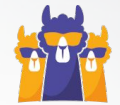
Safer Together

Open Source | IPS & | Participative CTI | Engine

Leveraging the power of the crowd to fight back against cyber criminals

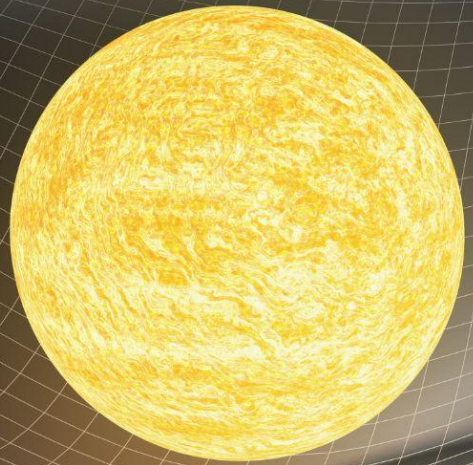
Agenda

1. Overview
2. Let’s get down and dirty



Cybersecurity *is not* a complicated problem

$$W\left[\frac{\xi}{\alpha}\left(\frac{\partial f}{\partial t}-\beta^r\frac{\partial f}{\partial r}\right)+\frac{v}{\phi^2}\frac{\partial f}{\partial r}\right]-\frac{\varepsilon W^3}{r\alpha\phi^3}\frac{\partial f}{\partial \varepsilon}$$
$$\times\left\{\beta^r\phi^3\left(-\psi-r\mu\frac{\partial v_r}{\partial r}\right)+v_r^2\phi\left[\beta^r\phi\left(2r\frac{\partial\phi}{\partial r}-\psi\phi\right)\right.\right.$$
$$\left.+r\left(-\mu\frac{\partial\alpha}{\partial r}+\mu^2\phi^2\frac{\partial\beta^r}{\partial r}-\frac{\partial\phi^2}{\partial t}\right)\right]$$
$$+v_r^3\left[r\mu\phi\left(-\mu\frac{\partial\alpha}{\partial r}+\frac{\partial\beta^r\phi^2}{\partial r}-\frac{\partial\phi^2}{\partial t}\right)-\psi\frac{\alpha}{\phi}\frac{\partial r\phi^2}{\partial r}\right]$$
$$+\phi\left[r\mu\left(\mu\alpha\frac{\partial v_r}{\partial r}+\frac{\partial\alpha}{\partial r}+\phi^2\left(-\mu\frac{\partial\beta^r}{\partial r}+\frac{\partial v_r}{\partial t}\right)\right)\right.$$
$$\left.+r\frac{\partial\phi^2}{\partial t}-r\beta^r\frac{\partial\phi^2}{\partial r}\right]+v_r\alpha\left[\phi\left(\psi+r\mu\frac{\partial v_r}{\partial r}\right)\right.$$
$$\left.\left.+2r\psi\frac{\partial\phi}{\partial r}+\phi^2\left(\mu\frac{\partial v_r}{\partial t}-\frac{\partial\beta^r}{\partial r}\right)+\frac{\partial\phi^2}{\partial t}\right]\right\}$$
$$+\frac{W^3(1-\mu^2)}{r\alpha\phi^3}\frac{\partial f}{\partial\mu}\left\{\alpha\left[\phi\left(\frac{\xi}{W^2}-rv\frac{\partial v_r}{\partial r}\right)+2r\frac{\xi}{W^2}\frac{\partial\phi}{\partial r}\right]\right.$$
$$+\phi\left[\beta\phi^2\left(r\xi\frac{\partial v_r}{\partial r}-\frac{v}{W^2}\right)-\frac{r}{W^2}\left(\xi\frac{\partial\alpha}{\partial r}-v\phi^2\frac{\partial\beta^r}{\partial r}\right)\right.$$
$$\left.\left.-r\xi\phi^2\frac{\partial v_r}{\partial t}\right]\right\}=\mathbb{C}[f],$$



(*This* was a complicated one)

It’s a complex one

(*Like sending people to the moon*)

CYBERSECURITY IS NOT EITHER A PROBLEM OF MEANS

EQUIFAX	**800K** records **57000** users	MGM GRAND	**142M** accounts
zoom	**500K** accounts		**267M** records
solarwind	**5.2M** accounts		**32M** accounts high profile hack
Microsoft	**Tens of thousands** of emails servers	CapitalOne	**$80M**
easyJet	**9M** accounts	J.P.Morgan	**83M** accounts

