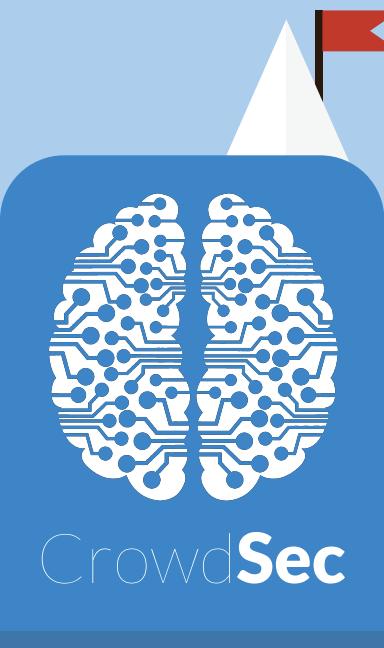


Safer
Together.



Open Source

Collaborative

Dynamic

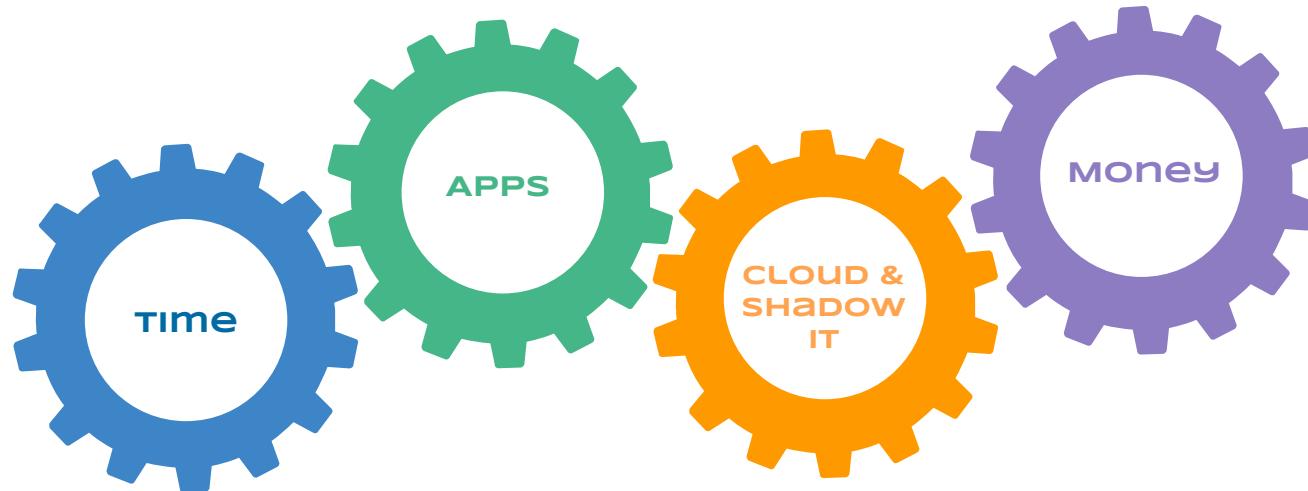
Security engine

Why

“Cyber defense collaboration is the space race of our generation.”

