|  |  |  |
| --- | --- | --- |
| **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

# 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.

# 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