The others

CrowdSec

Since the 90's, we addressed Cybersecurity as a complicated problem

Outpowering

FAILED

Outsmarting

FAILED

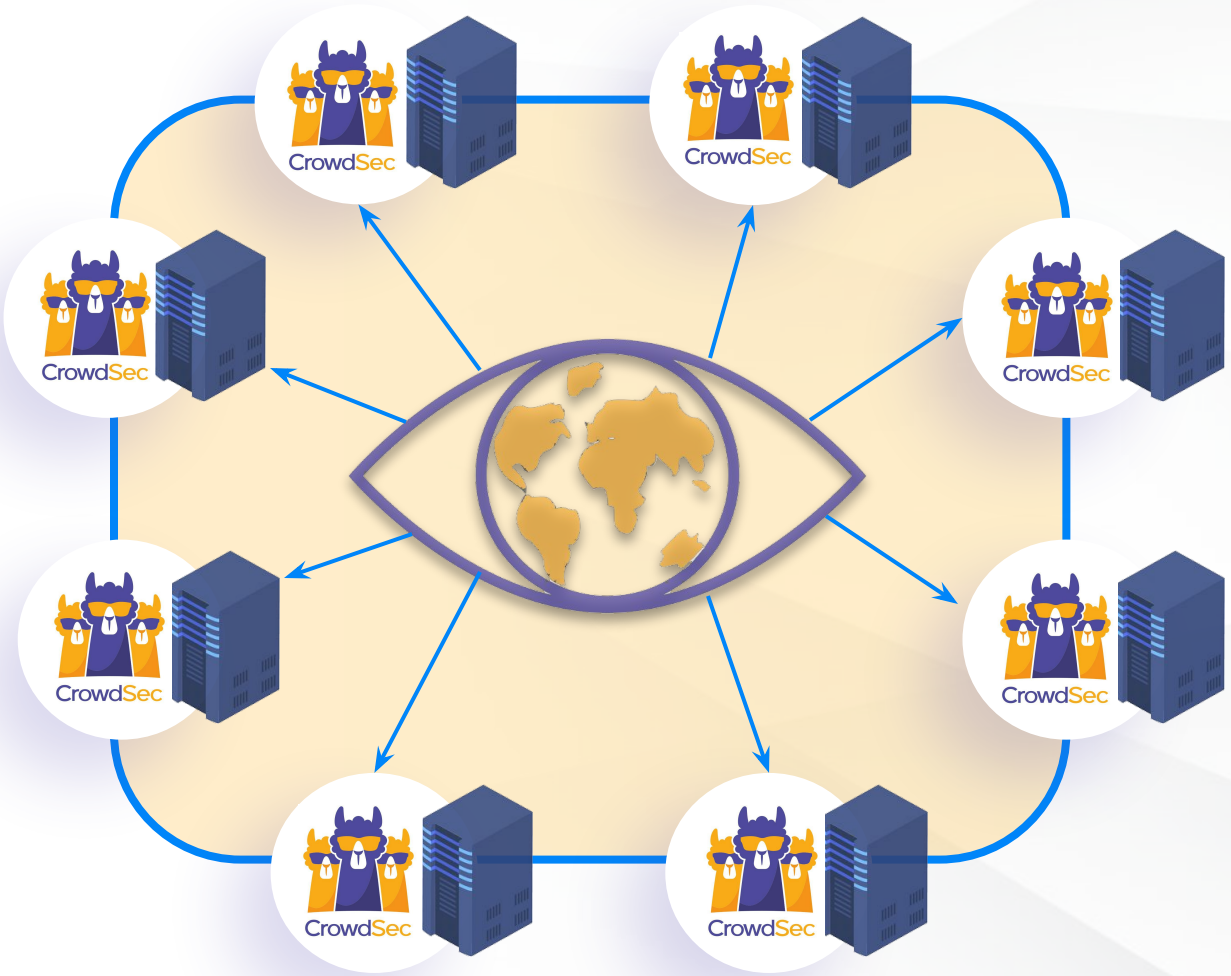
Outnumbering

Shall we try a participative approach?

Instead of a complex one...

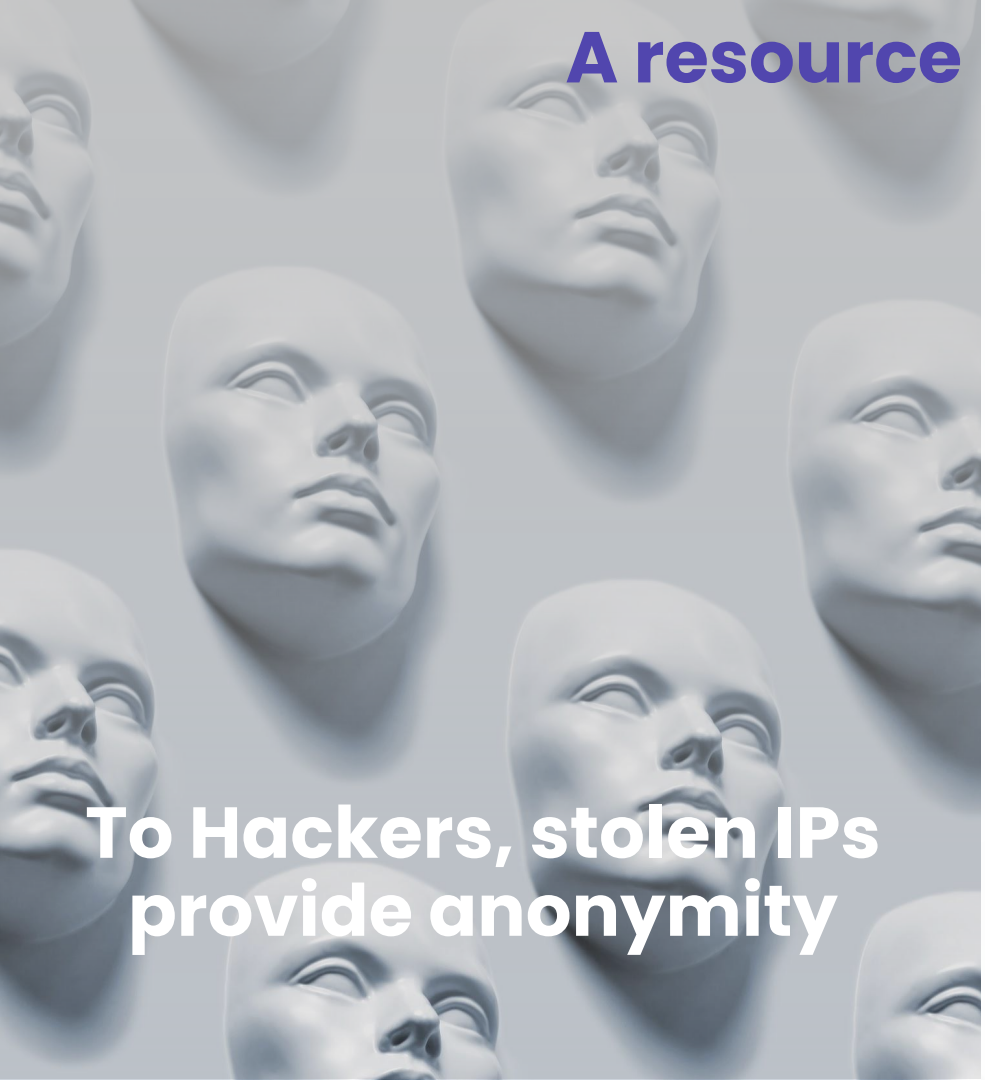
CrowdSec

BUILDING THE *"WAZE OF CYBER SECURITY"*



Local IPS
Global CTI

A resource WAR



To Hackers, stolen IPs provide anonymity

CrowdSec

Our community is peeling the onion

(and, spoiler alert, we're not the one crying)

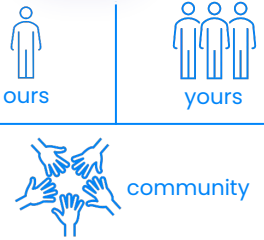
Massively Participative IPS

1

Syslog, Splunk journald, Cloudtrails, SIEM, ELK, Kafka, etc.