Williams David

Not solved, for a reason



The next generation solution

Real Time

Decoupled
detection &
remediation

Crowd intel
sharing

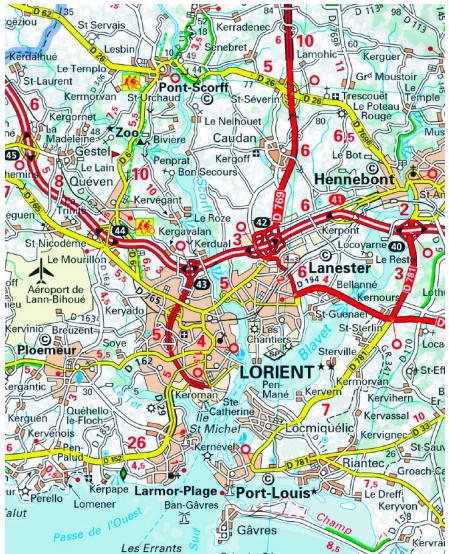


Reputation
assessment

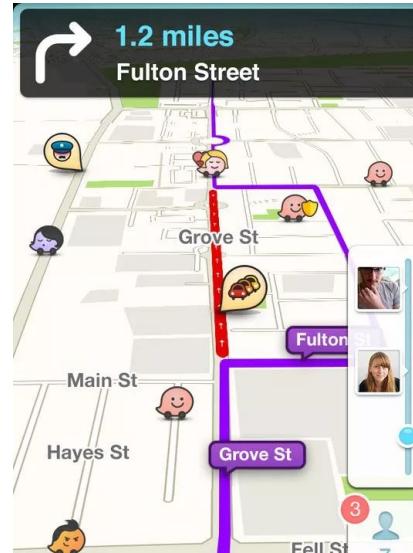
Behavior
assessment



Crowd is the remedy to large scale hacking



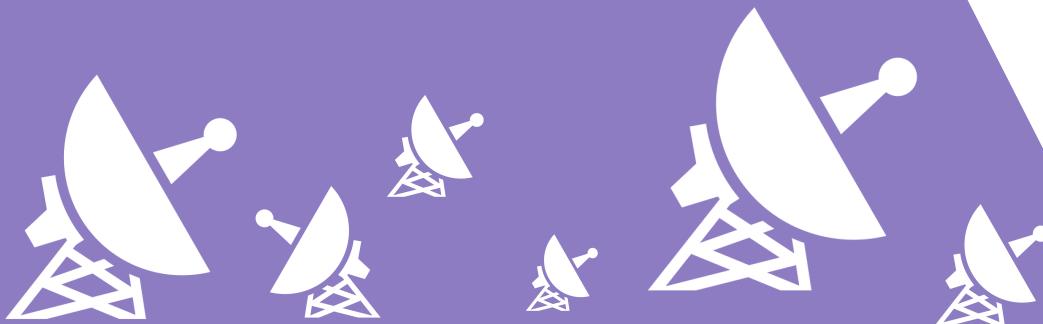
Our parents used this.



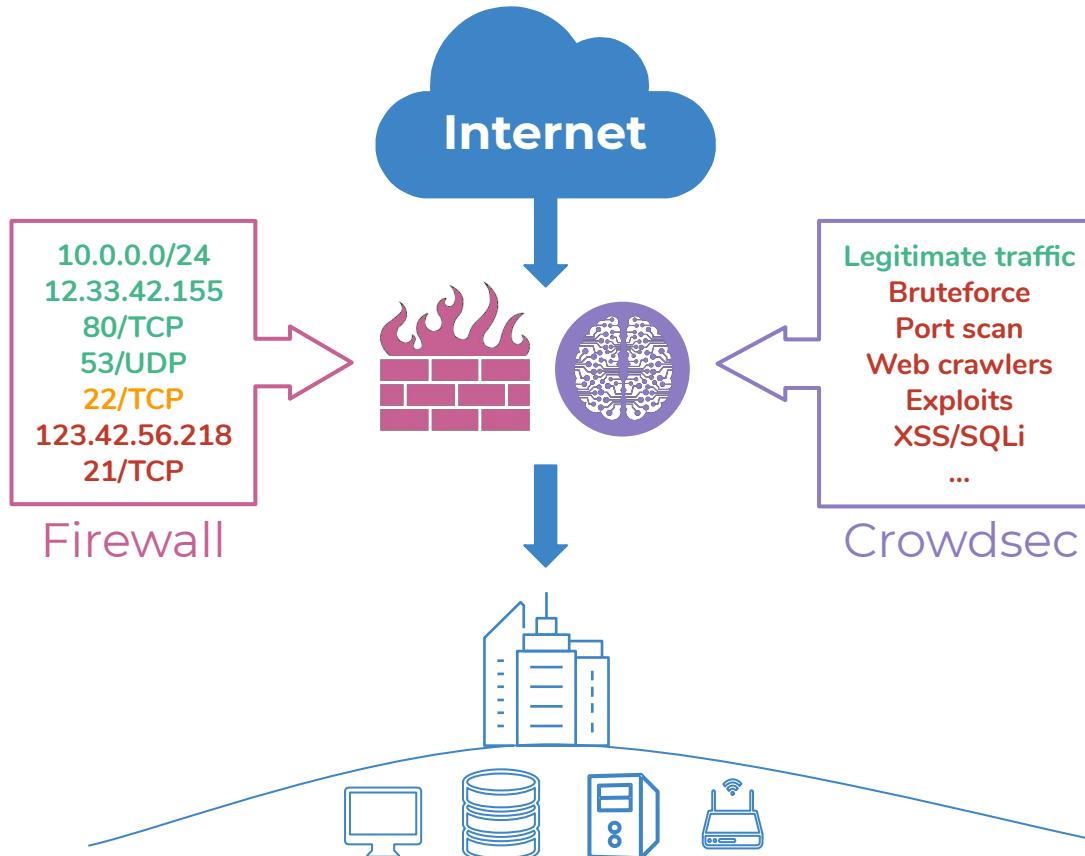
We use this, because it's free, real time, fed by community and gives traffic insights.

