Safer Together

Open Source | IPS & | Participative CTI | Engine

Forsvar din infrastruktur ved brug af open source og crowdsourcing

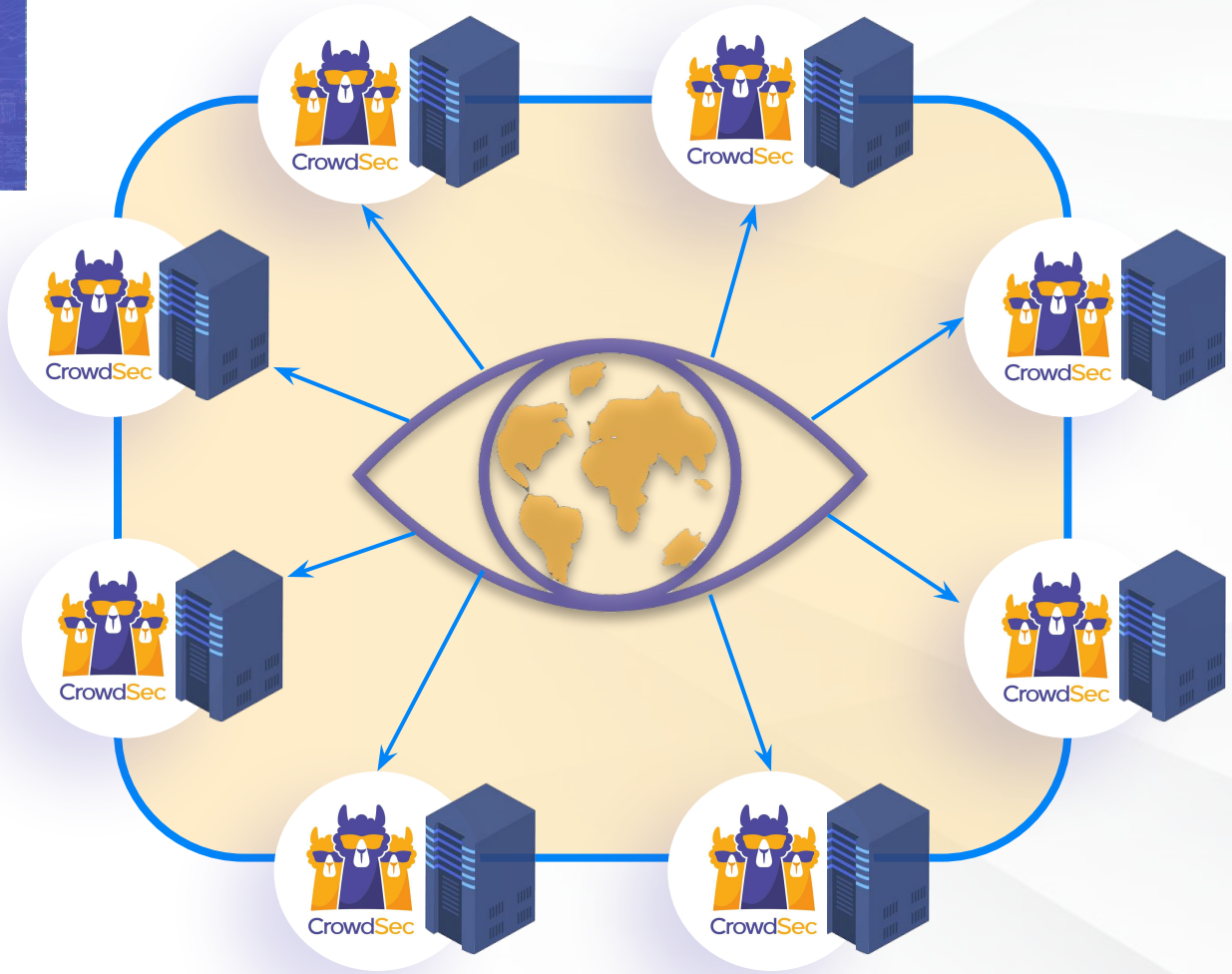
Hvem er jeg?

Klaus Agnoletti
Head of Community hos CrowdSec
17 år bredt med infosec - primært teknisk

Arbejder i spændingsfeltet mellem teknik, marketing og community

CrowdSec

Vi bygger Cybersikkerheds svar på Waze



Lokal IPS
Global CTI

Cybersikkerhed *er ikke* et kompliceret problem

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

(Det var *det her* til gengæld)

Det er komplekst!