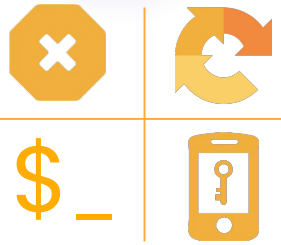
Connect the data source you want

2



*The **Agent** detects threats based on behavior scenarios*

3



*The **Bouncer** remedy them where & how you want*

4

Share with community

Scenarios

L7 DDoS (Applicative)

Ransomware (*lateral move*)

Resource abuse

Credentials Brute-forcing

Php-based armageddons

Port scans

Web scans

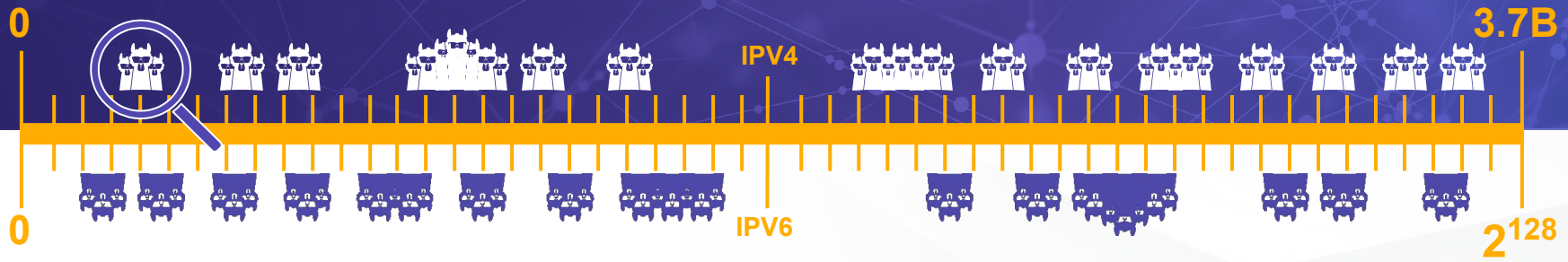
Credential or credit card stuffing

Bot Scalping & Scraping

Targeted attacks

CrowdSec

Crowd sourced Cyber Threat Intelligence



Instead of running simulated services (honeypots) over a few hundreds of servers on a couple of clouds

We harness the power of thousands of real servers, running real services across all types of environments & connections

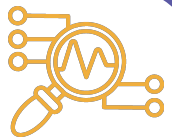
CrowdSec

Free. Forever. Period.

01 **OPEN SOURCE (MIT)**

02 **FREE** (*to use, copy, modify*)

MIT license.
As free as it can be.



Transparent, auditable and trustable.

Open to contribution

CrowdSec

BAD IP?
Context is key

Time dependant

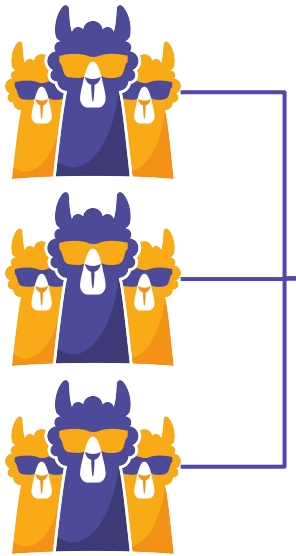
- A malicious IP was once clean
- It's rogue only when a hacker owns it
- And it will be cleaned one day

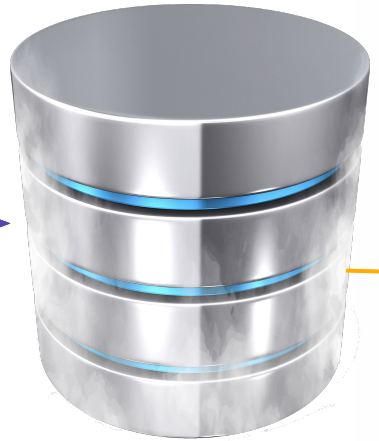
Each IP is refreshed every 72 hours max

CrowdSec

No Smoke without Fire

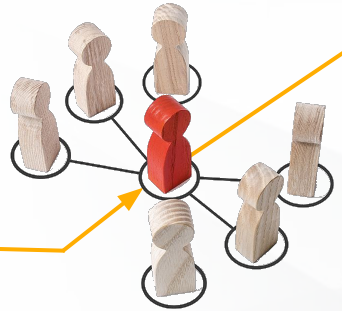
Agents send rogue IPs to the "**Smoke**" **DB**