Our goal is to become,
“the Waze of Firewalls”

Building the detection Network with Open Source



Crowdsec analyses behavior, not IP:port



Crowdsec is as simple as 1,2,3,4

Collect data where you want...

Logs Community

SIEM 3rd Party

1

Behavior scenarii detect hack attempts

Ours Yours

Community

2

React the way you want, where you want

Block Captcha

Limit rights or speed 2FA/MFA

3

Share your sightings and get informed

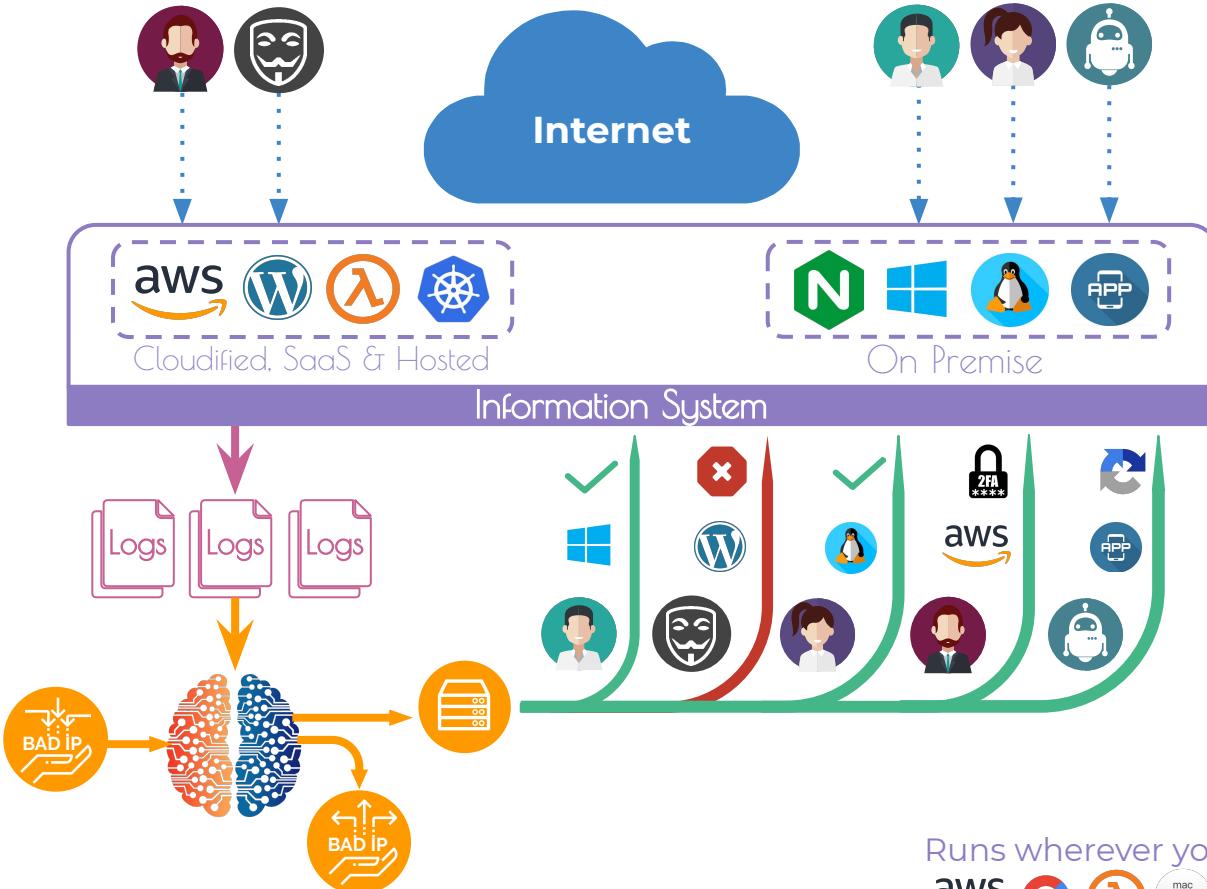
BAD IP

4

DEMO TIME



Detecting & enforce

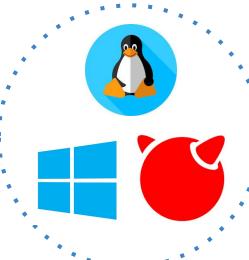


Blockers : Protection at any level



- Relies on local DB fed by API
- Reusable libraries for integration in most components.
- Counter-measure is defined by plugin : ban, slow, captcha ...

Simple design allows integration at any level of the stack.



Open Source licensing

1 | Open Source

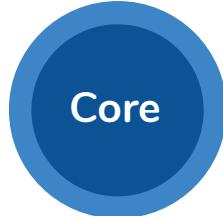
2 | Free (to use, copy, modify)