(*Som at sende folk til månen*)

Siden 90'erne har vi set på cybersikkerhed som et kompliceret problem

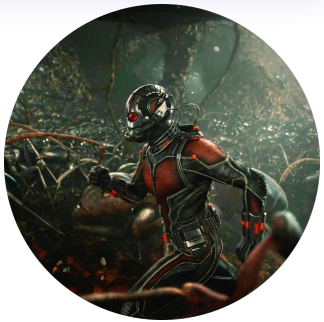
Vi overmander!

FAILED

Vi overlister!

FAILED

Skal vi bringe os i overtal i stedet?



Hvad med at samarbejde?

I stedet for et komplekst...

CrowdSec

Cybersikkerhed
Er ikke et spørgsmål om midler

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

De andre..

CrowdSec

Ikke løst... Det er der en grund til

Tid

Perimeter

Penge

CrowdSec

“Borg strategien” hører til i 80’erne – ligesom Sony Walkman

Enheder spredt over mange leverandører

Hvem kan man stole på?

Crowdsourcing og “reputation” er måden at gøre det på!

CrowdSec

Massively
Participative
IPS

1

Syslogd, journald, Cloudtrail, filer

Forbind de ønskede datakilder

2

vores

dit

community

***Agenten** opdager trusler baseret på 'behavior' scenarier*

3

$ _

***Bounceren** neutraliserer truslerne som det passer dig*

4

BAD IP

Del med communityet

Massively
Participative
IPS

1

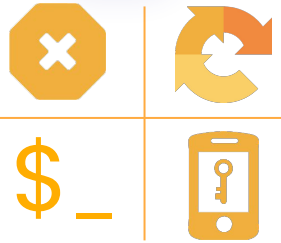
Syslogd, journald, Cloudtrail, filer

Forbind de ønskede datakilder

2

***Agenten** opdager trusler baseret på 'behavior' scenarier*

3



***Bounceren** neutraliserer truslerne som det passer dig*

4

Del med fællesskabet

BEHAVIOR ENGINE = CYBERSEC HYGIENE

Alt genererer logs i dag. Hvis du kan beskrive det angrebsmønster du leder efter kan CrowdSec finde det.

CrowdSec

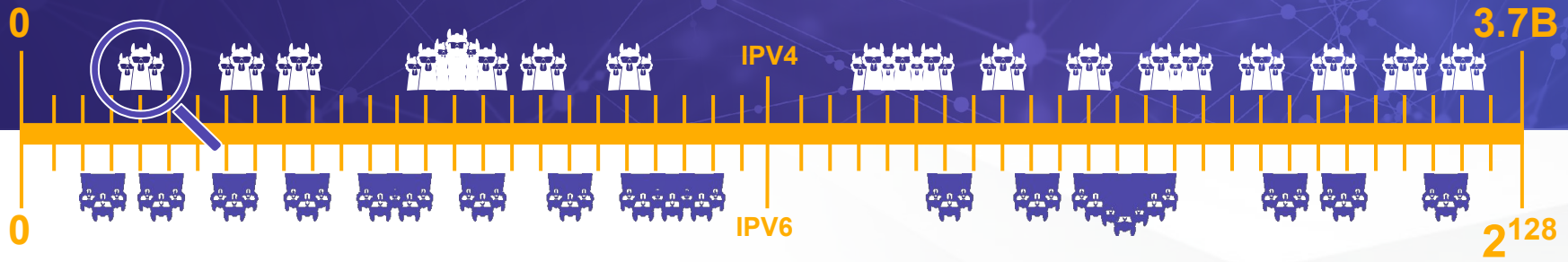
En KRIG om ressourcer

For Hackere giver stjålne IP numre anonymitet

CrowdSec

Vort community skræller lagene af ét efter ét

Crowd sourced Cyber Threat Intelligence



I stedet for at køre simulerede services (honeypots) på få hundrede servere på et par forskellige cloud-udbydere -

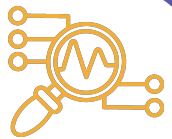
Tøjler vi kræfterne fra tusindvis af rigtige servere der kører rigtige server på mange forskellige miljøer og forbindelser

CrowdSec

Frit. Altid. Punktum.