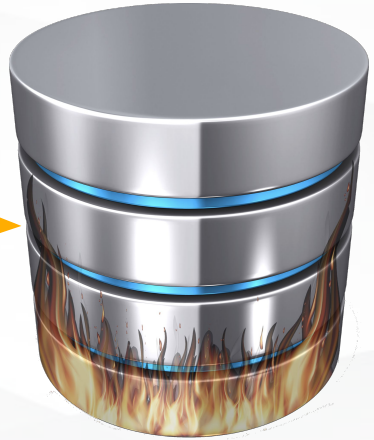




Goal: Feed CTI, SIEM, SoC

If the network reaches a ***consensus*** the IP enters the "**Fire**" **DB**





Goal: Instruct all bouncers in the world to treat this IP as hostile

Your logs are never exported

CrowdSec only collects

CrowdSec

Slowly conquering the world

CrowdSec

>20K installations worldwide
Across 110 countries and 6 continents

700 000 malicious IPs detected
72 hours fresh

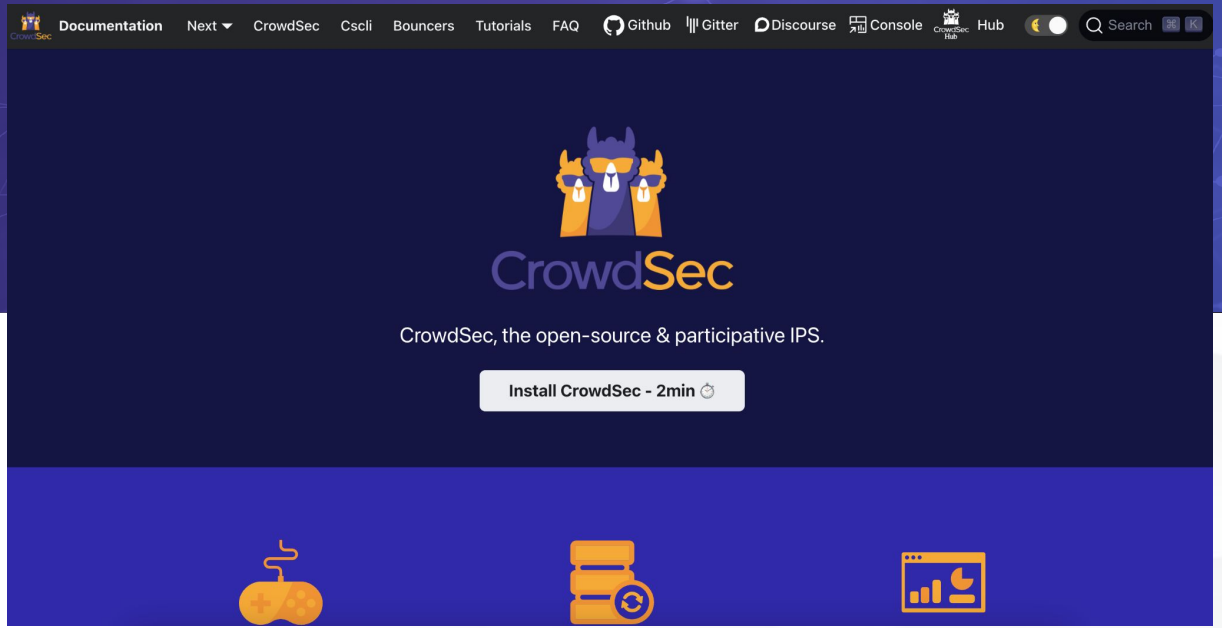
Use cases across various industries
Hosters, universities, research centers, municipalities etc.
Blocked HTTP DDoS botnets, Credit card stuffers, etc.

2024 goal
10^6 machines in our CTI Network

Let’s get our hands (a little) dirty

CrowdSec

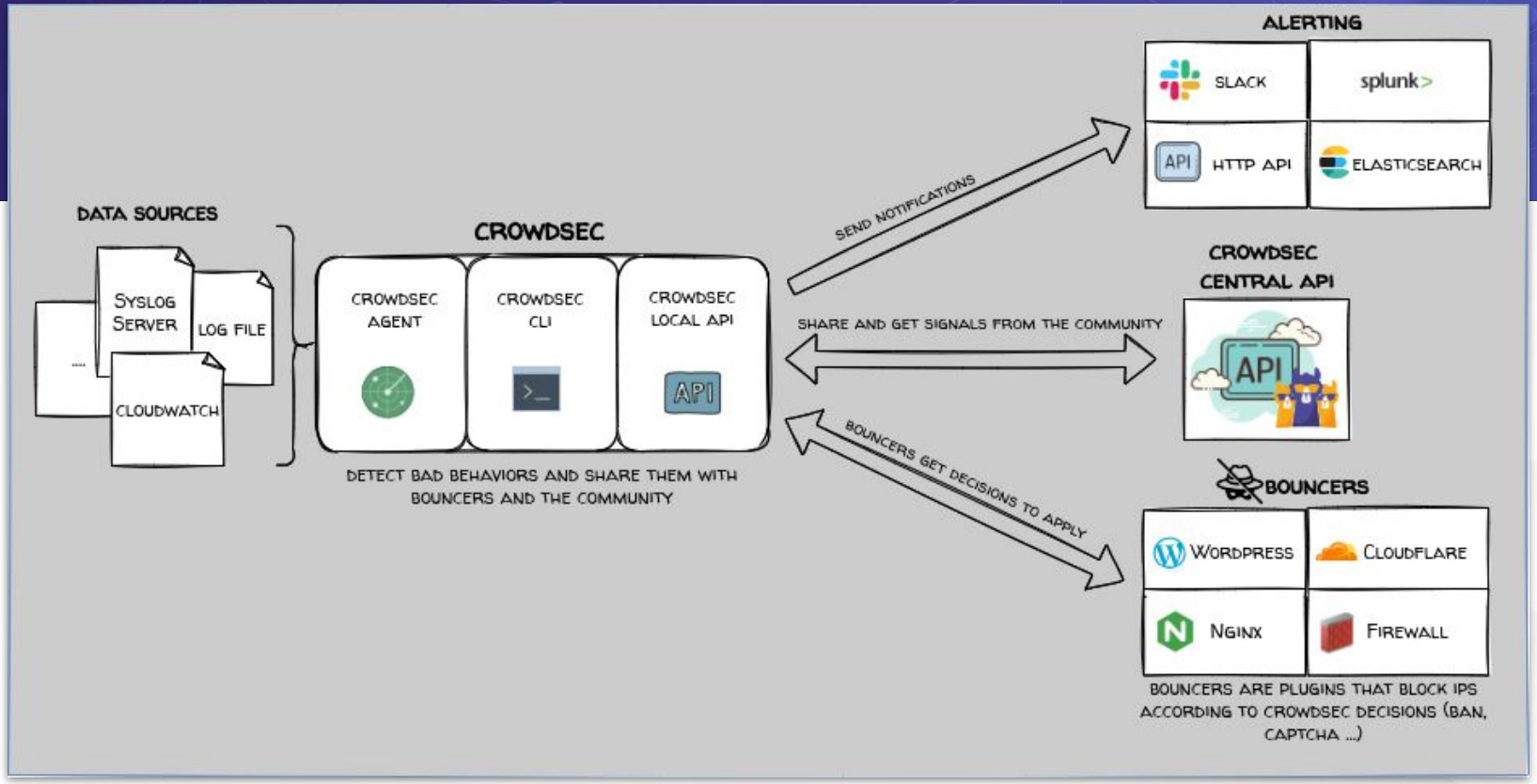
CrowdSec docs



- https://doc.crowdsec.net/
- Made with Docusarus
- Code at https://github.com/crowdsecurity/crowdsec-docs

CrowdSec

Now let's get ~~physi~~technical



CrowdSec

Data Sources

Name	Type	Stream	One-Shot
file	Single files, glob expressions, gz files	yes	yes
journald	Via filter	yes	yes
AWS cloudwatch	Single stream or log group	yes	yes
Syslog service	Read logs received via syslog protocol	Yes	no

