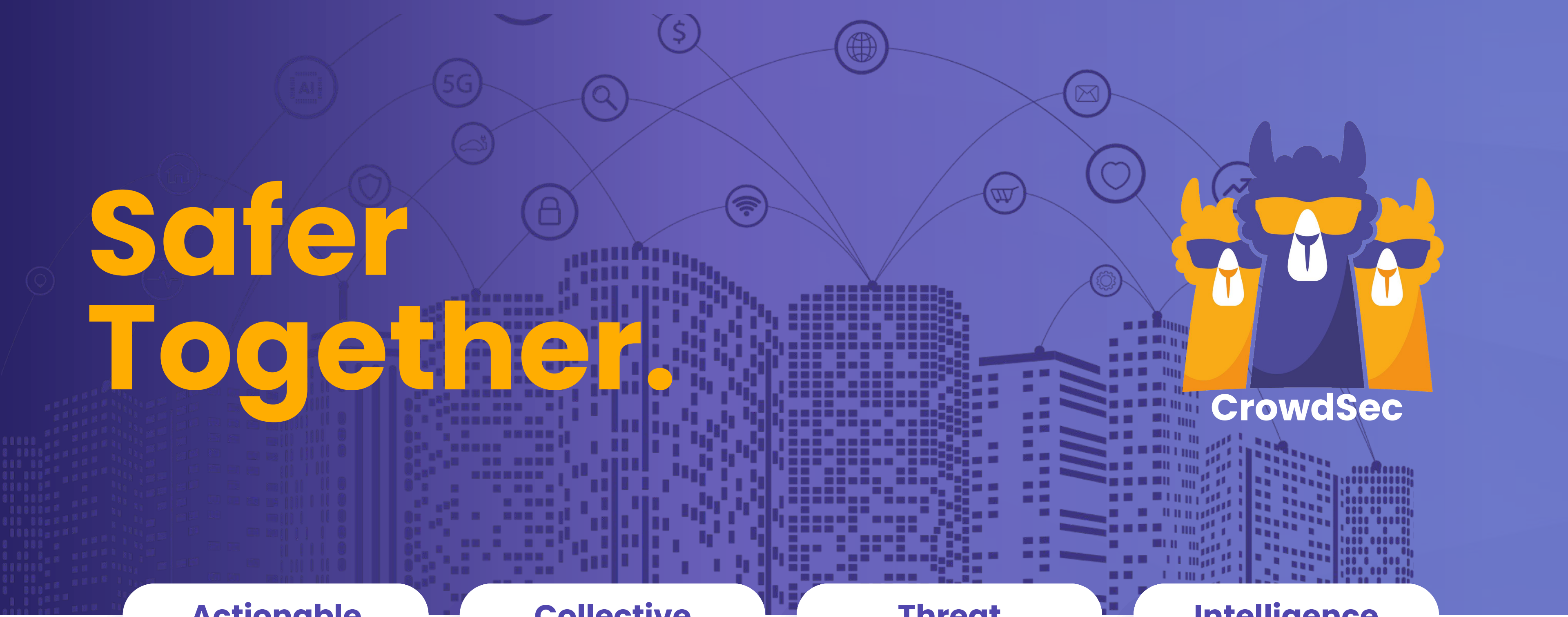


Safer Together.

CrowdSec

Actionable

Collective

Threat

Intelligence

Crowd-Powered Cyber Threat Intelligence

CYBERSECURITY IS NOT EITHER A PROBLEM OF MEANS

EQUIFAX	800K records 57000 users	MGM GRAND	142M accounts
zoom	500K accounts	f	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

Their unfair advantages

Time

Time between vulnerability & patch, intrusion and detection, safe and … sorry.

Perimeter

Shadow IT, Cloud, SaaS, VPNs, cloud drives, Containers, and VMs created an uneven security level across the perimeter. Supply chain attack.

Money

Hackers use stolen servers, and (mostly) free tools. According to Deloitte, Cyber criminals don't even need 1% of your budget to attack you.

