1. Najpierw zatrzymujemy działanie CrowdSec poleceniem
   sudo systemctl stop crowdsec
2. Później pokazujemy status działania CrowdSec poleceniem
   sudo systemctl status crowdsec
3. Później uruchamiamy CrowdSeca poleceniem
   sudo systemctl start crowdsec
4. Znowu sprawdzamy działanie CrowdSec poleceniem
   sudo systemctl status crowdsec
5. CrowdSec działa w jako usługa, która może startować automatycznie wraz z systemem, jeśli użyjemy odpowiedniego polecenia.
6. Pokazać polecenia instalacyjne i konfiguracyjne z naszego opracowania w pdfie i krótko je omówić.
7. Wywołujemy polecenie i omawiamy poszczególne elementy. To polecenie zawiera jedynie główną bazę artefaktów CrowdSec Hub i nie widać tutaj bouncerów, ponieważ są one dodatkowymi elementami
   sudo cscli hub list
   a. **PARSERS -** Pliki konfiguracyjne, które określają, **jak CrowdSec czyta i interpretuje logi** (np. z /var/log/auth.log dla SSH).
      Zawierają: Reguły parsowania logów (np. rozpoznawanie failed login attempts w logach SSH).
   b. **SCENARIOS -** Gotowe **reguły wykrywania ataków** (np. brute force, skanowanie portów).
      Zawierają: Definicje, jakie zachowania uznawać za atak (np. "5 failed SSH logins w 30 sekund = brute force").
   c. **CONTEXTS** - Dodatkowe **metadane lub dane pomocnicze**, które mogą być używane przez scenariusze (np. lista podejrzanych adresów IP).
      Zawierają: Np. listy geolokalizacji, tagi, informacje o botach.
   d. **COLLECTIONS - Zestawy powiązanych ze sobą parserów i scenariuszy** dla konkretnych usług (np. cała konfiguracja dla ochrony LAMP stack).
      Zawierają: Np. linux, nginx, wordpress – kolekcja zawiera wszystkie potrzebne parsery i scenariusze dla danej technologii.
8. Tak jak wcześniej wspomniano bouncery nie zostały tam wymienione, ponieważ są one traktowane jako **osobne komponenty** i nie są częścią głównej bazy. Możemy je wyświetlić wywołując polecenie:
   sudo cscli bouncers list
9. Teraz pokazujemy Dashboarda uruchamiając go poleceniem. Wspomnieć, że przy instalacji dashboarda zostaje podane hasło, które należy zapamiętać, bo bez niego nie dostaniemy się do dashboarda.
   sudo cscli dashboard start

2

a. baza CAPI to baza od CrowdSeca. Baza LAPI to lokalne api CrowdSeca

b. W Dashboardzie pokazać Our analytics -> CS -Mainboard (wykresy pojawią się po ataku)

10. Przechodzimy do prezentacji ataku. Uruchamiamy 2 polecenia i pokazujemy, że nie ma żadnych aktywnych alertów ani decyzji. Pokazujemy, że maszyny mogą się pingować. Adres IP maszyny sprawdzamy poleceniem 'ip a'.
sudo cscli alerts list
sudo cscli decisions list

a. Wspomnieć że korzystamy z kalilinux z narzędzia Hydra, które wykorzystuje słownik rockyou.txt do ataku bruteforce na ssh.

b. Wspomnieć, że żeby CrowdSec obsłużył takie ataki w lokalnej sieci, to trzeba było zmodyfikować whitelistę, żeby nie wykluczało odgórnie lokalnych adresów.

11. Wykonujemy atak na maszynie KaliLinux na SSH maszyny z CrowdSec (pamiętać, że adresy IP mogą się zmienić)

12. Pokazujemy na maszynie z CrowdSec nowe decyzje i alerty zarówno w konsoli jak i w dashboardzie.

13. Pokazujemy, że maszyny nie mogą się już pingować.

14. Usuwamy blokady i pokazujemy, że mogą się na nowo pingować.

Cel: Symulacja łamania hasła do SSH.
Kroki:

1. **Przeprowadź atak** (z Kali Linux):

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

2. **Sprawdź blokadę** (na Ubuntu z CrowdSec):

```
sudo cscli decisions list
sudo cscli alerts list
```

3. **Odblokuj IP** (pełne czyszczenie po teście):

```
sudo cscli decisions delete --ip 192.168.0.177
sudo cscli alerts delete --ip 192.168.0.177
sudo iptables -F
sudo nft flush ruleset
sudo systemctl restart crowdsec
```