluje się główny silnik CrowdSec komendą:

```
sudo apt install crowdsec -y
```

która pobiera i instaluje podstawową aplikację odpowiedzialną za analizę logów i wykrywanie zagrożeń. Po zakończeniu instalacji uruchamia się usługę i konfiguruje ją tak, aby startowała automatycznie razem z systemem:

```
sudo systemctl enable --now crowdsec
```

11.2. Wstępna konfiguracja CrowdSec

Kolejnym krokiem jest wstępna konfiguracja polegająca na dostosowaniu CrowdSec do środowiska użytkownika. Można to zrobić m.in. poprzez instalację parserów (tzw. kolekcji), które pozwalają analizować logi z konkretnych usług. Przykładowo, parser do SSH instalujemy komendą:

```
sudo cscli collections install crowdsecurity/sshd
```

natomiast jeśli chcemy analizować logi z serwera Nginx, używamy:

```
sudo cscli collections install crowdsecurity/nginx
```

Aby program mógł nie tylko wykrywać, ale i automatycznie reagować na zagrożenia, należy zainstalować tzw. bouncery – moduły wykonawcze, które wprowadzają decyzje blokujące w życie. Do ochrony na poziomie zapory sieciowej (iptables) służy:

```
sudo apt install crowdsec-firewall-bouncer-iptables -y
```

a dla serwera Apache:

```
sudo apt install crowdsec-crowdsec-apache2-bouncer -y
```

Aby zwiększyć dokładność wykrywania ataków, można zainstalować dodatkowe scenariusze, np. do wykrywania prób bruteforce SSH:

```
sudo cscli collections install crowdsecurity/ssh-bf
```

Po dodaniu nowych kolekcji i scenariuszy warto zrestartować usługę, aby zmiany zostały wprowadzone:

`sudo systemctl restart crowdsec`

Na koniec, przydatnym poleceniem do weryfikacji zainstalowanych komponentów jest:

`sudo cscli hub list`

które pozwala sprawdzić, jakie parsery, scenariusze i bouncery zostały już wdrożone. Cały proces instalacji i konfiguracji jest modularny, co daje użytkownikowi pełną kontrolę nad tym, jakie logi są analizowane i jak system ma reagować na wykryte zagrożeni

```
admin@Ubuntu-Server-24:~$ sudo cscli hub list
Loaded: 141 parsers, 10 postoverflows, 759 scenarios, 8 contexts, 4 appsec-configs, 105 appsec-rules, 138 collections
Unmanaged items: 1 local, 1 tainted
```

PARSERS				
Name	Status	Version	Local Path	
02-enrich.yaml	enabled, local		/etc/crowdsec/parsers/s02-enrich/02-enrich.yaml	
crowdsecurity/apache2-logs	enabled	1.5	/etc/crowdsec/parsers/s01-parse/apache2-logs.yaml	
crowdsecurity/dateparse-enrich	enabled	0.2	/etc/crowdsec/parsers/s02-enrich/dateparse-enrich.yaml	
crowdsecurity/dovecot-logs	enabled	0.9	/etc/crowdsec/parsers/s01-parse/dovecot-logs.yaml	
crowdsecurity/geoip-enrich	enabled	0.5	/etc/crowdsec/parsers/s02-enrich/geoip-enrich.yaml	
crowdsecurity/haproxy-logs	enabled	0.8	/etc/crowdsec/parsers/s01-parse/haproxy-logs.yaml	

SCENARIOS				
Name	Status	Version	Local Path	
crowdsecurity/apache_log4j2_cve-2021-44228	enabled	0.6	/etc/crowdsec/scenarios/apache_log4j2_cve-2021-44228.yaml	
crowdsecurity/CVE-2017-9841	enabled	0.2	/etc/crowdsec/scenarios/CVE-2017-9841.yaml	
crowdsecurity/CVE-2019-18935	enabled	0.2	/etc/crowdsec/scenarios/CVE-2019-18935.yaml	
crowdsecurity/CVE-2022-26134	enabled	0.2	/etc/crowdsec/scenarios/CVE-2022-26134.yaml	
crowdsecurity/CVE-2022-35914	enabled	0.2	/etc/crowdsec/scenarios/CVE-2022-35914.yaml	
crowdsecurity/CVE-2022-37042	enabled	0.2	/etc/crowdsec/scenarios/CVE-2022-37042.yaml	
crowdsecurity/CVE-2022-40684	enabled	0.3	/etc/crowdsec/scenarios/CVE-2022-40684.yaml	