CrowdSec

The "*Castle strategy*", like the walkman, belong to the *80's*

Since IT ressources are scattered across

Let's help them assess who to trust in millisec

Reputation can & Crowd is the key to it

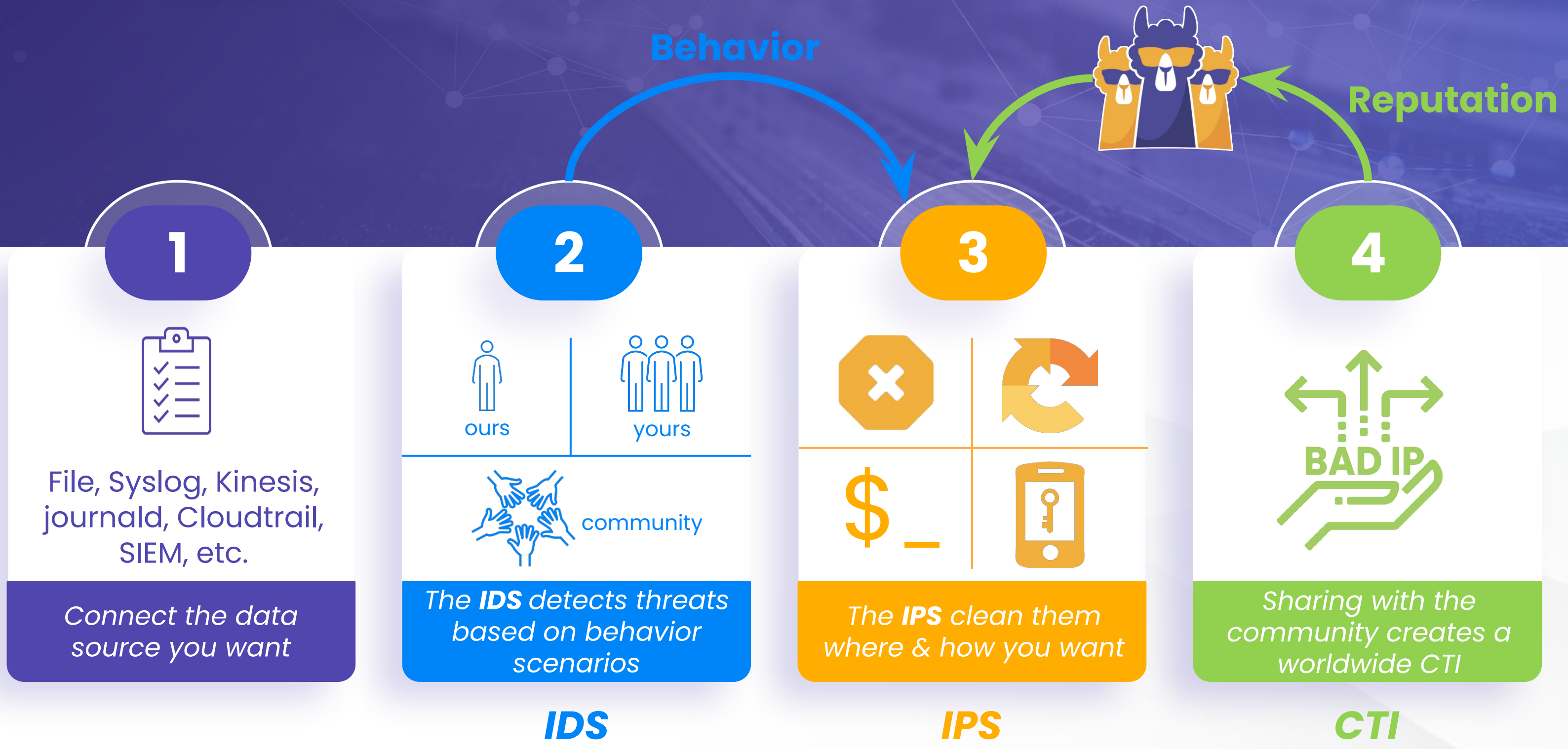
CrowdSec

Already organizing the fight back in 155 countries… in 15 months.

Local IPS
Global CTI

BUILDING THE *"WAZE OF IP REPUTATION"*

Massively
└ collaborative
└ IDPS



1

File, Syslog, Kinesis, journald, Cloudtrail, SIEM, etc.

Connect the data source you want

2

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

IDS

3

*The **IPS** clean them where & how you want*

IPS

4

Sharing with the community creates a worldwide CTI

CTI

BEHAVIOR ENGINE = CYBERSEC HYGIENE

- L7 DDoS (Applicative)
- Ransomware (*lateral move*)
- Resource abuse
- Credentials Brute-forcing
- XSS, SQLi, & Php-based armageddons
- 21 22 23 25 80 Port scans
- Web scans
- Credential or credit card stuffing
- Bot Scalping & Scraping
- Targeted attacks

Nowadays, everything generates logs and if you can describe the behavior you look for, CrowdSec will find it.

