

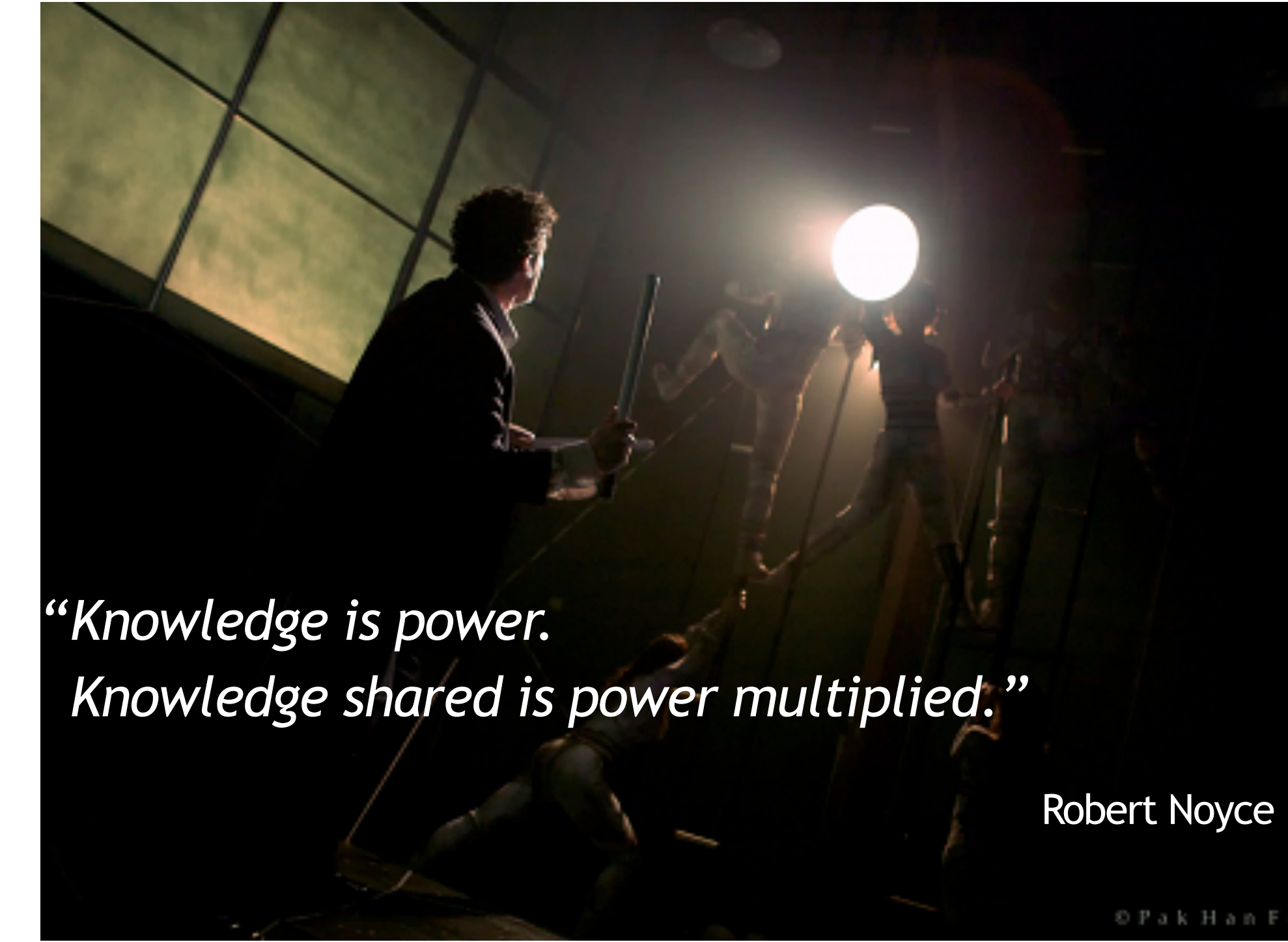


CERT.be
The Federal Cyber Emergency Team

Proposal for a new model for information sharing between CSIRTs

Ir. David Durvaux - Security Analyst
Christian Van Heurck - Coordinator

24th annual FIRST conference - Malta - 17-22 June 2012



*“Knowledge is power.
Knowledge shared is power multiplied.”*

Robert Noyce

About CERT.be and us

CERT.be

The federal cyber emergency team

a service of Fedict
operated by Belnet

Agenda

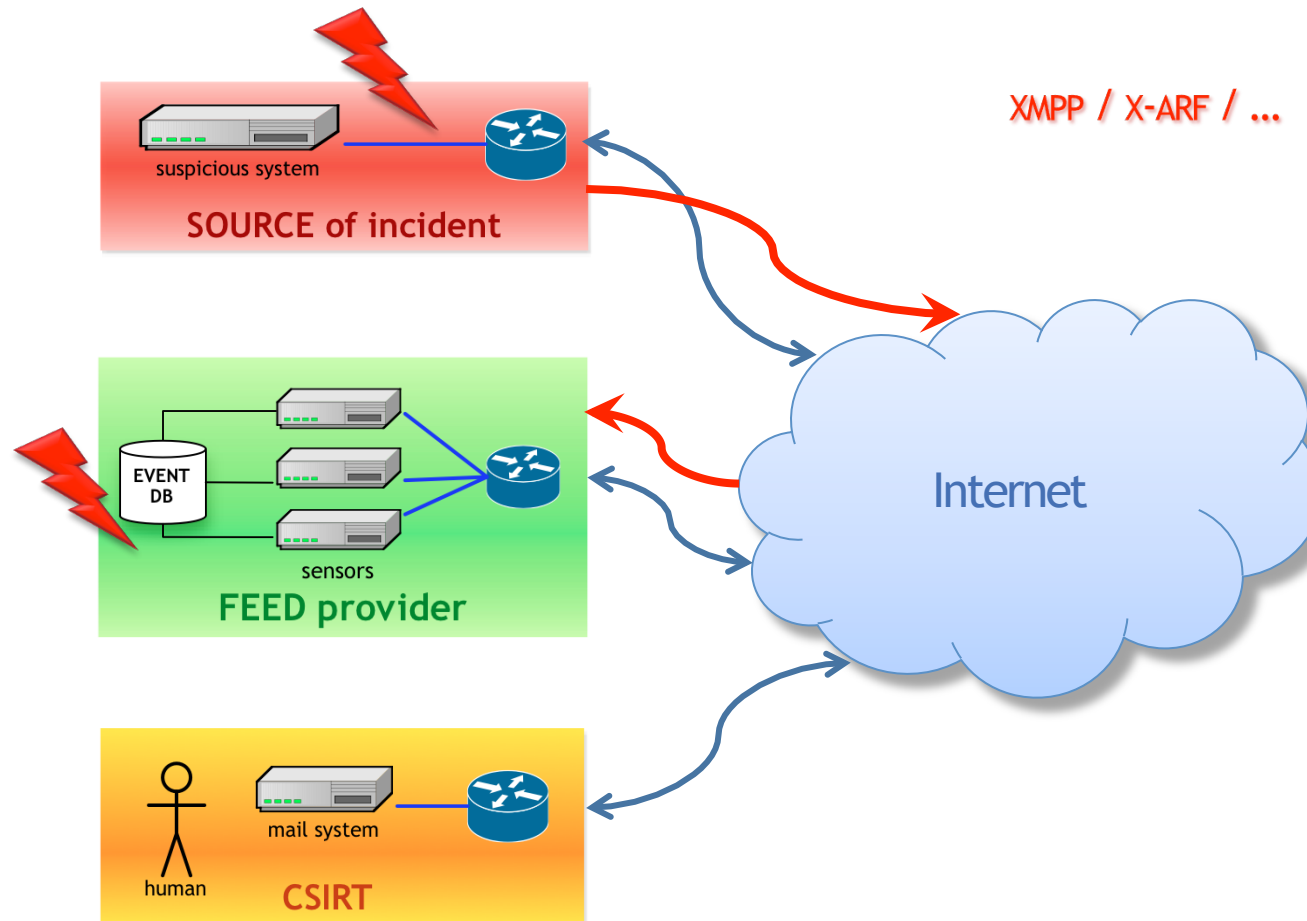
- 1 Current situation**
- 2 Proposal for a new model for sharing**
- 3 New issues**
- 4 Sharing time = Q&A**