CrowdSec

Agents


Linux


FreeBSD


Docker

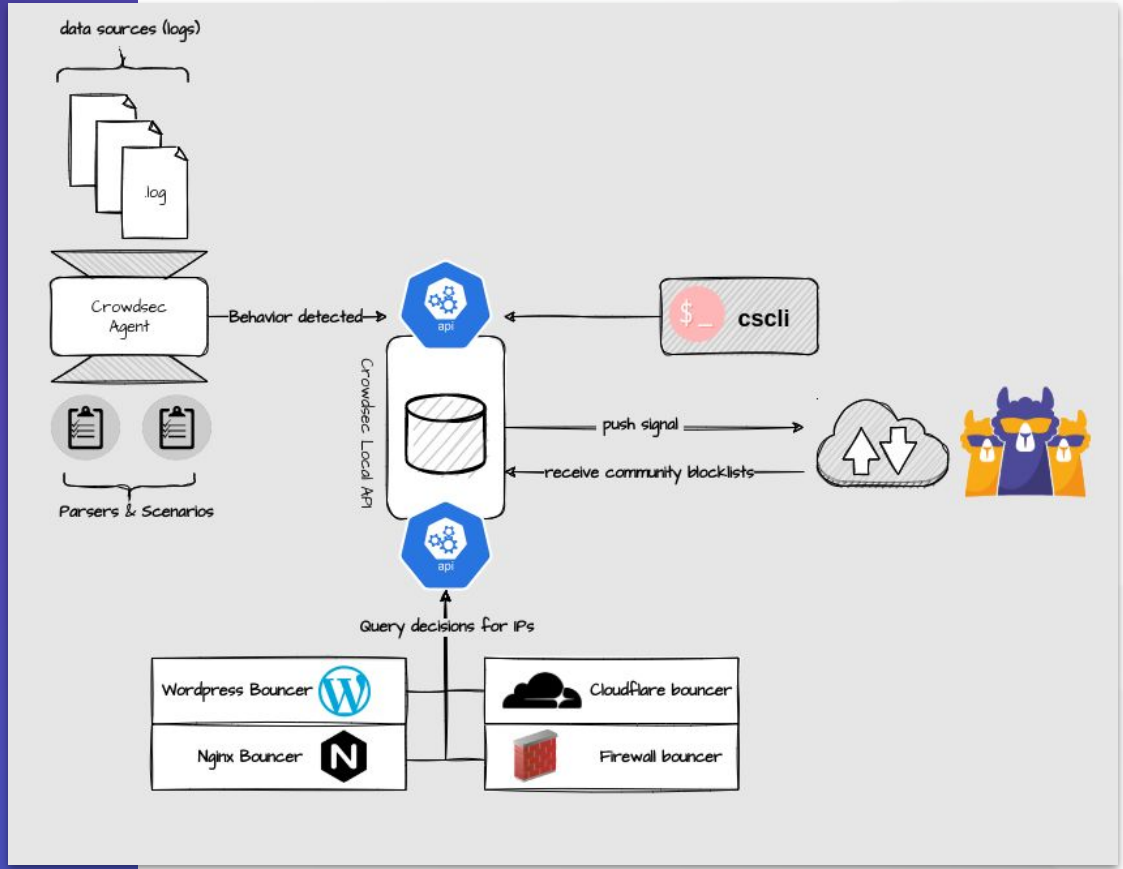

k8s


OpenWRT


Windows

CrowdSec

CrowdSec Dataflow

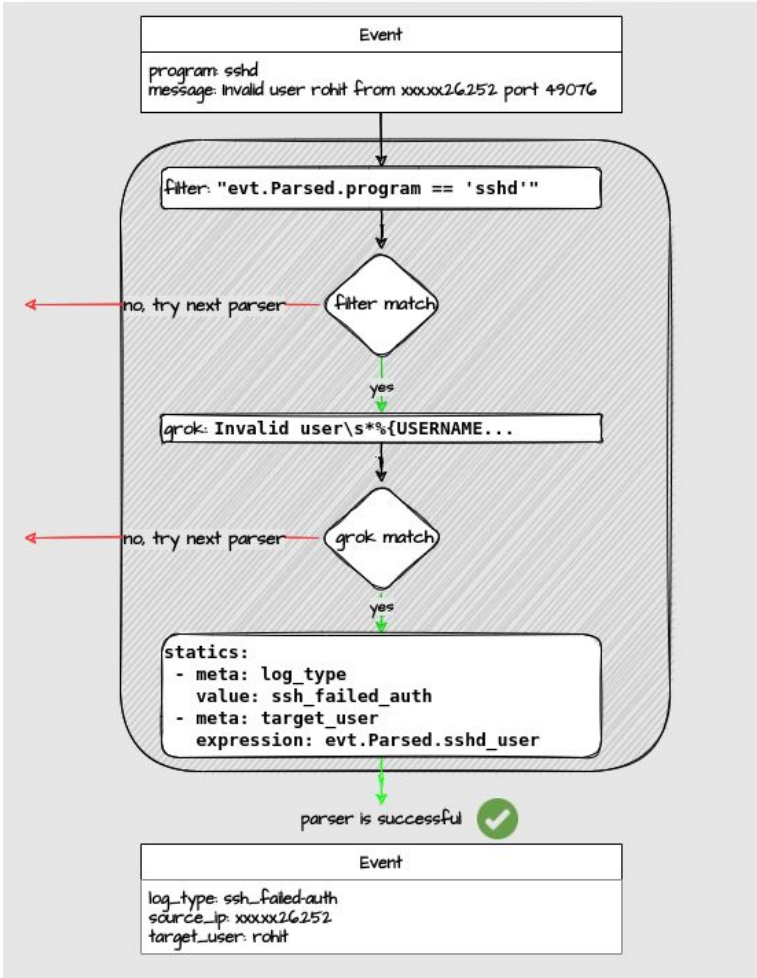


CrowdSec

CrowdSec foundations

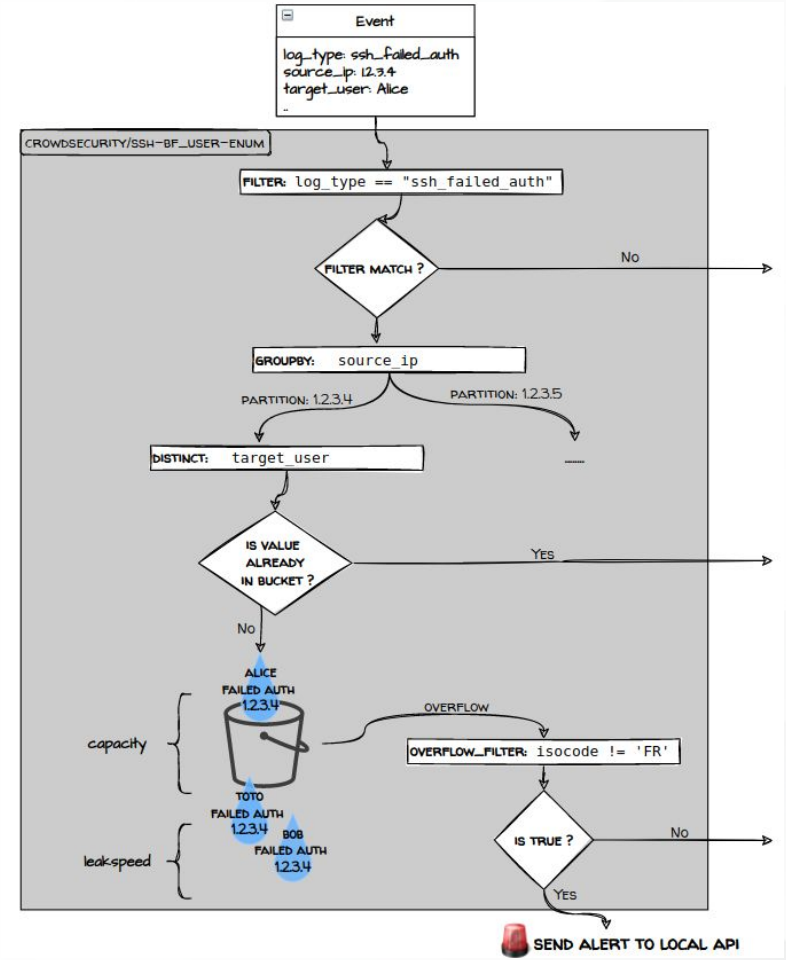