API-driven

Allows complex setups

Ops friendly

Observability & IAC

DevOps friendly

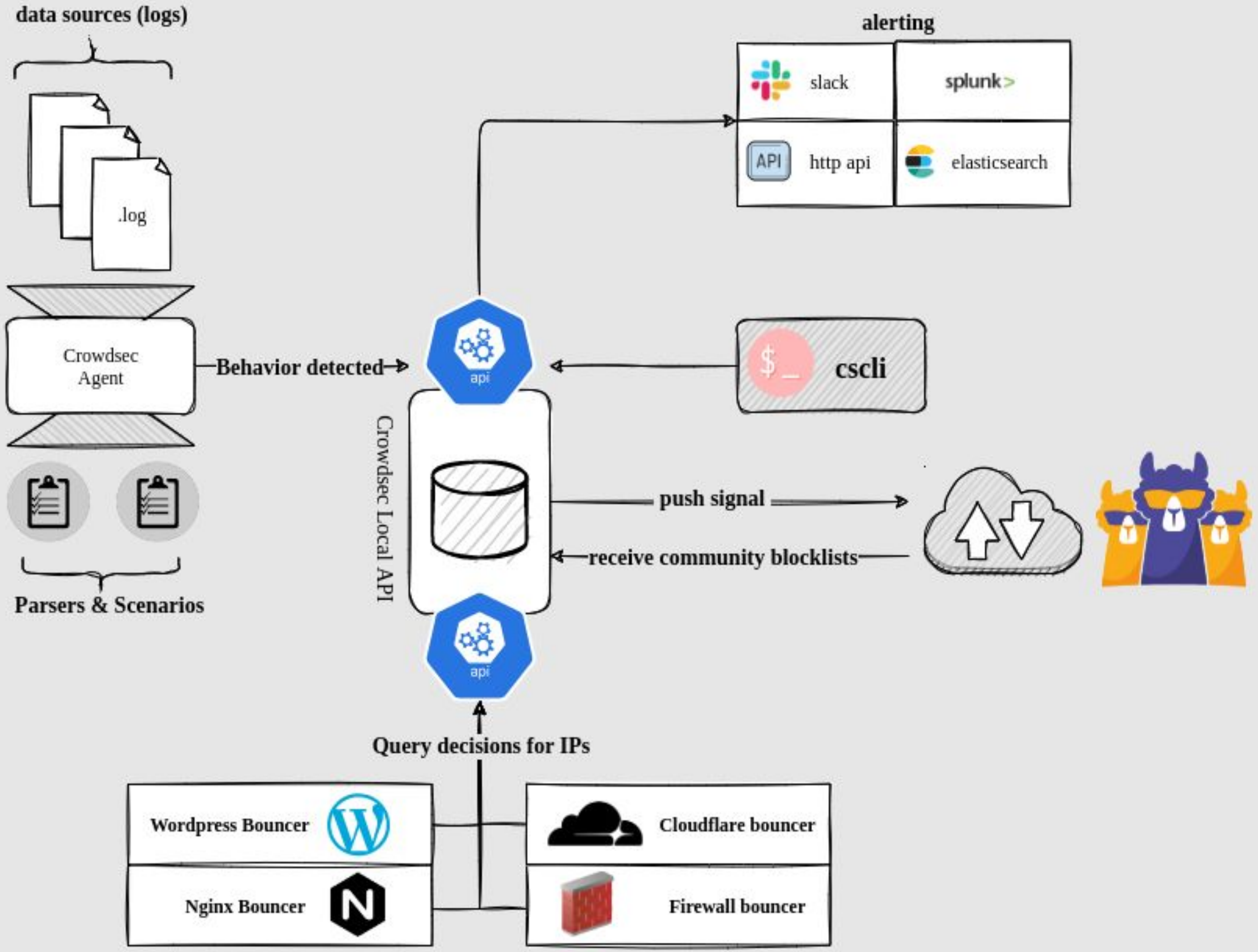
Helm, serverless etc.

Scales

Logs are great for sharding.
CrowdSec too

Portabilité

Debian/RPM/Docker/FreeBSD/
Windows



Run (nearly) everywhere

1

Linux distributions

2

Windows ?!!