Propagation time

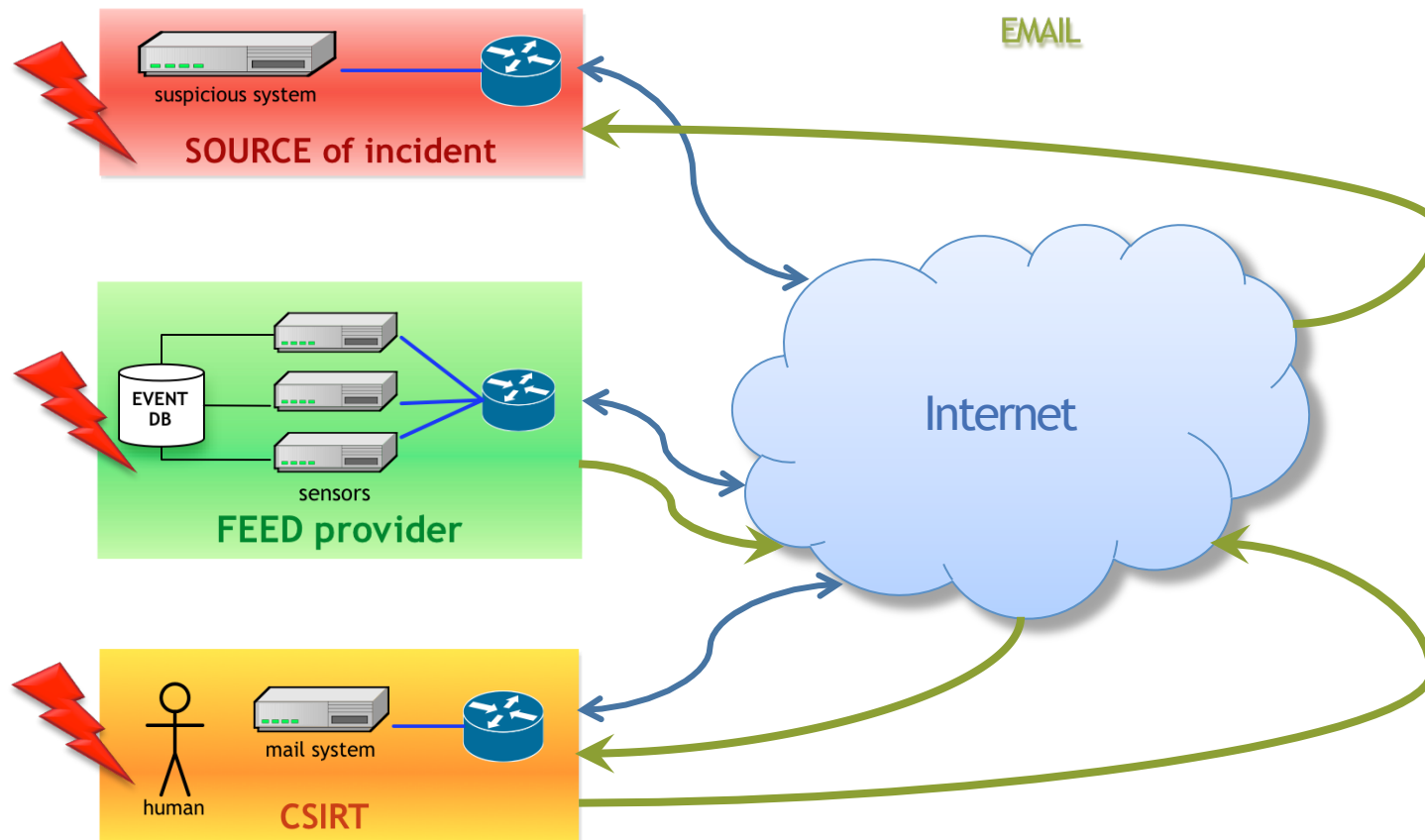
- **Internet delay: milliseconds**

```
Terminal — bash — 69x31
Last login: Fri May 18 15:34:20 on ttys001
You have mail.
Christian-Van-Heurcks-MacBook-Pro:~ christian$ ping cert.be
PING cert.be (193.190.198.61): 56 data bytes
64 bytes from 193.190.198.61: icmp_seq=0 ttl=56 time=15.555 ms
64 bytes from 193.190.198.61: icmp_seq=1 ttl=56 time=15.219 ms
64 bytes from 193.190.198.61: icmp_seq=2 ttl=56 time=14.995 ms
^C
--- cert.be ping statistics ---
3 packets transmitted, 3 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 14.995/15.256/15.555/0.230 ms
Christian-Van-Heurcks-MacBook-Pro:~ christian$ ping cert.at
PING cert.at (83.136.33.148): 56 data bytes
64 bytes from 83.136.33.148: icmp_seq=0 ttl=48 time=54.930 ms
64 bytes from 83.136.33.148: icmp_seq=1 ttl=48 time=53.603 ms
64 bytes from 83.136.33.148: icmp_seq=2 ttl=48 time=54.256 ms
^C
--- cert.at ping statistics ---
3 packets transmitted, 3 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 53.603/54.263/54.930/0.542 ms
Christian-Van-Heurcks-MacBook-Pro:~ christian$ ping first.org
PING first.org (72.3.219.184): 56 data bytes
64 bytes from 72.3.219.184: icmp_seq=0 ttl=40 time=125.394 ms
64 bytes from 72.3.219.184: icmp_seq=1 ttl=40 time=124.970 ms
64 bytes from 72.3.219.184: icmp_seq=2 ttl=40 time=124.729 ms
^C
--- first.org ping statistics ---
3 packets transmitted, 3 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 124.729/125.031/125.394/0.275 ms
Christian-Van-Heurcks-MacBook-Pro:~ christian$
```