Collections:
Bundled parsers and scenarios

Parsers



CrowdSec

Scenarios



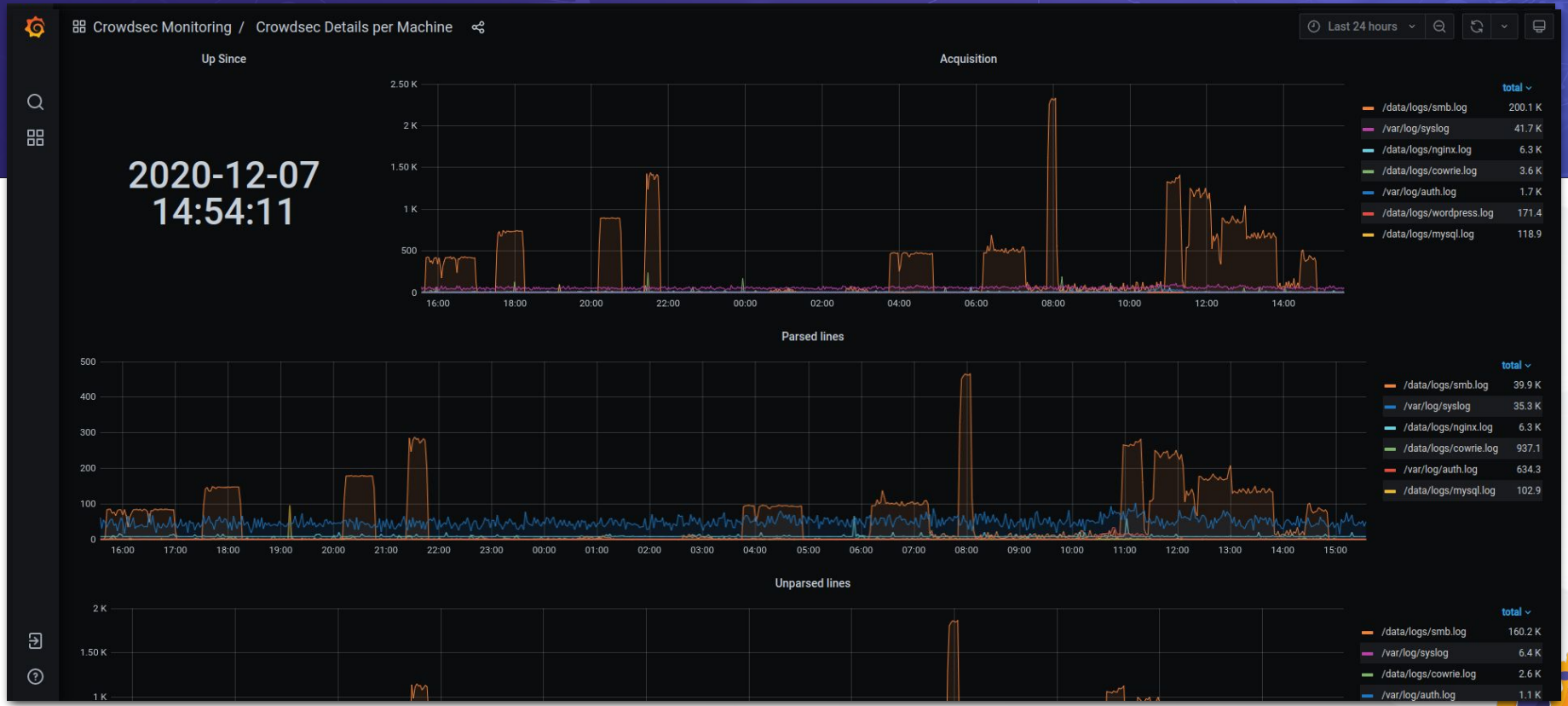
CrowdSec

Observability

- Prometheus
- `cscli`
- agent's own easy-to-parse log file
- Metabase dashboard
- Brand new web console