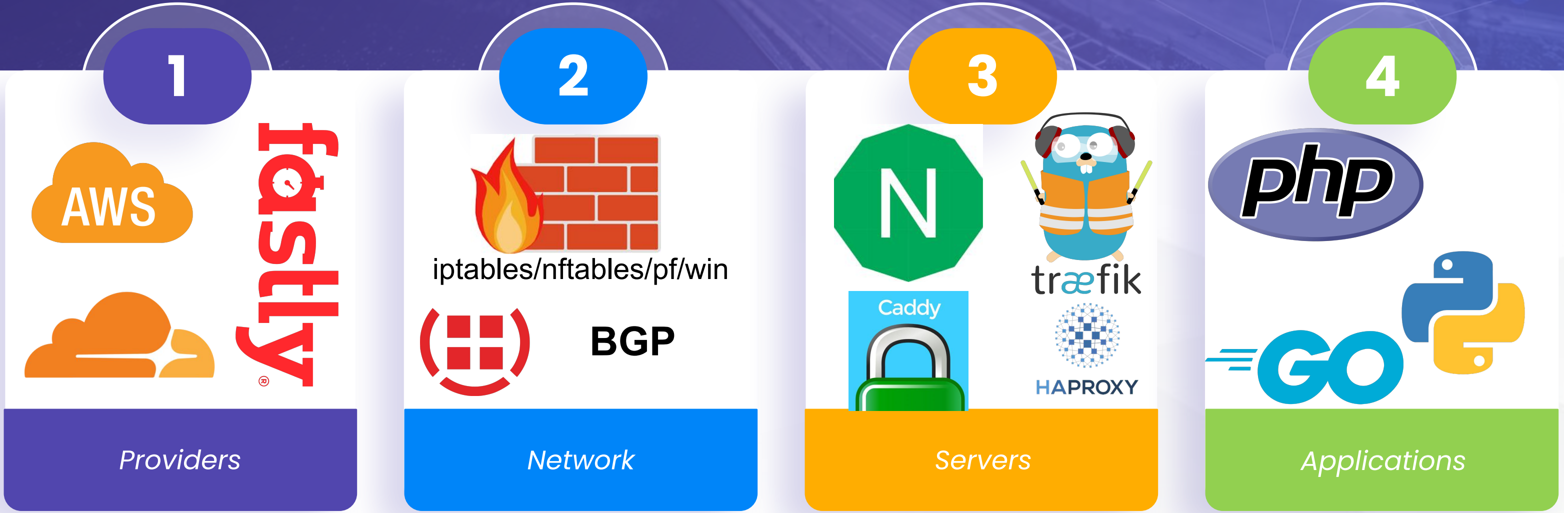
3

BSD

4

Containers

Bouncing at every level



1

AWS

fastly

Providers

2

iptables/nftables/pf/win

BGP

Network

3

Caddy

træfik

HAPROXY

Servers

4

php

GO

Applications

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.

We monetize access to CTI for those not sharing

Opened to contribution

Give... and thou shall receive.

CrowdSec

YOUR LOGS ARE *NEVER* EXPORTED

We only collect

- Timestamp
- Offending IP
- Behavior

GDPR
GENERAL DATA
PROTECTION REGULATION

YOU CAN CHOOSE NOT TO HAVE ANY ONLINE DEPENDENCY

We only monetize

- Fleet features
- Self monitoring & forensic
- API access (only for people not sharing)