CONTEXTS				
Name	Status	Version	Local Path	
crowdsecurity/bf_base	enabled	0.1	/etc/crowdsec/contexts/bf_base.yaml	
crowdsecurity/http_base	enabled	0.3	/etc/crowdsec/contexts/http_base.yaml	

COLLECTIONS				
Name	Status	Version	Local Path	
crowdsecurity/apache2	enabled	0.1	/etc/crowdsec/collections/apache2.yaml	
crowdsecurity/apiscp	enabled	0.1	/etc/crowdsec/collections/apiscp.yaml	
crowdsecurity/base-http-scenarios	enabled	1.0	/etc/crowdsec/collections/base-http-scenarios.yaml	
crowdsecurity/dovecot	enabled	0.1	/etc/crowdsec/collections/dovecot.yaml	
crowdsecurity/haproxy	enabled	0.1	/etc/crowdsec/collections/haproxy.yaml	
crowdsecurity/http-cve	enabled	2.9	/etc/crowdsec/collections/http-cve.yaml	
crowdsecurity/http-dos	enabled	0.2	/etc/crowdsec/collections/http-dos.yaml	
crowdsecurity/linux	enabled	0.2	/etc/crowdsec/collections/linux.yaml	
crowdsecurity/mysql	enabled	0.1	/etc/crowdsec/collections/mysql.yaml	

Fragment wizualizacji wszystkich zainstalowanych komponentów CrowdSec

11.3. Testowanie działania

W celu praktycznej weryfikacji skuteczności CrowdSec, przygotowaliśmy środowisko testowe składające się z **dwóch maszyn wirtualnych**:

1. **Ubuntu Server 22.04 LTS** (192.168.0.172) z interfejsem graficznym LXQT, na którym zainstalowano CrowdSec w podstawowej konfiguracji wraz z bouncerem firewallowym.
2. **Kali Linux** (192.168.0.177) wyposażony w narzędzia ofensywne, służący do symulacji ataków.

Przebieg testu:

Atak brute-force na SSH

Z maszyny Kali Linux wykonano atak na serwer Ubuntu za pomocą narzędzia hydra. Atak polegał na automatycznym sprawdzaniu haseł ze słownika *rockyou.txt*. W tym celu użyto polecenia:

```
hydra -L root -P /usr/share/wordlists/rockyou.txt -t 4
ssh://192.168.0.172
```

```
(kali@kali)-[~]
$ hydra -l root -P /usr/share/wordlists/rockyou.txt -t 4 ssh://192.168.0.172
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizati
ons, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-05-08 18:48:19
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session fou
nd, to prevent overwriting, ./hydra.restore
[DATA] max 4 tasks per 1 server, overall 4 tasks, 14344399 login tries (l:1/p:14344399), ~3586100 tries per task
[DATA] attacking ssh://192.168.0.172:22/
[STATUS] 80.00 tries/min, 80 tries in 00:01h, 14344319 to do in 2988:24h, 4 active
```

Atak bruteforce na ssh maszyny o IP 192.168.0.172

Reakcja CrowdSec

- CrowdSec wykrył wielokrotne nieudane próby logowania i zaklasyfikował je jako atak **ssh_bruteforce**.
- Adres IP Kali Linux (192.168.0.177) został automatycznie zablokowany na **4 godziny** (domyślny czas dla scenariusza ssh-bf).
- Bouncer firewallowy dodał regułę blokującą w firewallu systemowym

```
admin@Ubuntu-Server-24:~$ sudo cscli decisions list
```

ID	Source	Scope:Value	Reason	Action	Country	AS	Events	expiration	Alert ID
558449	crowdsec	Ip:192.168.0.177	crowdsecurity/ssh-slow-bf	ban			11	3h59m24s	119

```
11 duplicated entries skipped
```

Decyzja blokująca adres IP KaliLinux po wykryciu ataku bruteforce

Dodatkowo w **Dashboardzie CrowdSec** (dostępnym przez przeglądarkę) zarejestrowano alert w formie graficznej, zawierający szczegóły ataku (czas, źródło, typ).