3 | Free of charge

4 | Can be embedded

5 | No usage limit

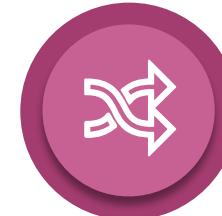
6 | Must name author



MIT License.
Core contributors
abandon rights



Configurations
stays their authors
properties



Blockers stay their
authors properties

Crowdsec

Non elitist security

Easy setup

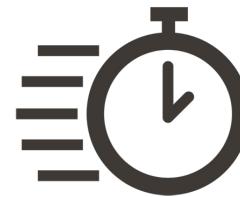


DevOPS in their deployment environment

Developers through a Library or direct API call

Sysadmins

IT engineers on an infrastructure

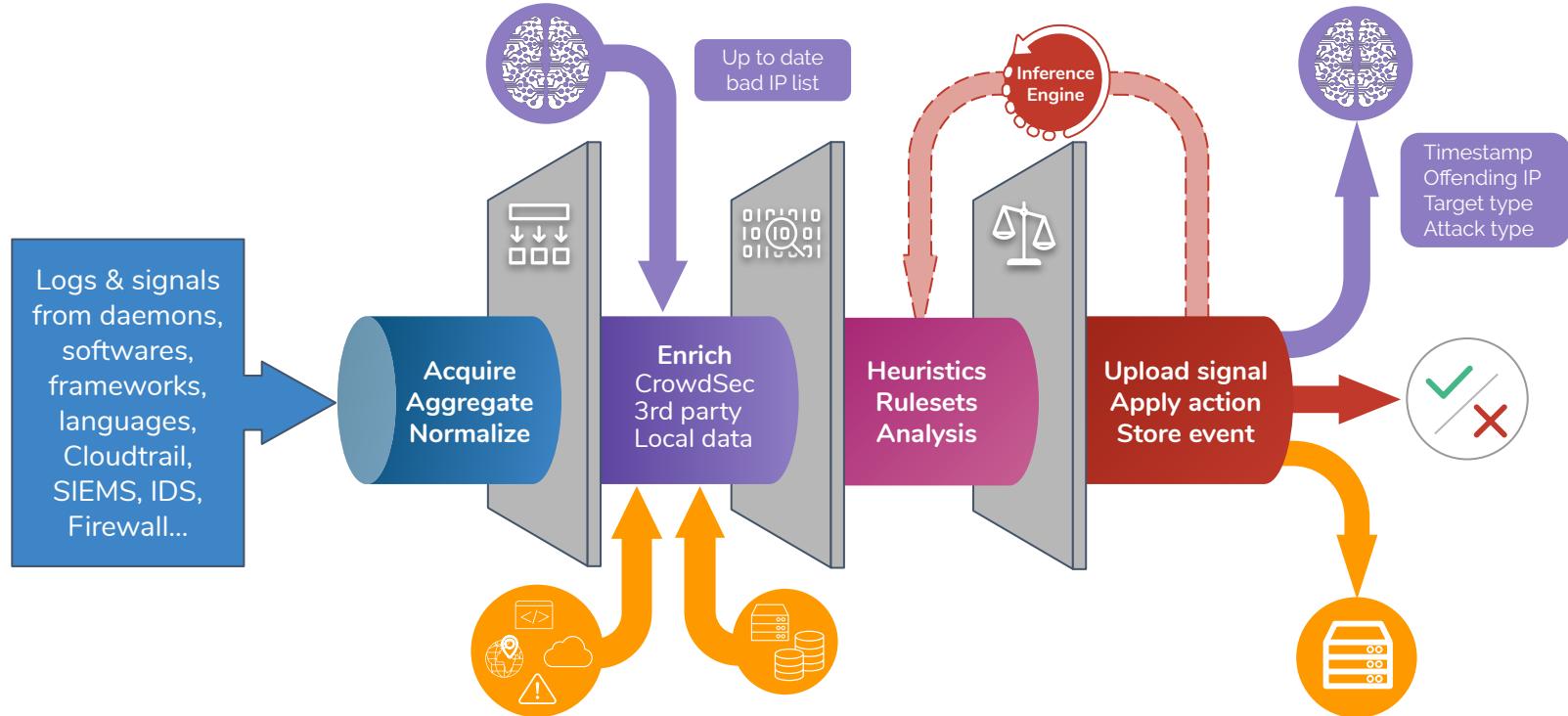


Operational install in less than 5 minutes



Heavily assisted setup, no technical entry barrier

CrowdSec



Coded in Golang runs on all major OS



Engineered for Cloud, Kubes, VMs

Configuration Hub



One place to find
community
scenarios.

One click to
enable them.