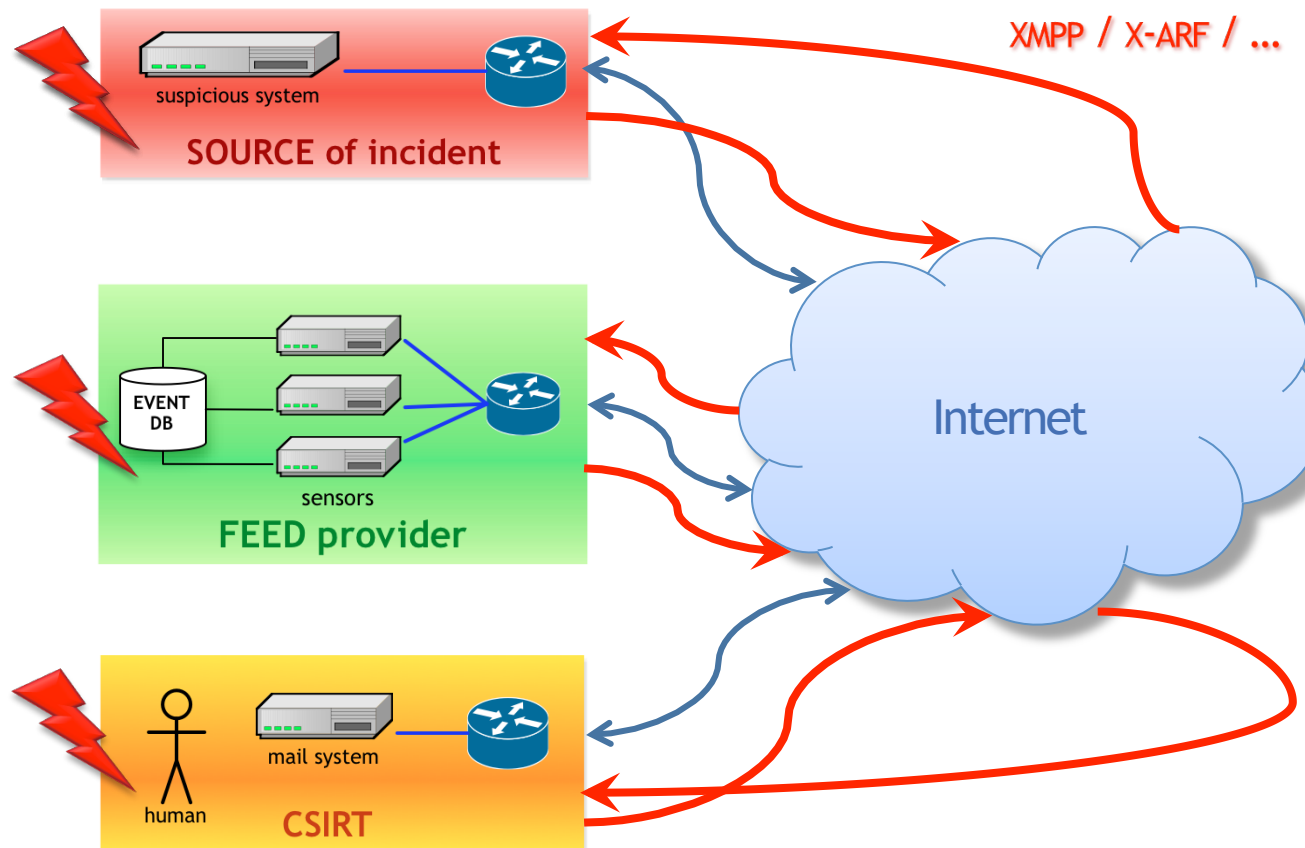
Propagation time: milliseconds



Propagation time: days to weeks



Propagation time: back to milliseconds



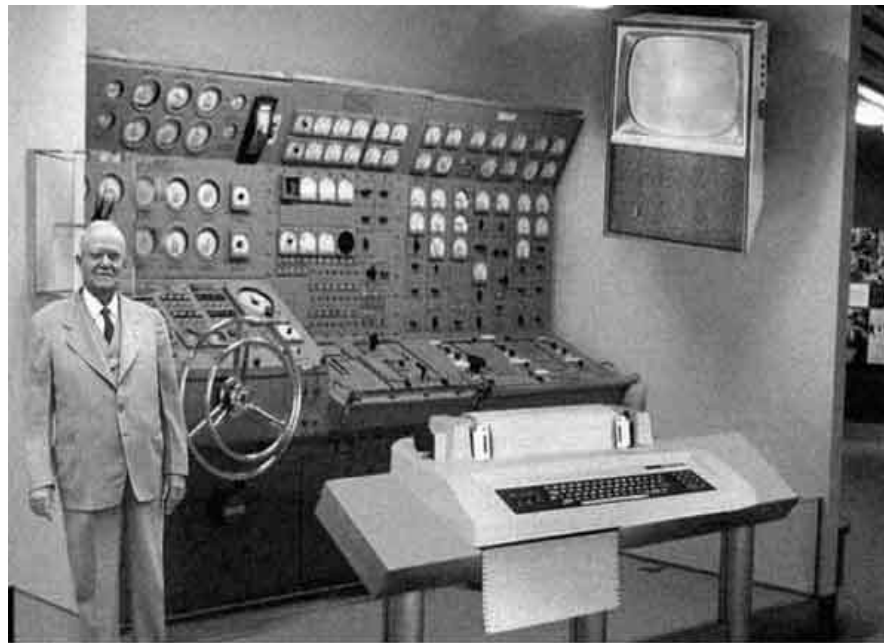
Propagation time: back to seconds

We need to

SHARE

more efficiently!