CS - Alerts History

Aa Machine

ID	Date	Origin	Reason	Scope	Value	Country	AS	Started	Stopped	Message
123	2025-05-08 16:55:59	crowdsec	crowdsecurity/ssh-slow-bf	Ip	192.168.0.177			2025-05-08 16:55:52	2025-05-08 16:55:59	Ip 192.168.0.177 performed 'crowdsecurity/ssh-slow-bf' (11 events c
122	2025-05-08 16:55:46	crowdsec	crowdsecurity/ssh-bf	Ip	192.168.0.177			2025-05-08 16:55:43	2025-05-08 16:55:45	Ip 192.168.0.177 performed 'crowdsecurity/ssh-bf' (6 events over 2.0
121	2025-05-08 16:54:54	crowdsec	crowdsecurity/ssh-slow-bf	Ip	192.168.0.177			2025-05-08 16:54:47	2025-05-08 16:54:53	Ip 192.168.0.177 performed 'crowdsecurity/ssh-slow-bf' (11 events c
120	2025-05-08 16:54:45	crowdsec	crowdsecurity/ssh-bf	Ip	192.168.0.177			2025-05-08 16:54:42	2025-05-08 16:54:45	Ip 192.168.0.177 performed 'crowdsecurity/ssh-bf' (6 events over 3.0
119	2025-05-08 16:53:50	crowdsec	crowdsecurity/ssh-slow-bf	Ip	192.168.0.177			2025-05-08 16:53:44	2025-05-08 16:53:49	Ip 192.168.0.177 performed 'crowdsecurity/ssh-slow-bf' (11 events c
118	2025-05-08 16:53:42	crowdsec	crowdsecurity/ssh-bf	Ip	192.168.0.177			2025-05-08 16:53:39	2025-05-08 16:53:42	Ip 192.168.0.177 performed 'crowdsecurity/ssh-bf' (6 events over 2.0
117	2025-05-08 16:52:46	crowdsec	crowdsecurity/ssh-slow-bf	Ip	192.168.0.177			2025-05-08 16:52:39	2025-05-08 16:52:45	Ip 192.168.0.177 performed 'crowdsecurity/ssh-slow-bf' (11 events c
116	2025-05-08 16:52:37	crowdsec	crowdsecurity/ssh-bf	Ip	192.168.0.177			2025-05-08 16:52:34	2025-05-08 16:52:36	Ip 192.168.0.177 performed 'crowdsecurity/ssh-bf' (6 events over 2.0
115	2025-05-08 16:51:42	crowdsec	crowdsecurity/ssh-slow-bf	Ip	192.168.0.177			2025-05-08 16:51:36	2025-05-08 16:51:41	Ip 192.168.0.177 performed 'crowdsecurity/ssh-slow-bf' (11 events c

Szczegóły wykrytego ataku w graficznym interfejsie CrowdSec

12. Opinie użytkowników

CrowdSec cieszy się bardzo pozytywnym odbiorem wśród społeczności administratorów, specjalistów DevOps oraz entuzjastów bezpieczeństwa IT. Użytkownicy chwalą program przede wszystkim za jego skuteczność w wykrywaniu i blokowaniu realnych zagrożeń przy minimalnym wpływie na wydajność systemu.

Dużym uznaniem cieszy się również otwartość projektu – dostępność kodu źródłowego, rozbudowana dokumentacja oraz aktywna społeczność sprawiają, że wdrożenie i dostosowanie CrowdSec do konkretnych środowisk jest stosunkowo proste nawet dla mniej doświadczonych użytkowników. Wiele administratorów podkreśla, że w porównaniu do starszych rozwiązań, takich jak Fail2Ban, CrowdSec oferuje lepszą skalowalność, szybszą reakcję na nowe zagrożenia oraz wyjątkowo przydatną funkcję współdzielonej bazy blokowanych adresów IP.