CrowdSec

Grafana



CrowdSec

cscli pr0n

```
bui@sd-126005:~$ cscli  metrics
INFO[05-10-2021 03:42:43 PM] Buckets Metrics:
+-----------------------------------------+---------------+-----------+-------------+--------+---------+
|                  BUCKET                 | CURRENT COUNT | OVERFLOWS | INSTANCIATED | POURED | EXPIRED |
+-----------------------------------------+---------------+-----------+-------------+--------+---------+
| crowdsecurity/http-bad-user-agent       | -             |        40 |         168 |    210 |     128 |
| crowdsecurity/http-crawl-non_statics    | -             | -         |        1231 |   1728 |    1231 |
| crowdsecurity/http-path-traversal-probing | -           | -         |           2 |      2 |       2 |
| crowdsecurity/http-probing              | -             |        24 |         611 |   1092 |     587 |
| crowdsecurity/http-sensitive-files      | -             | -         |          52 |     52 |      52 |
| crowdsecurity/iptables-scan-multi_ports |            38 |      6151 |      118843 | 311961 |  112654 |
| crowdsecurity/ssh-bf                    | -             |        45 |        1211 |   2569 |    1166 |
| crowdsecurity/ssh-bf_user-enum          | -             |        13 |        1256 |   1820 |    1243 |
| crowdsecurity/ssh-slow-bf               | -             |        96 |        1050 |   2569 |     954 |
| crowdsecurity/ssh-slow-bf_user-enum     | -             |        35 |         998 |   1711 |     963 |
+-----------------------------------------+---------------+-----------+-------------+--------+---------+
INFO[05-10-2021 03:42:43 PM] Acquisition Metrics:
+-----------------------------------------+------------+--------------+----------------+-----------------------+
|                  SOURCE                 | LINES READ | LINES PARSED | LINES UNPARSED | LINES POURED TO BUCKET |
+-----------------------------------------+------------+--------------+----------------+-----------------------+
| file:/var/log/auth.log                  |      23103 |        11269 |          11834 |                  8669 |
| file:/var/log/kern.log                  |     801186 |       800377 |            809 |                 92469 |
| file:/var/log/messages                  |     801195 |       800377 |            818 |                112795 |
| file:/var/log/nginx/error.log           |       3000 | -            |           3000 | -                     |
| file:/var/log/nginx/memze.ro-http.access.log |     1230 |         1124 |            106 |                  1615 |
| file:/var/log/nginx/memze.ro-https.access.log |    1196 |         1172 |             24 |                  1469 |
| file:/var/log/syslog                    |     812354 |       800372 |          11982 |                106697 |
+-----------------------------------------+------------+--------------+----------------+-----------------------+
INFO[05-10-2021 03:42:43 PM] Parser Metrics:
+---------------------------------+---------+---------+----------+
|             PARSERS             |  HITS   | PARSED  | UNPARSED |
+---------------------------------+---------+---------+----------+
| child-crowdsecurity/http-logs   |    6888 |    4138 |     2750 |
| child-crowdsecurity/nginx-logs  |   12360 |    2296 |    10064 |
| child-crowdsecurity/sshd-logs   |   89611 |   11269 |    78342 |
| crowdsecurity/dateparse-enrich  | 2414691 | 2414691 | -        |
| crowdsecurity/geoip-enrich      | 2414691 | 2414691 | -        |
| crowdsecurity/http-logs         |    2296 |    1503 |      793 |
| crowdsecurity/iptables-logs     | 2403556 | 2401126 |     2430 |
| crowdsecurity/nginx-logs        |    7328 |    2296 |     5032 |
| crowdsecurity/non-syslog        |    5426 |    5426 | -        |
| crowdsecurity/sshd-logs         |   20732 |   11269 |     9463 |
| crowdsecurity/syslog-logs       | 2437838 | 2437834 |        4 |
| crowdsecurity/whitelists        | 2414691 | 2414691 | -        |
+---------------------------------+---------+---------+----------+
INFO[05-10-2021 03:42:43 PM] Local Api Metrics:
```