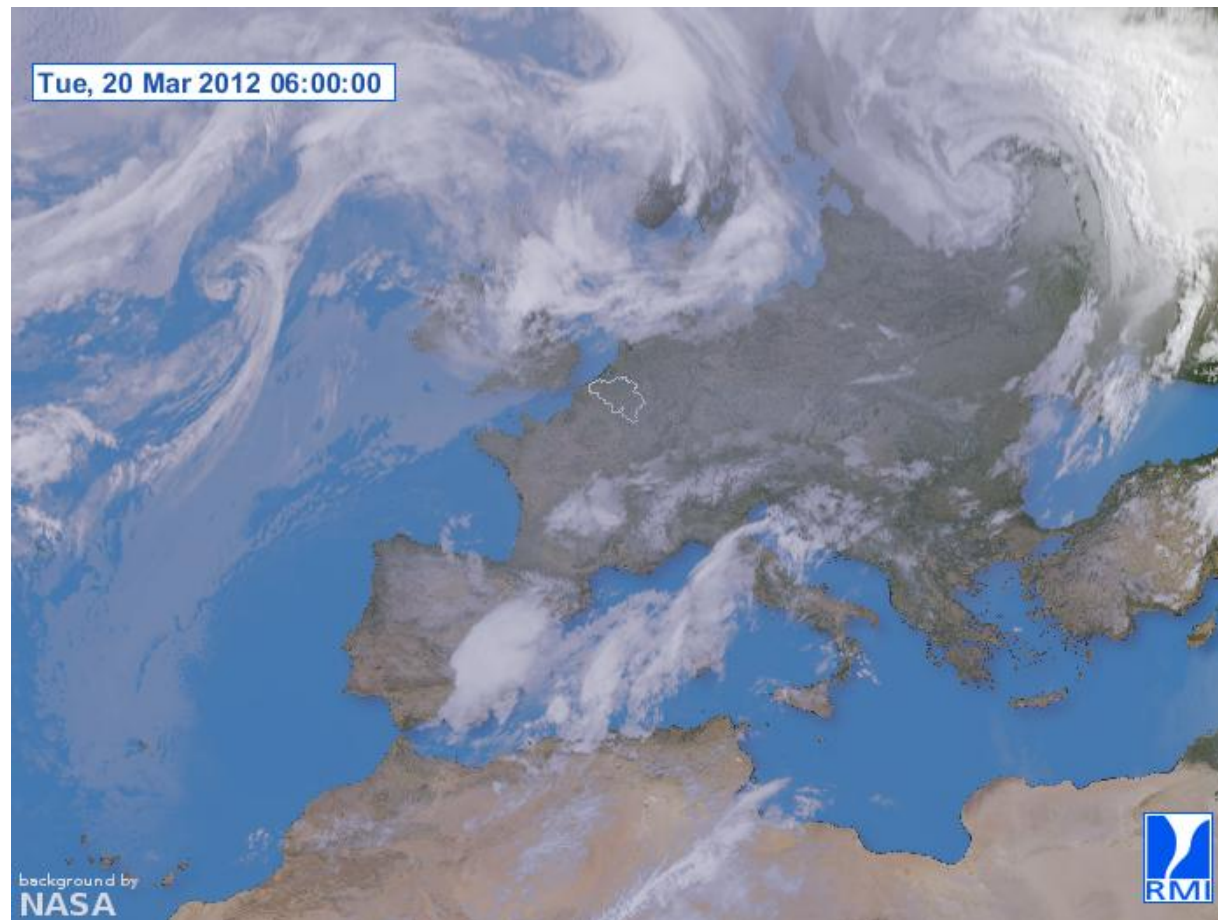
1 Current situation



Information overflow

- **Numerous valuable sources**
 - remote
 - local
 - near real-time
- **Processing all the data**
 - how: scripting?
 - what to treat?

Lack of large-scale overview



.be

Contact point issues

Whom



Criminals are organised and DO share

The screenshot shows the website for Damagelab, a cybertech lab. The header includes the logo 'DL DAMAGELAB THE CYBERTECH LAB' and a 'DDoS Service' banner. Below the header is a navigation menu with various links. The main content area features a black banner with the text 'Ministry of Fraudulently Affairs' flanked by Om symbols. Below this is a 'User guide' section with a link to 'Description' and a sub-link for 'Bot'. The central focus is a large advertisement for 'DARKNESS X', a powerful DDoS bot. The ad includes an illustration of a hacker character named 'Optima' and a diagram showing traffic (HTTP, ICMP, SYN, UDP) being sent to server racks. The text describes it as a 'Powerful DDoS Bot with premim admin-panel "Optima" [From Russia with love]' and lists features: '4 types of DDoS Attacks / Additional modules / 7 packages / Amazing Support'. It also mentions '2009-2012. SW_Team'.

CSIRTs are like islands



.be

Legal issues

- Allowed?
- What?
- With whom?
- How?



.be

Political issues

Voici l'arme de la FN que portait Kadhafi

HUGUES DORZEE, DAMIEN SPLEETERS ET ALAIN LALLEMAND
vendredi 21 octobre 2011, 15:37

Exclusif Le dictateur déchu, capturé puis tué ce jeudi près de la ville de Syrte, avait en sa possession une arme dorée fabriquée en Belgique.



Le pistolet doré que le combattant rebelle Mohammed al-Bibi brandit dans les airs est l'arme personnelle du colonel Kadhafi, mort hier dans des circonstances encore floues, après avoir été capturé près de la ville de Syrte.

Hissé sur les épaules de ses camarades, Mohammed, la vingtaine, une casquette des

main des plus grands

- La fin de Kadhafi (Attention les images peuvent choquer)
- La mention Made in Belgium
- Le numéro de série

lire aussi

- L'ONU demande une enquête sur la mort de Kadhafi
- La mort de Kadhafi reste entourée de zones d'ombre
- L'édito - La fin sordide d'un dictateur
- Chat : « La mort Kadhafi, un mauvais départ pour une démocratie »
- Le 11h02 : « La liquidation de Kadhafi, un signe inquiétant de barbarie »
- Les F-16 belges ont largué 473 bombes en Libye
- La mort de Kadhafi, « la fin d'une tyrannie »
- Pas d'autopsie sur le

le fil info

lancer le fil info

- 17:18 Giro : Amador vainqueur, Hesjedal en rose
- 17:12 Rallye Var : une voiture fonce dans la foule, au moins 2 morts
- 17:22 Fanny Smets bat le record de Belgique du saut à la perche
- 16:13 WTA Brussels Open : Bonaventure éliminée en qualif
- 15:40 Combats nocturnes entre Al-Qaïda et l'armée yéménite : 26 morts

les plus consultés

- Obama : « François, tu pouvais enlever la cravate ! »
- Di Rupo quittera Chicago avec l'avion gouvernemental
- Les salaires de nos ministres sont-ils trop élevés ?
- « Si on retournait à des monnaies nationales... »
- Hollande : « La situation de la Grèce doit être au menu du G8 »

LE SOIR on aura toujours raison de l'ouvrir

Gratuit l'album + 16 autocollants inédits !