Użytkownicy doceniają również integrację z narzędziami do wizualizacji (np. Grafana) oraz centralne zarządzanie przez CrowdSec Console, co znacząco ułatwia monitorowanie bezpieczeństwa w środowiskach rozproszonych. Pojawiające się uwagi krytyczne najczęściej dotyczą początkowej konfiguracji w bardziej złożonych infrastrukturach oraz potrzeby dostosowania scenariuszy do specyfiki logów, jednak ogólna opinia o programie pozostaje zdecydowanie pozytywna – wielu użytkowników określa go jako "nowoczesne i inteligentne podejście do prewencji zagrożeń".

87 CrowdSec Reviews

★★★★☆ 4.7 out of 5



Oceny programu CrowdSec z platformy G2

RB

Rei B.
Small-Business (50 or fewer emp.)

Validated Reviewer ✓

Verified Current User ✓

Review source: Seller invite

Incentivized Review

★★★★★ 6/7/2023

"It's a real life-saver in terms of hosting stuff"

What do you like best about CrowdSec?

What I love about it is its open source nature. By parsing logs you can block bad actors just like you would with fail2ban - but with grok patterns which are way easier to write and implement. New parsers are easily constructed and it's really easy to keep a ton of bad traffic out of your network.

What do you dislike about CrowdSec?

A bad thing about it is that you'd have to get a premium subscription in case you want more 'signals' than you share. Mostly ssh and http scenarios do although cover most of your bases.

Przykładowa ocena jednego z użytkowników CrowdSec porównującego go do Fail2Ban

13. Podsumowanie

Podsumowując, CrowdSec to nowoczesne narzędzie open-source, które łączy w sobie zaawansowane mechanizmy wykrywania zagrożeń z crowdsourcingowym modelem współpracy. Dzięki temu użytkownicy na całym świecie mogą dzielić się informacjami o atakach, co znacząco zwiększa skuteczność ochrony przed cyberzagrożeniami, takimi jak ataki brute-force, skanowanie portów czy DDoS.

Program wyróżnia się modularną architekturą, która umożliwia łatwą integrację z różnymi środowiskami, w tym systemami Linux, serwerami WWW (Nginx, Apache), usługami chmurowymi (AWS, Azure, Cloudflare) oraz narzędziami DevOps (Kubernetes, Docker). Dzięki temu CrowdSec może być dostosowany do potrzeb zarówno małych serwerów, jak i rozbudowanych infrastruktur korporacyjnych.

CrowdSec automatycznie wykrywa i blokuje zagrożenia, minimalizując konieczność interwencji administratora. Mechanizm bouncerów pozwala na natychmiastowe reagowanie na ataki, np. poprzez blokadę adresów IP na zaporze sieciowej lub w usługach chmurowych.

Współdzielenie danych o zagrożeniach w ramach społeczności CrowdSec przyspiesza reakcję na nowe wektory ataków i zmniejsza liczbę fałszywych alarmów. To sprawia, że program jest szczególnie skuteczny w walce z atakami zero-day.

Dzięki zoptymalizowanej architekturze CrowdSec działa wydajnie, nie obciążając nadmiernie systemu, co jest istotne w przypadku dużych środowisk produkcyjnych lub aplikacji chmurowych.

Instalacja i podstawowa konfiguracja CrowdSec są stosunkowo proste, co czyni go dostępnym nawet dla mniej doświadczonych użytkowników. Rozbudowana dokumentacja i wsparcie społeczności dodatkowo ułatwiają wdrożenie.

Mimo wielu zalet, początkowy proces konfiguracji w złożonych środowiskach może wymagać dostosowania scenariuszy detekcji do specyfiki logów. Ponadto, użytkownicy powinni zwracać uwagę na bezpieczeństwo lokalnego API i bouncerów, aby uniknąć potencjalnych ataków.

CrowdSec dynamicznie się rozwija, dodając nowe funkcje i integracje. Jego otwarty model rozwoju i współpraca z użytkownikami sprawiają, że ma potencjał, aby stać się jednym z wiodących rozwiązań w dziedzinie cyberbezpieczeństwa.

14. Bibliografia

- <https://docs.crowdsec.net/docs>
- <https://www.g2.com/products/crowdsec/reviews>
- <https://github.com/crowdsecurity/crowdsec>