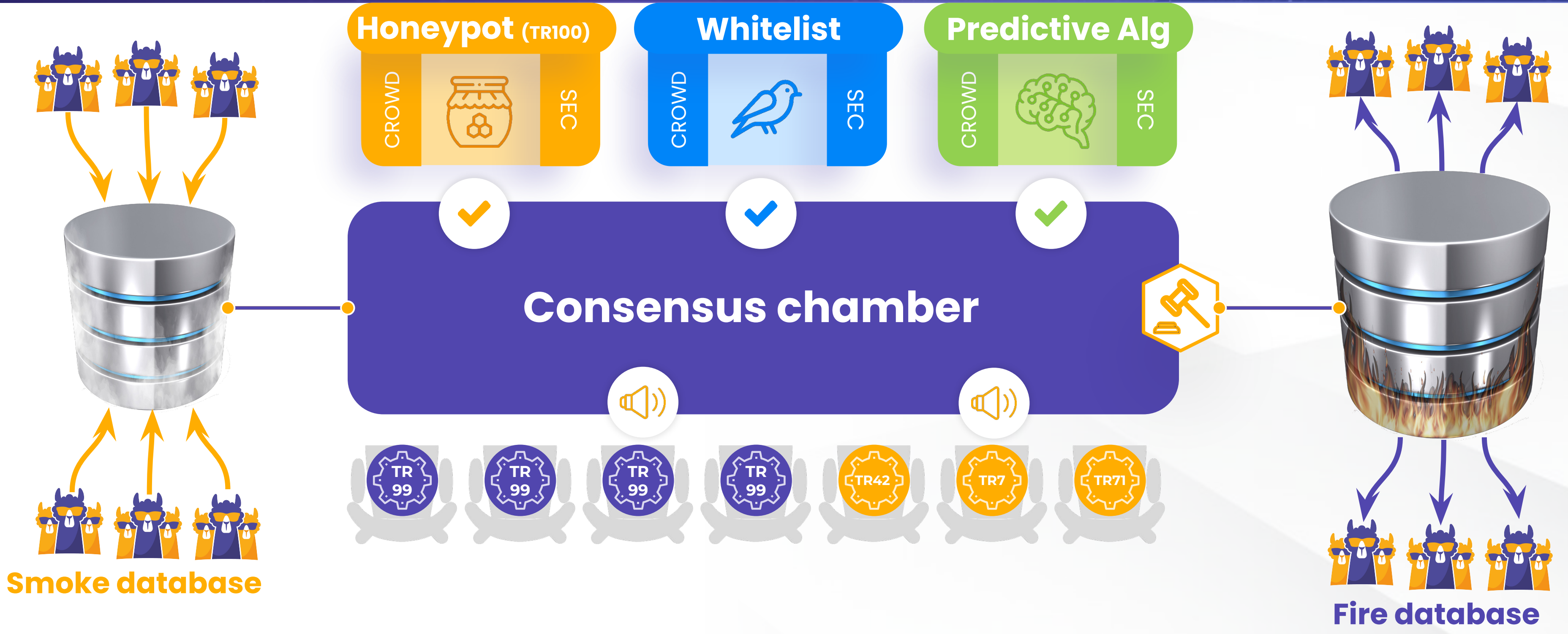
BAD IP?
Context is key

Time dependant

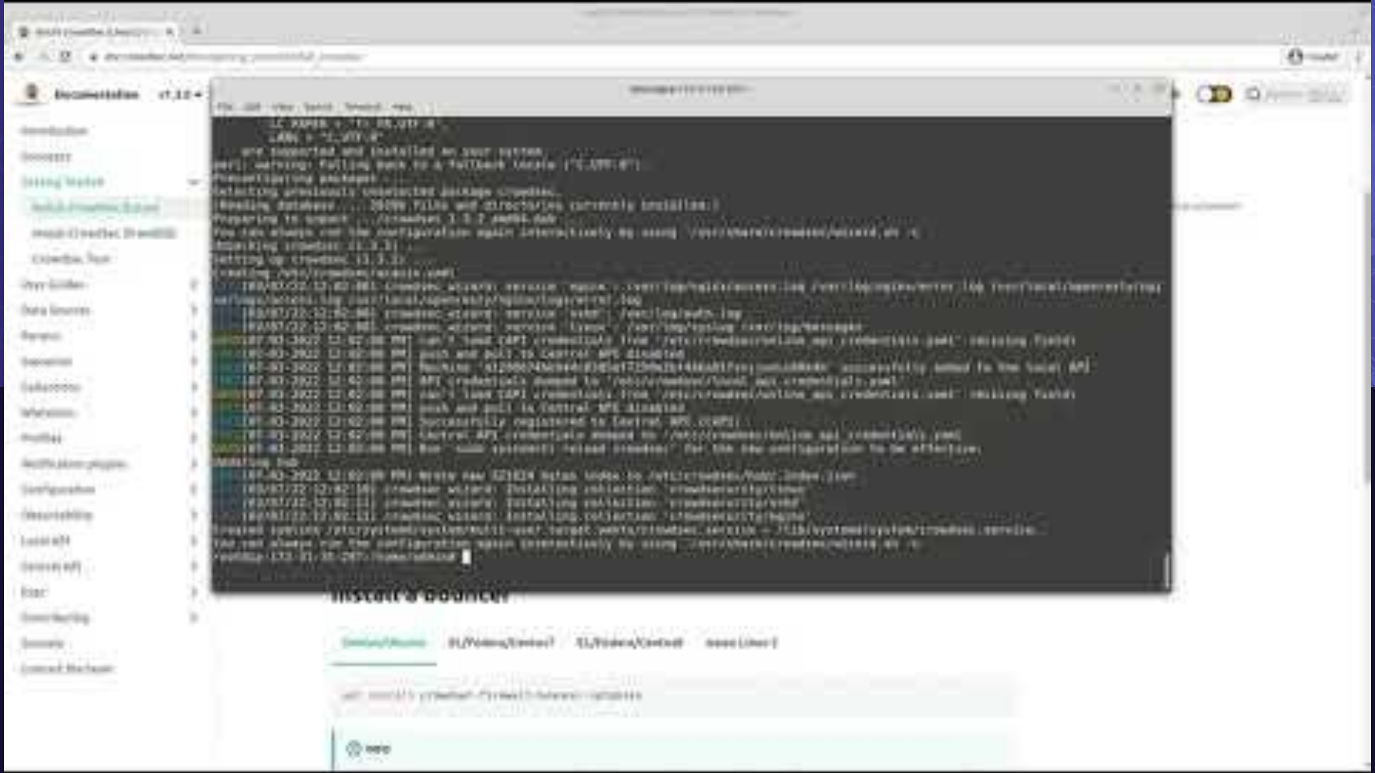
- A malicious IP was once clean
- It’s rogue only when a criminal owns it
- We detect it through its activity
- And it will be cleaned one day by its owner