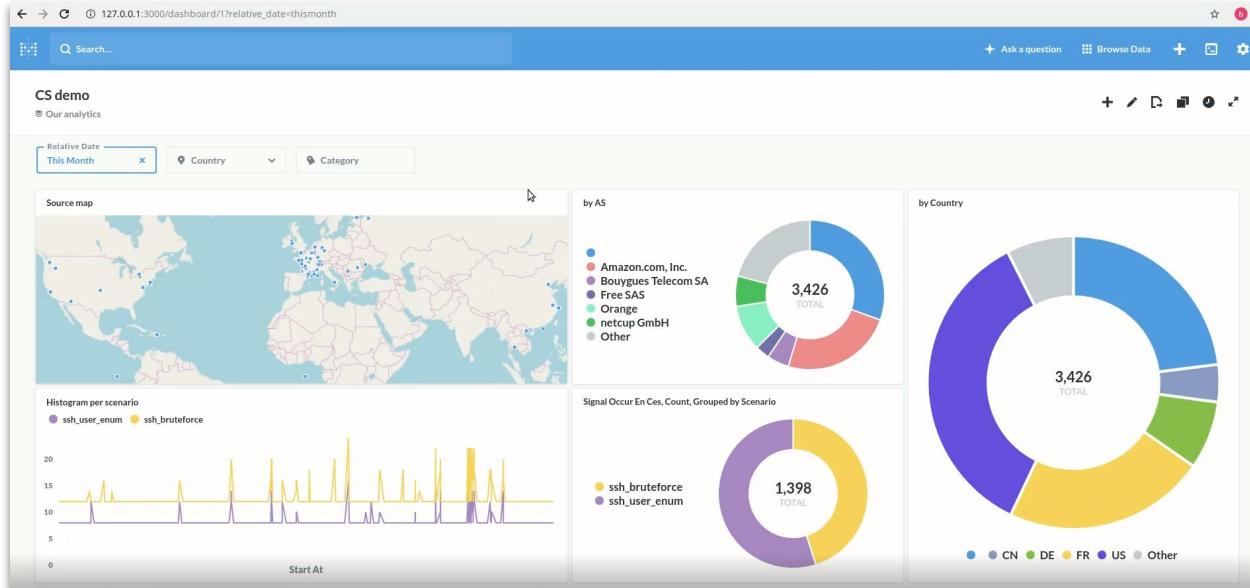
The screenshot shows a web interface for the CrowdSec Configuration Hub. At the top, there's a navigation bar with the CrowdSec logo and a 'Hub' button, and a 'Browse' link on the right. Below the header, a card displays the repository information for 'crowdsecurity / cs-nginx-blocker'. It includes a green hexagonal icon with a white 'N', the repository name, a brief description 'nginx blocker', a star icon with '0' downloads, a download icon with '9 DOWNLOADS', and a 'VERSION: v0.0.1' link. Below this card is a larger box labeled 'Info' with an info icon. It contains a 'Download URL' field with the value '<https://github.com/crowdsecurity/cs-nginx-blocker/releases/download/v0.0.1>'. At the bottom of this box are 'Tags' and 'BLOCKERS' buttons.

Visualisation

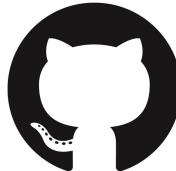


One command to access reporting.

Relying on metabase.