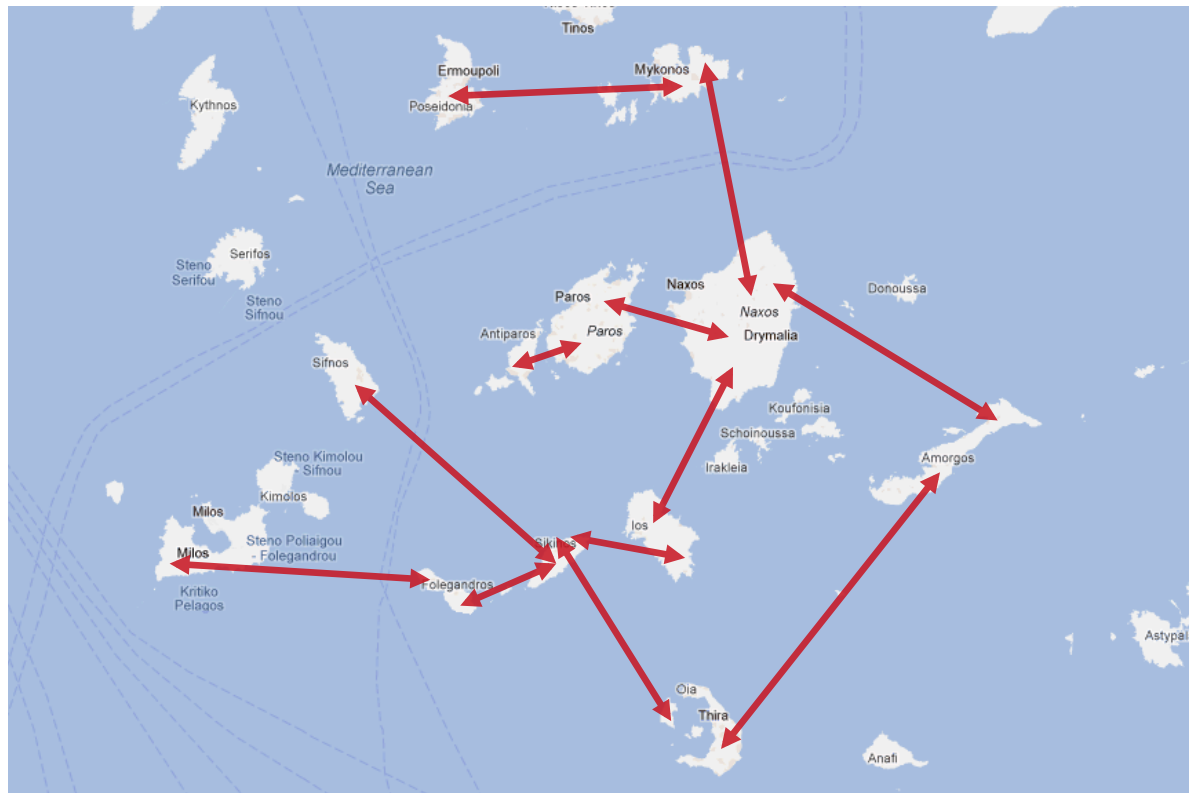
Technical issues



2 Proposal for a new model for sharing



Connecting our islands efficiently



Creating archipelagoes

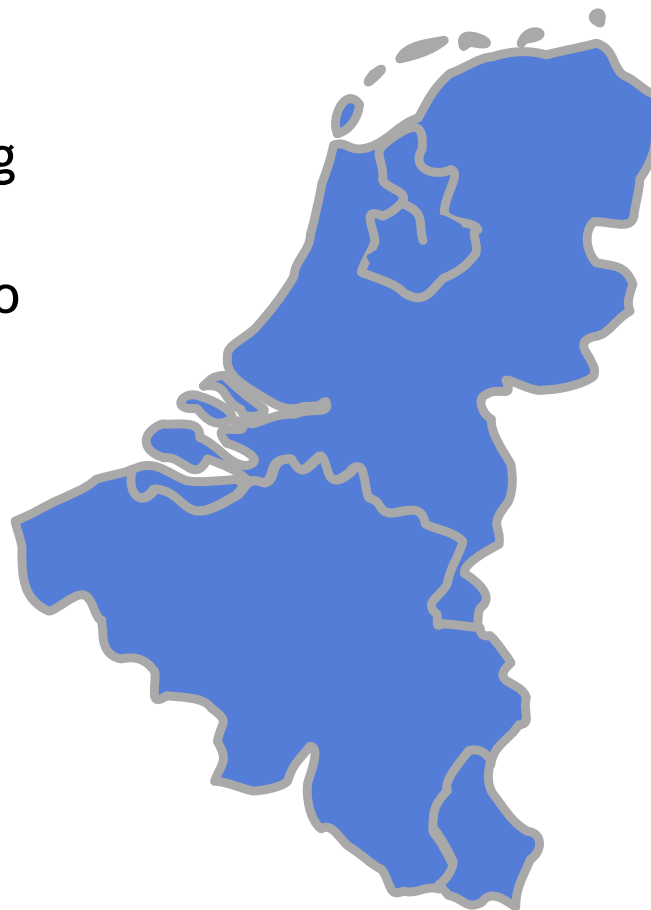
- **European Union .eu**
 - 27 countries already sharing
 - Why not on incidents?



.be

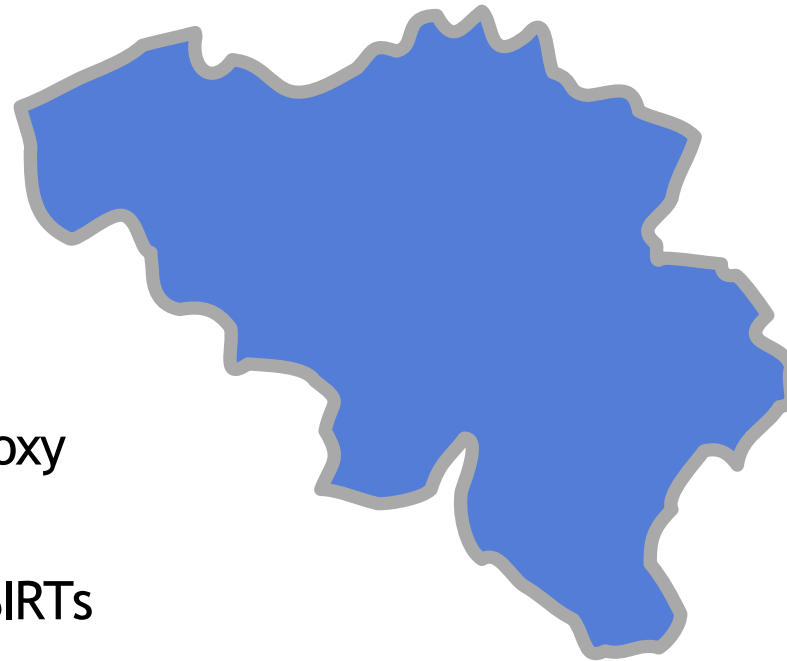
Creating archipelagoes

- **Benelux .be .nl .lu**
 - 3 countries sharing since 1944
 - EU sub archipelago