Each IP is refreshed every 72 hours max

There is no fire without smoke



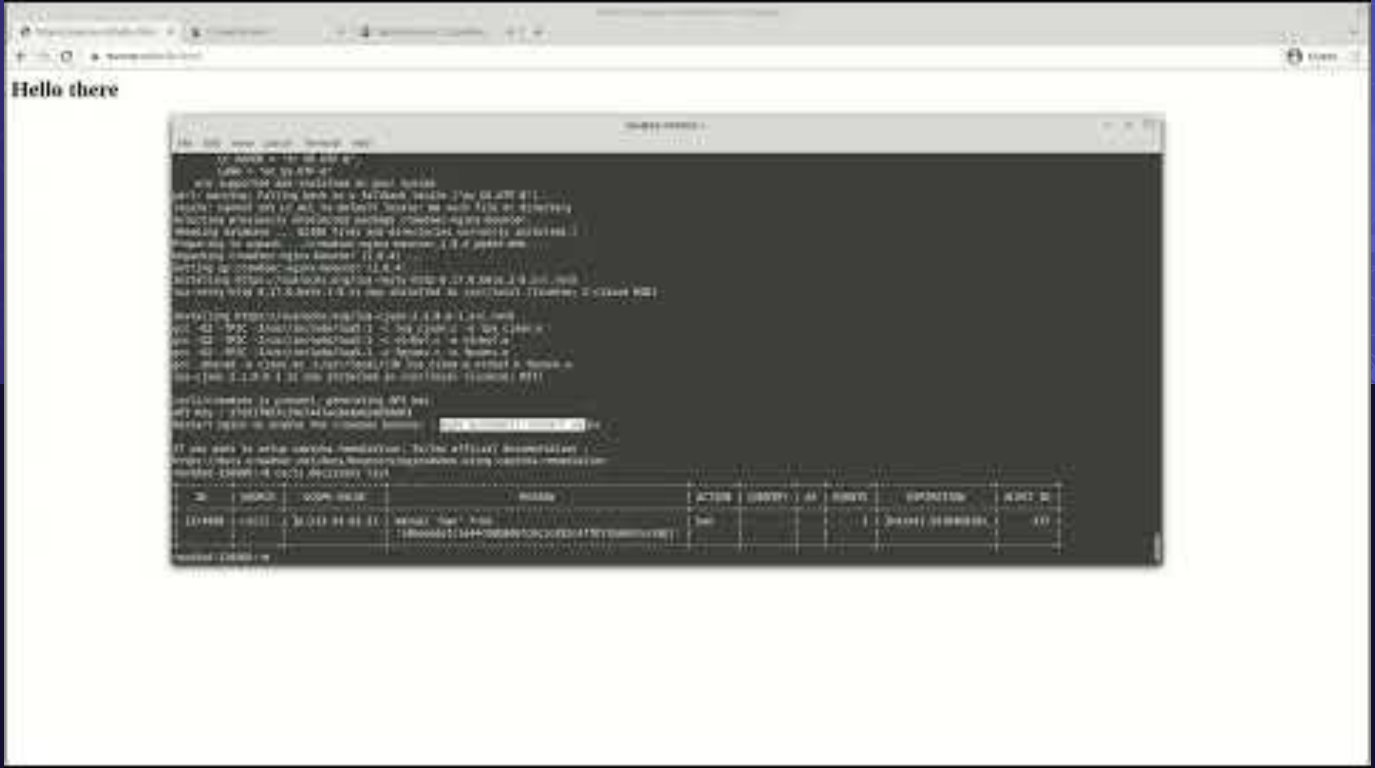
A demo?



```
        LC_PAPER = "fr_FR.UTF-8",
        LANG = "C.UTF-8"
    are supported and installed on your system.
perl: warning: Falling back to a fallback locale ("C.UTF-8").
Preconfiguring packages ...
Selecting previously unselected package crowdsec.
(Reading database ... 28096 files and directories currently installed.)
Preparing to unpack .../crowdsec_1.3.2_amd64.deb ...
You can always run the configuration again interactively by using '/usr/share/crowdsec/wizard.sh -c'
Unpacking crowdsec (1.3.1) ...
Setting up crowdsec (1.3.1) ...
Creating /etc/crowdsec/acquis.yaml
INFO[03/07/22 12:02:00] crowdsec_wizard: service 'nginx': /var/log/nginx/access.log /var/log/nginx/error.log /usr/local/openresty/nginx/logs/access.log /usr/local/openresty/nginx/logs/error.log
INFO[03/07/22 12:02:00] crowdsec_wizard: service 'sshd': /var/log/auth.log
INFO[03/07/22 12:02:00] crowdsec_wizard: service 'linux': /var/log/syslog /var/log/messages
WARN[07-03-2022 12:02:00 PM] can't load CAPI credentials from '/etc/crowdsec/online_api_credentials.yaml' (missing field)
INFO[07-03-2022 12:02:00 PM] push and pull to Central API disabled
INFO[07-03-2022 12:02:00 PM] Machine '[illegible]' successfully added to the local API
INFO[07-03-2022 12:02:00 PM] API credentials dumped to '/etc/crowdsec/local_api_credentials.yaml'
WARN[07-03-2022 12:02:00 PM] can't load CAPI credentials from '/etc/crowdsec/online_api_credentials.yaml' (missing field)
INFO[07-03-2022 12:02:00 PM] push and pull to Central API disabled
INFO[07-03-2022 12:02:00 PM] Successfully registered to Central API (CAPI)
INFO[07-03-2022 12:02:00 PM] Central API credentials dumped to '/etc/crowdsec/online_api_credentials.yaml'
WARN[07-03-2022 12:02:00 PM] Run 'sudo systemctl reload crowdsec' for the new configuration to be effective.
Updating hub
INFO[07-03-2022 12:02:00 PM] Wrote new 323824 bytes index to /etc/crowdsec/hub/.index.json
INFO[03/07/22 12:02:10] crowdsec_wizard: Installing collection 'crowdsecurity/linux'
INFO[03/07/22 12:02:11] crowdsec_wizard: Installing collection 'crowdsecurity/sshd'
INFO[03/07/22 12:02:11] crowdsec_wizard: Installing collection 'crowdsecurity/nginx'
Created symlink /etc/systemd/system/multi-user.target.wants/crowdsec.service → /lib/systemd/system/crowdsec.service.
You can always run the configuration again interactively by using '/usr/share/crowdsec/wizard.sh -c'
root@ip-172-31-30-207:/home/admin# 
```