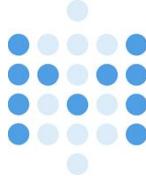
Technical takeaways : Crowdsec



Written in golang, community driven



Prometheus



Observability, for users and OPs



docker



kubernetes

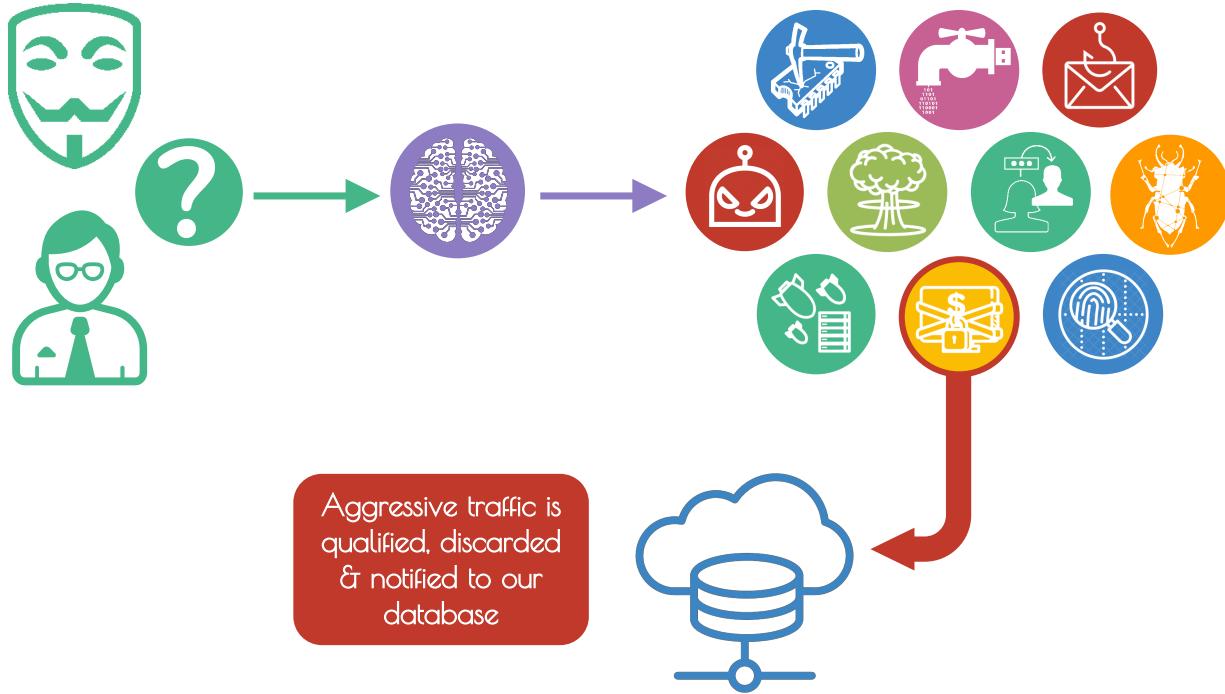


Lightweight and declarative for versatile deployment

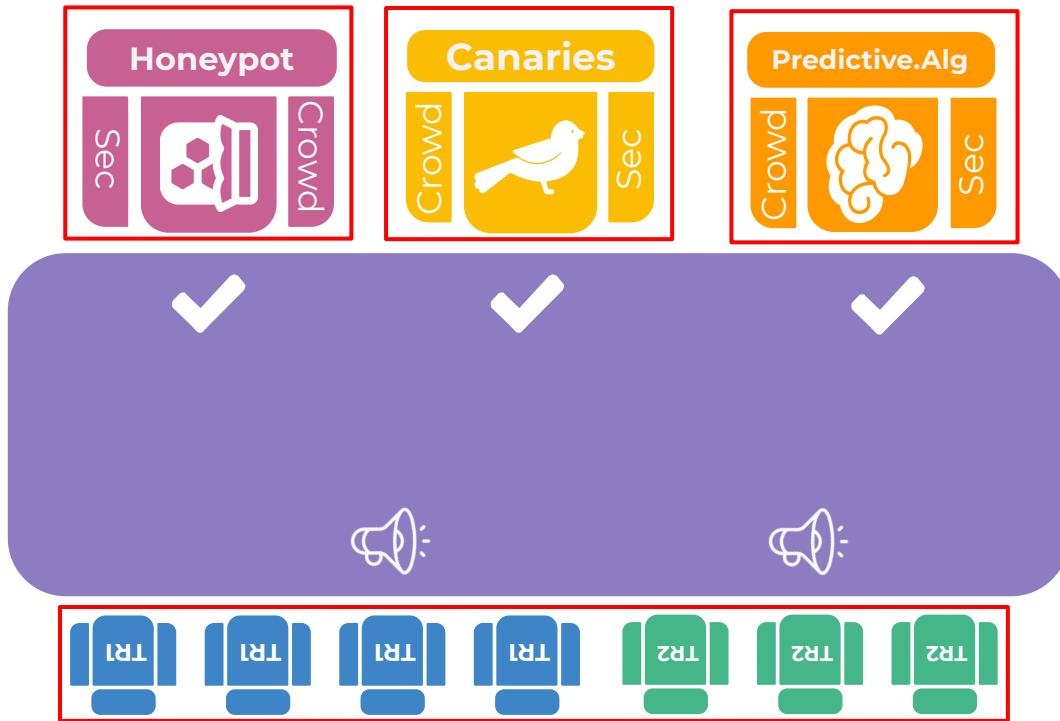
Crowd fed decisions

Stronger together

One stone, ten birds



The secret sauce: Consensus



You will generate False Positives



We broadcast “canaries”, IP whitelists of trustable actors (ie so that you won’t ruin your SEO by banning Google by mistake)



If a scenario (community or Crowdsec one) kicks a whitelisted IP, it is marked as potentially triggering FP.



Those IP addresses are crowdsourced as well, on our Github project, and curated by our staff, to diversify sources



If a previously trusted actor changes behavior, we’ll notice it by having reliable scenarii being triggered by those, now evil, canaries

Thank
you

*Only the crowd can defeat
mass scale hacking...*



Crowd
Security

Crowdsec.net

github.com/crowdsecurity/crowdsec