.be

Creating archipelagoes



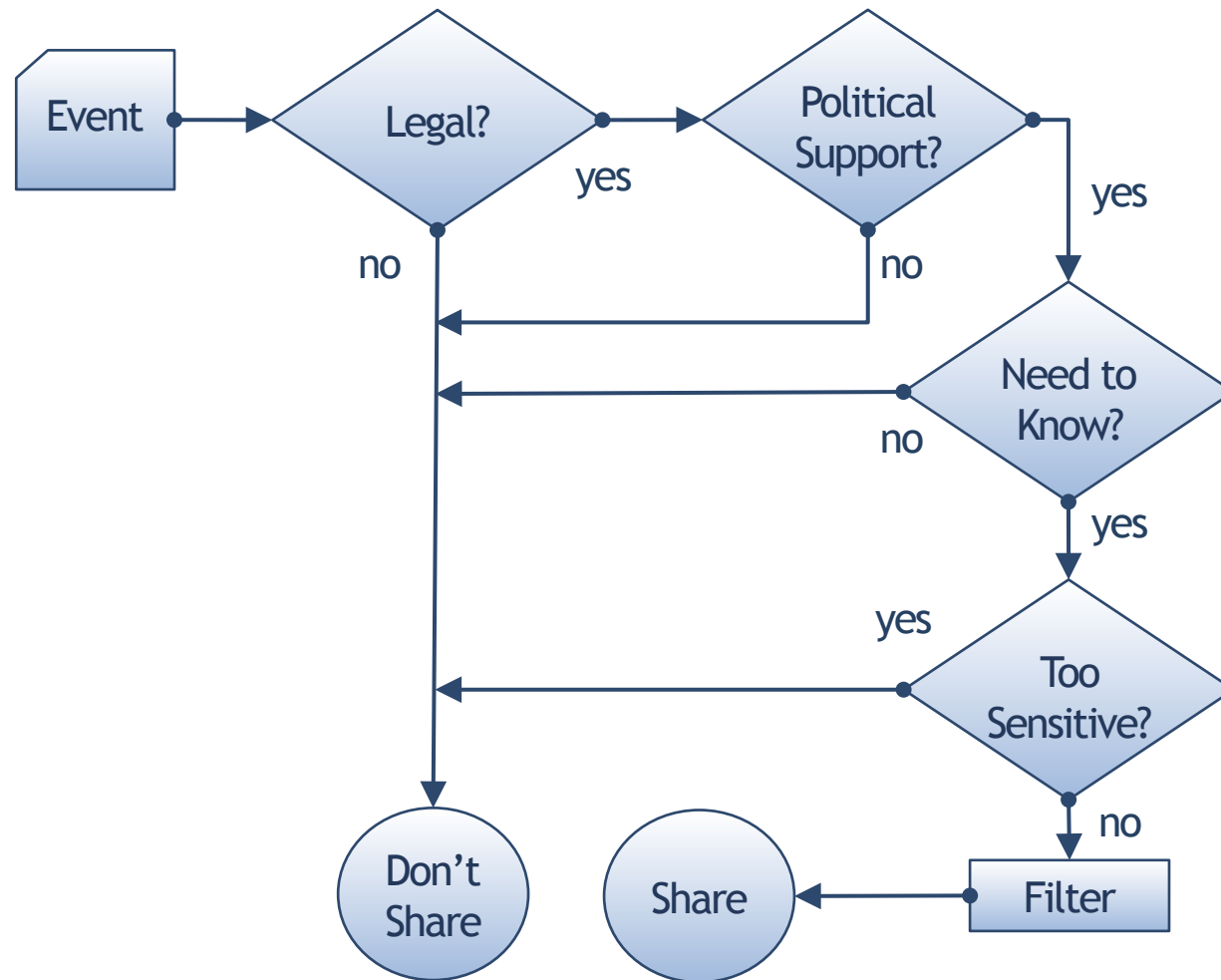
- **Belgium .be**
 - CERT.be proxy
 - Febelfin
 - Sectorial CSIRTs
 - ISP's
 - Law Enforcement

.be

Seeds for archipelagoes

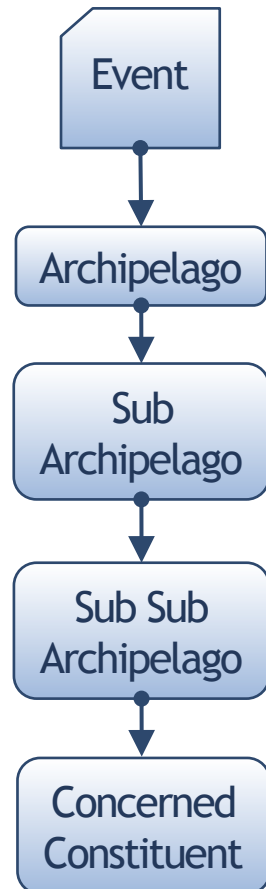
- **Geo-political decisions / history**
- **Existing organizations**
 - FIRST
 - TF-CSIRT
 - ENISA
 - National / governmental CSIRTs
- **Fighting a common issue**
 - DCWG.org
- **Anything that pushes countries to collaborate!**
- **Requires TRUST!**