Install a bouncer

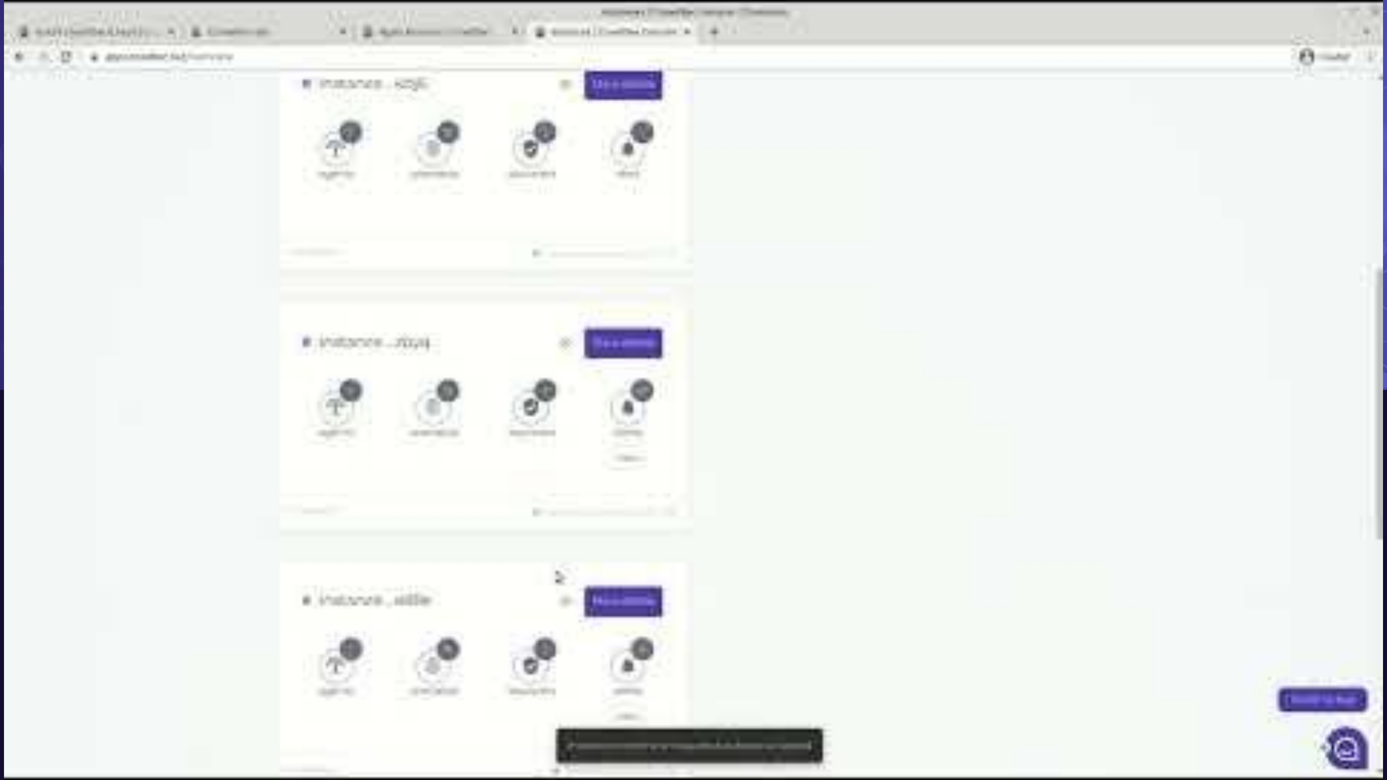
```
apt install crowdsec-firewall-bouncer-iptables
```

