|  |  |  |
| --- | --- | --- |
| **Politechnika Świętokrzyska**  Wydział Elektrotechniki, Automatyki i Informatyki | | |
| **Społeczne Aspekty Cyberbezpieczeństwa – Laboratorium** | | |
| **TEMAT:**  Opis programu CrowdSec | | **SKŁAD ZESPOŁU:**   * Przemysław Kałuziński (91271) * Jakub Kuśmierczyk (97504) * Michał Kaczor (91268) |
| **DATA:**  15.01.2025 | **GRUPA:**  1IZ22B |

# Spis treści

[1. Spis treści 2](#_Toc194134256)

[2. Wstęp 3](#_Toc194134257)

[3. Opis funkcjonalności 3](#_Toc194134258)

[4. Wybrane najważniejsze funkcjonalności 6](#_Toc194134259)

# 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

# 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.

# 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.

# 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. 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 dostarczanymi 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.

Obraz zawierający tekst, zrzut ekranu, diagram, Czcionka

Zawartość wygenerowana przez sztuczną inteligencję może być niepoprawna.

# 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.

Obraz zawierający tekst, zrzut ekranu, diagram, Czcionka

Zawartość wygenerowana przez sztuczną inteligencję może być niepoprawna.

Architektura działania CrowdSec

# 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.

**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.

**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.

**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.

**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 żądaniami,
* 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).

**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 zostałoby 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.

# 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.

* 1. **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.

* 1. **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.

# 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.

Obraz zawierający tekst, diagram, zrzut ekranu, Plan

Zawartość wygenerowana przez sztuczną inteligencję może być niepoprawna.

# 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.

# 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. Wielu 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".

# Krótka instrukcja obsługi

## Instalacja CrowdSec na świeżym serwerze Ubuntu

## Wstępna konfiguracja CrowdSec

## Uruchomienie CrowdSec i Dashboarda

## Testowanie CrowdSec w lokalnej sieci

# Instalacja, konfiguracja i uruchomienie CrowdSec na serwerze Ubuntu

## Instalacja CrowdSec na świeżym serwerze Ubuntu

Aktualizacja pakietów – Pobiera najnowsze wersje pakietów i aktualizuje system.

***sudo apt update && sudo apt upgrade -y***

Dodanie repozytorium CrowdSec – Automatycznie konfiguruje źródła pakietów dla Ubuntu.

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

Instalacja głównego silnika CrowdSec – Pobiera i instaluje główną aplikację.

***sudo apt install crowdsec -y***

Włączenie i uruchomienie usługi – Aktywuje CrowdSec i uruchamia go automatycznie przy starcie systemu.

***sudo systemctl enable --now crowdsec***

## Wstępna konfiguracja CrowdSec

Instalacja parsera dla SSH – Umożliwia analizowanie logów SSH w celu wykrywania ataków.

***sudo cscli collections install crowdsecurity/sshd***

Dodanie parsera dla serwera Nginx – Opcjonalnie, jeśli chcesz analizować logi z Nginx.

***sudo cscli collections install crowdsecurity/nginx***

Wyświetlenie dostępnych parserów – Sprawdza, jakie moduły przetwarzania logów są aktywne.

***sudo cscli parsers list***

Sprawdzenie dostępnych scenariuszy – Wyświetla reguły detekcji zagrożeń.

***sudo cscli scenarios list***

Podgląd aktualnych blokad – Wyświetla listę zablokowanych adresów IP.

***sudo cscli decisions list***

Instalacja bouncera (blokera) – Pozwala na automatyczne blokowanie złośliwego ruchu w iptables.

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

Instalacja bouncera serwera Apache – Pozwala na automatyczne blokowanie złośliwego ruchu dla serwera Apache

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

Nowe scenariusze– Dodaje więcej scenariuszy (np. w tym przypadku dla bruteforce SSH)

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

Restart CrowdSec – Wymuszona ponowna inicjalizacja po dodaniu nowych konfiguracji.

***sudo systemctl restart crowdsec***

Lista zainstalowanych kolekcji – Pozwala sprawdzić zainstalowane kolekcje CrowdSec

***sudo cscli hub list***

## Uruchomienie CrowdSec i Dashboarda

Instalacja dockera – Przed uruchomieniem Dashboarda trzeba zainstalować dockera

***sudo apt install docker.io***

Instalacja dashboarda – Konfiguruje interfejs webowy CrowdSec na otwartym porcie.

***sudo cscli dashboard setup –listen 0.0.0.0***

Uruchomienie dashboarda – Odpala serwer WWW dla panelu CrowdSec.

***sudo cscli dashboard start***

Sprawdzenie statusu CrowdSec – Informacja, czy usługa działa poprawnie.

***sudo systemctl status crowdsec***

Sprawdzenie, czy dashboard działa – Weryfikuje, czy CrowdSec Dashboard nasłuchuje na porcie 8080.

***sudo ss -tulnp | grep 8080***

Sprawdzenie statystyk działania – Wyświetla informacje o analizowanych logach i detekcjach.

***sudo cscli metrics***

Sprawdzenie dostępnych parserów i scenariuszy

***sudo cscli parsers list***

***sudo cscli scenarios list***

Sprawdzenie zablokowanych adresów IP

***sudo cscli decisions list***

Sprawdzenie zablokowanych adresów IP

***sudo cscli alerts list***

## Testowanie CrowdSec w lokalnej sieci

Jeżeli chcemy testować działanie CrowdSec w lokalnej sieci (np. pomiędzy 2 maszynami wirtualnymi), to trzeba najpierw zmodyfikować whitelistę, żeby blokowała również lokalne adresy (domyślnie Crowdsec pozwala na wszystkie scenariusze i ataki pochodzące z lokalnych adresów).

Wykonujemy polecenie:

sudo nano /etc/crowdsec/parsers/s02-enrich/whitelists.yaml

Następnie zastępujemy zawartość pliku poniższą:

name: crowdsecurity/whitelists

description: "Whitelist events from private ipv4 addresses"

whitelist:

reason: "localhost"

ip:

- "::1"

cidr:

- "127.0.0.0/8"

# Wykomentuj lokalne sieci, jeśli chcesz wykrywać ataki z LAN:

# - "192.168.0.0/16"

# - "10.0.0.0/8"

# - "172.16.0.0/12"

Na koniec restartujemy CrowdSec:

sudo systemctl restart crowdsec

PEŁNE SPRAWOZDANIE MA ZAWIERAĆ MIĘDZY INNYMI:

Opis narzędzia (producent, wersje, itd.)

Opis funkcjonalności ze screenami z najważniejszych fragmentów aplikacji

Przykład zastosowania

Opinie użytkowników