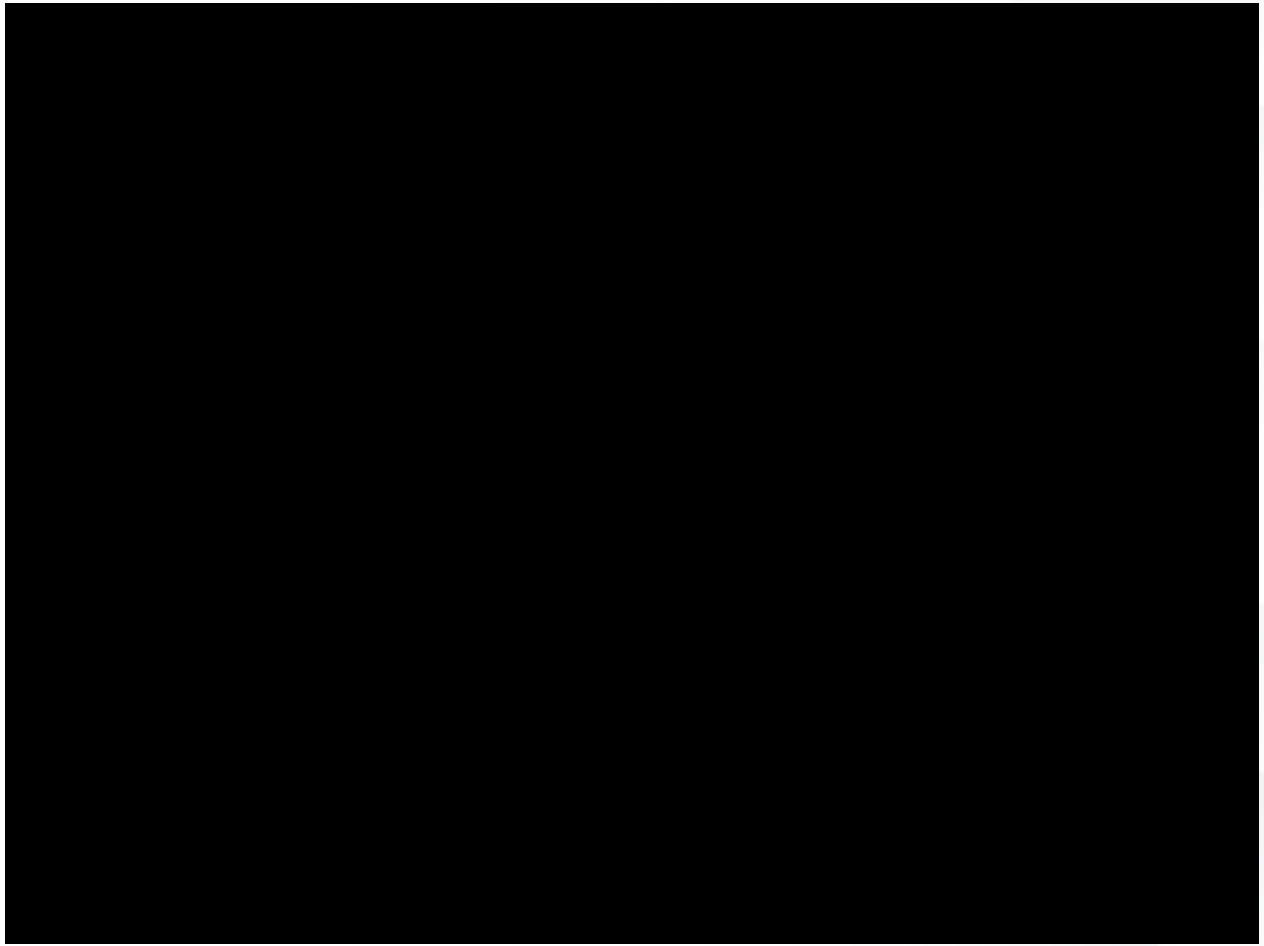
CrowdSec

cscli - management

```
INFO[05-10-2021 03:46:04 PM] SCENARIOS:
NAME                                    STATUS                    VERSION  LOCAL PATH
crowdsecurity/mysql-bf                  ✔ enabled                 0.1      /etc/crowdsec/scenarios/mysql-bf.yaml
crowdsecurity/http-backdoors-attempts   ✔ enabled                 0.2      /etc/crowdsec/scenarios/http-backdoors-attempts.yaml
crowdsecurity/http-crawl-non_statics    ✔ enabled                 0.2      /etc/crowdsec/scenarios/http-crawl-non_statics.yaml
crowdsecurity/http-probing              ✔ enabled                 0.2      /etc/crowdsec/scenarios/http-probing.yaml
crowdsecurity/ssh-bf                    ✔ enabled                 0.1      /etc/crowdsec/scenarios/ssh-bf.yaml
crowdsecurity/http-path-traversal-probing ✔ enabled               0.2      /etc/crowdsec/scenarios/http-path-traversal-probing.yaml
crowdsecurity/iptables-scan-multi_ports ✔ enabled                 0.1      /etc/crowdsec/scenarios/iptables-scan-multi_ports.yaml
ltsich/http-w00tw00t                    ✔ enabled                 0.1      /etc/crowdsec/scenarios/http-w00tw00t.yaml
crowdsecurity/http-bad-user-agent       ✔ enabled                 0.4      /etc/crowdsec/scenarios/http-bad-user-agent.yaml
crowdsecurity/http-generic-bf           ✔ enabled                 0.1      /etc/crowdsec/scenarios/http-generic-bf.yaml
crowdsecurity/http-sqli-probing         ✔ enabled                 0.2      /etc/crowdsec/scenarios/http-sqli-probing.yaml
crowdsecurity/http-sensitive-files      ✔ enabled                 0.2      /etc/crowdsec/scenarios/http-sensitive-files.yaml
crowdsecurity/http-xss-probing          ✔ enabled                 0.2      /etc/crowdsec/scenarios/http-xss-probing.yaml
crowdsecurity/ssh-slow-bf               ⚠ enabled,update-available 0.1     /etc/crowdsec/scenarios/ssh-slow-bf.yaml
INFO[05-10-2021 03:46:04 PM] COLLECTIONS:
NAME                                STATUS                    VERSION  LOCAL PATH
crowdsecurity/sshd                  ⚠ enabled,update-available 0.2     /etc/crowdsec/collections/sshd.yaml
crowdsecurity/iptables              ✔ enabled                 0.1      /etc/crowdsec/collections/iptables.yaml
crowdsecurity/linux                 ✔ enabled                 0.2      /etc/crowdsec/collections/linux.yaml
crowdsecurity/base-http-scenarios   ⚠ enabled,update-available 0.4     /etc/crowdsec/collections/base-http-scenarios.yaml
crowdsecurity/mysql                 ✔ enabled                 0.1      /etc/crowdsec/collections/mysql.yaml
crowdsecurity/nginx                 ⚠ enabled,update-available 0.1     /etc/crowdsec/collections/nginx.yaml
INFO[05-10-2021 03:46:04 PM] POSTOVERFLOWS:
NAME  STATUS  VERSION  LOCAL PATH
root@sd-126005:/home/bui# cscli  hub upgrade
INFO[05-10-2021 03:46:13 PM] Upgrading collections
WARN[05-10-2021 03:46:13 PM] crowdsecurity/http-logs : overwrite
WARN[05-10-2021 03:46:13 PM] crowdsecurity/http-crawl-non_statics : overwrite
WARN[05-10-2021 03:46:13 PM] crowdsecurity/http-probing : overwrite
```

CrowdSec

Console



CrowdSec

Notification plugins

HTTP Push

APIs

- Local API
- Central API

CrowdSec

Bouncers

- Firewall
- Nginx
- Custom
- Cloudflare
- Wordpress
- Generic PHP
- DIY?

CrowdSec

Examples

- Protecting services (any service!)
- Canary device (portscan detection)
- Wordpress
- Generic PHP site protection

CrowdSec

Decision making in CrowdSec

What about the future?

- Serverless architecture
- Credential/Credit card stuffing/Data theft
- Integration with mod_security
- Exposing CTI

Any questions?

Mr Reputation

Mr Behavior

SecOps, DevOps, let's outnumber cybercriminals

Please get in touch

Try out CrowdSec:
https://crowdsec.net/
https://github.com/crowdsecurity/
Twitter: @crowd_security

Join our Discourse: https://discourse.crowdsec.net

Send me a mail:
klaus@crowdsec.net

CrowdSec