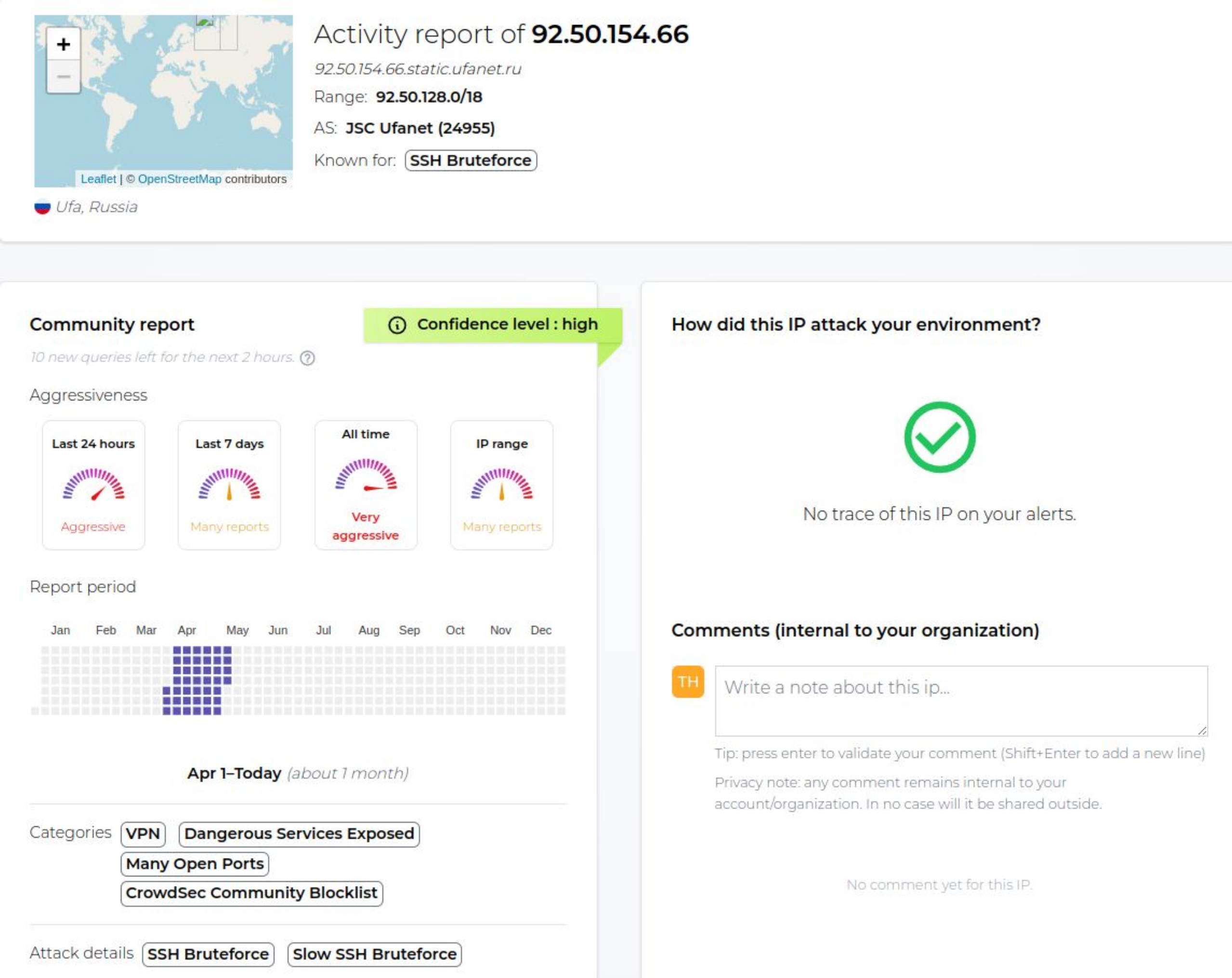


Hello there

```
[illegible]
Restart nginx to enable the crowdsec bouncer : [illegible]

If you want to setup captcha remediation, follow official documentation :
[illegible]
[illegible] cscli decisions list
+--------+--------+-------------+--------------------+--------+---------+----+--------+------------+----------+
|   ID   | SOURCE | SCOPE:VALUE |       REASON       | ACTION | COUNTRY | AS | EVENTS | EXPIRATION | ALERT ID |
+--------+--------+-------------+--------------------+--------+---------+----+--------+------------+----------+
| [illegible] | cscli | [illegible] | [illegible] | ban |   |   |   1 | [illegible] | [illegible] |
+--------+--------+-------------+--------------------+--------+---------+----+--------+------------+----------+
```


instance...
instance...
instance...



Activity report of **92.50.154.66**

92.50.154.66.static.ufanet.ru

Range: **92.50.128.0/18**

AS: **JSC Ufanet (24955)**

Known for: **SSH Bruteforce**

Ufa, Russia

Community report

ⓘ **Confidence level : high**

10 new queries left for the next 2 hours. ?

Aggressiveness

Last 24 hours	Last 7 days	All time	IP range
Aggressive	Many reports	Very aggressive	Many reports

Report period

Apr 1–Today *(about 1 month)*

Categories **VPN** **Dangerous Services Exposed** **Many Open Ports** **CrowdSec Community Blocklist**

Attack details **SSH Bruteforce** **Slow SSH Bruteforce**

How did this IP attack your environment?

✓

No trace of this IP on your alerts.

Comments (internal to your organization)

TH Write a note about this ip...

Tip: press enter to validate your comment (Shift+Enter to add a new line)

Privacy note: any comment remains internal to your account/organization. In no case will it be shared outside.

No comment yet for this IP.

SAFER TOGETHER

https://crowdsec.net