Decision tree



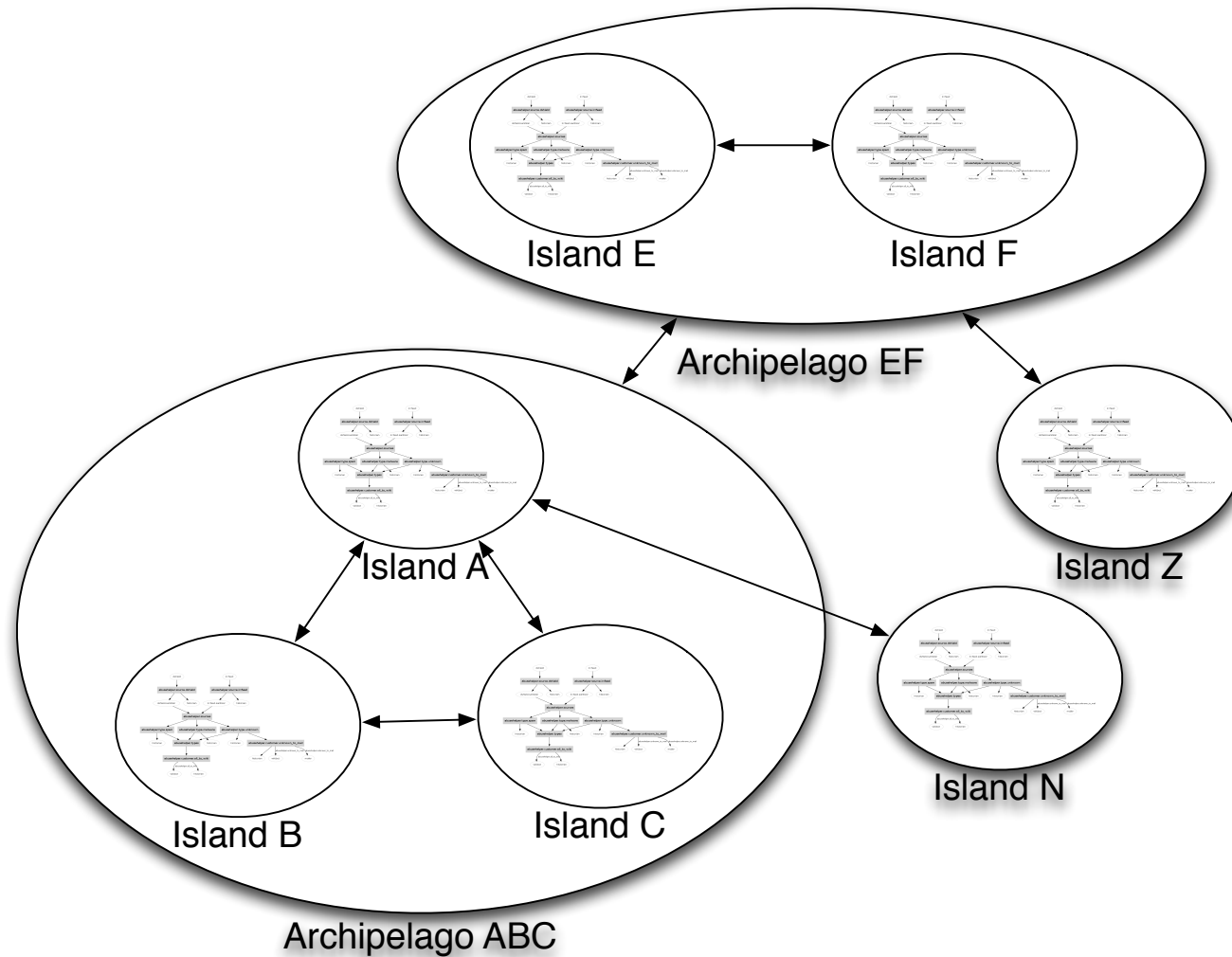
.be

Routing model: top-down

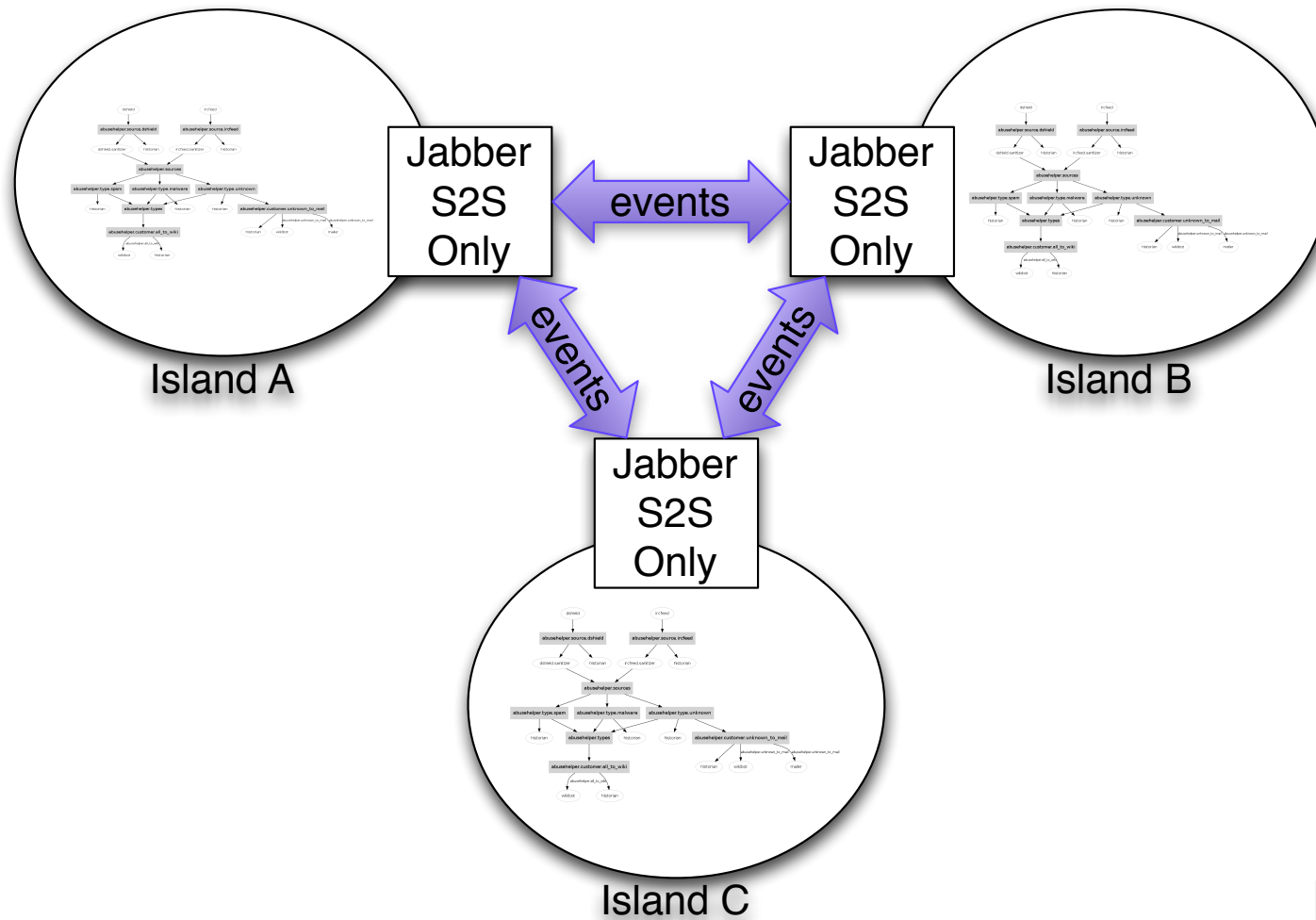


.be

Security is no longer an island!



How can we share?