01	**OPEN SOURCE (MIT)**
02	**FRIT** (*at bruge, kopiere, modificere*)

MIT licens.
Så frit som det kan være.



Transparent, auditérbart og troværdigt.

Vi tager penge for adgang til CTI til dem der ikke deler

Alle kan bidrage!

CrowdSec

BAD IP?
Det handler om kontekst!

Tidsafhængigt

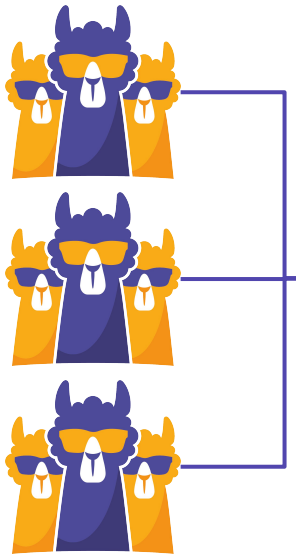
IP numre er kun ondsindede så længe en hacker ejer det - og engang bliver de 'clean' igen

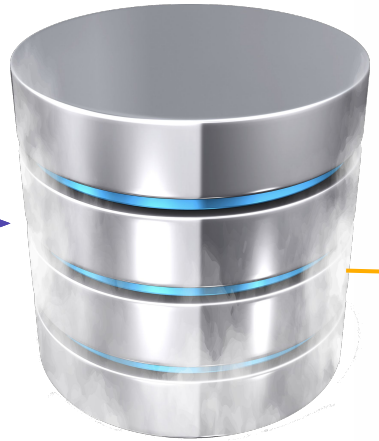
Ingen IPs lever mere end 72 timer i databasen

CrowdSec

Ingen røg uden ild

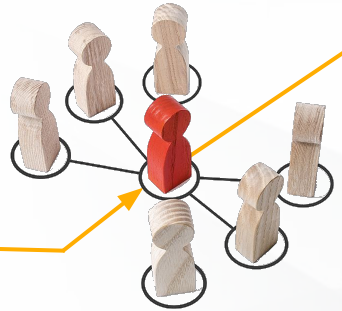
Agenter sender ondsindede IPs til **"Smoke" DB**

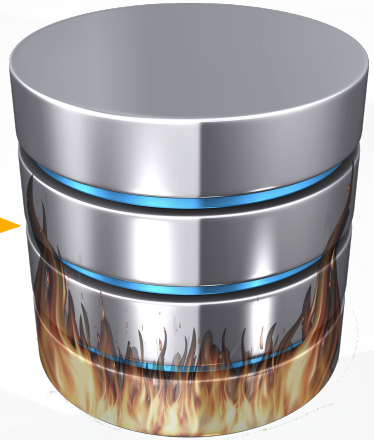




Mål: Fød CTI, SIEM, SOC

Hvis netværket opnår ***konsensus*** tilføjes IP nummeret til **"Fire" DB**





Mål: Instruér alle bouncers i at behandle dette IP som ondsindet.

Din log eksporteres aldrig!

CrowdSec opsamler kun:

CrowdSec

CrowdSec overtager verdens herredømmet - sammen med dig 😀

CrowdSec

>20.000 installationer over hele verden
I 110 lande og på 6 kontinenter

700.000 ondsindede IPs detekteret
Over 12 måneder

Bruges på tværs af brancher
Hosting virksomheder, universiteter, forskningscentre, kommuner (og tilsvarende) etc.
Har blokeret HTTP DDoS botnets, Credit card stuffers, etc.

Mål i 2024:
1.000.000 maskiner i vores CTI netværk

Så hvordan kommer jeg i gang?

CrowdSec

CrowdSec docs

- https://doc.crowdsec.net/

CrowdSec

Agents


Linux


FreeBSD


Docker


k8s


OpenWRT


Windows

CrowdSec

Bouncers

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

CrowdSec

Hvis du sidder fast

https://crowdsec.net/blog/
https://discourse.crowdsec.net/

CrowdSec

Vil du vide mere?

Se min talk fra ShellCon
Væsentligt mere detaljeret

CrowdSec

Spørgsmål?

Mr Reputation

Mr Behavior

Vi overvinder cyberbanditterne sammen!

Du er velkommen til at række ud

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

Send mig en mail:
klaus@crowdsec.net

CrowdSec