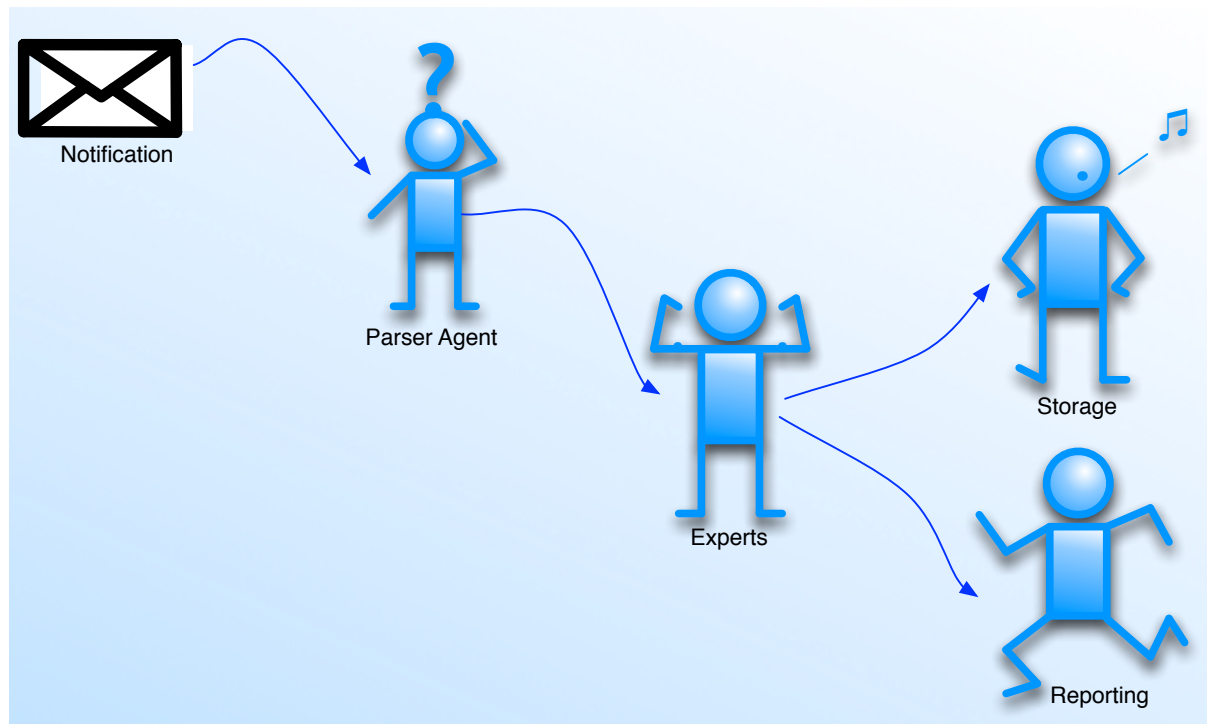
What can we share?

- **Events**
 - IP's (src & dst) - Ports - Protocols
 - URL's
- **Binaries and/or hashes of**
 - malware
 - suspicious files
- **Information on domains, IP's, AS's**
 - owner
 - history (passive DNS)
- **Binary answer to a question (yes/no)**
 - have you seen that IP before?
- **Contacts**

Tools already exist ... for years!

- **Phone**
- **mail**
- **chat**
- **FTP**
- **scripts**
- **AbuseHelper**
- **Megatron**
- **fordrop**

AbuseHelper: the collaborative agents



Megatron: the central vacuum cleaner



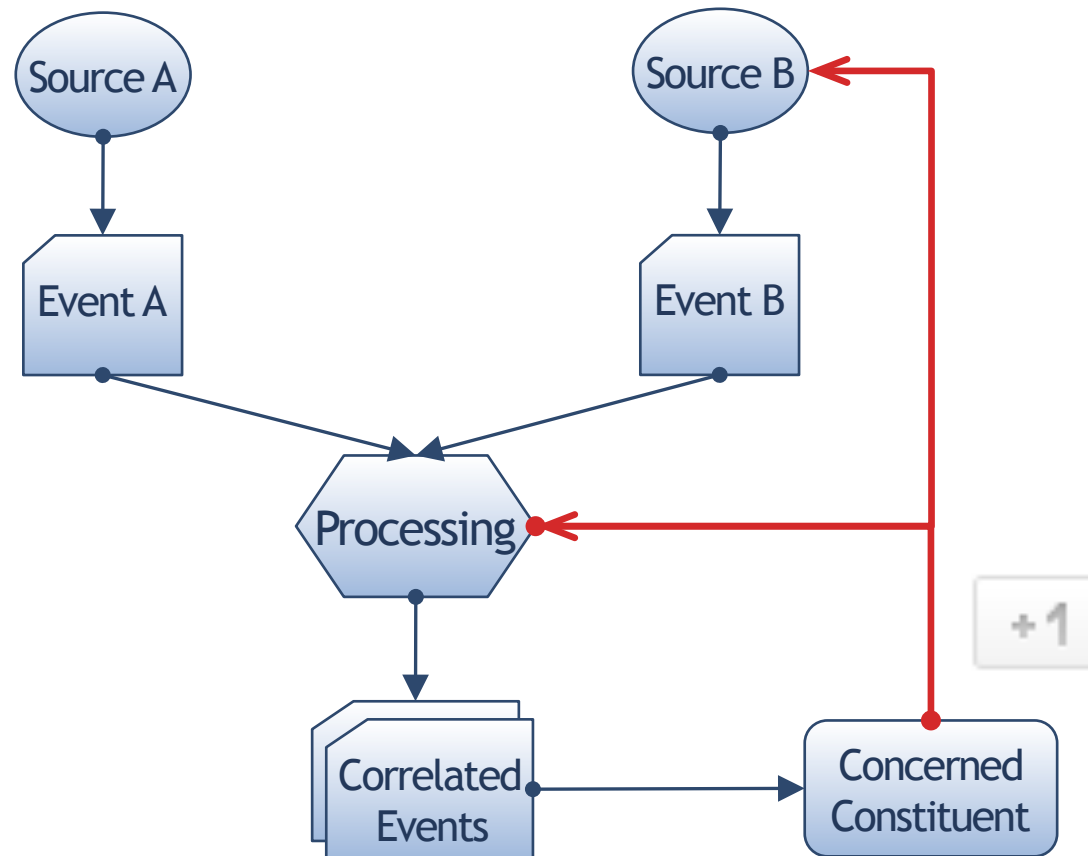
fordrop: human collaboration



3 New issues



Correlated events: rating & feedback



4 Conclusion



You can share too

Please

SHARE

and help us do that

EFFICIENTLY

.be

You are in good company



.be

Sharing time!

Please

SHARE

and help us do that

EFFICIENTLY

david@cert.be

christian@cert.be

.be