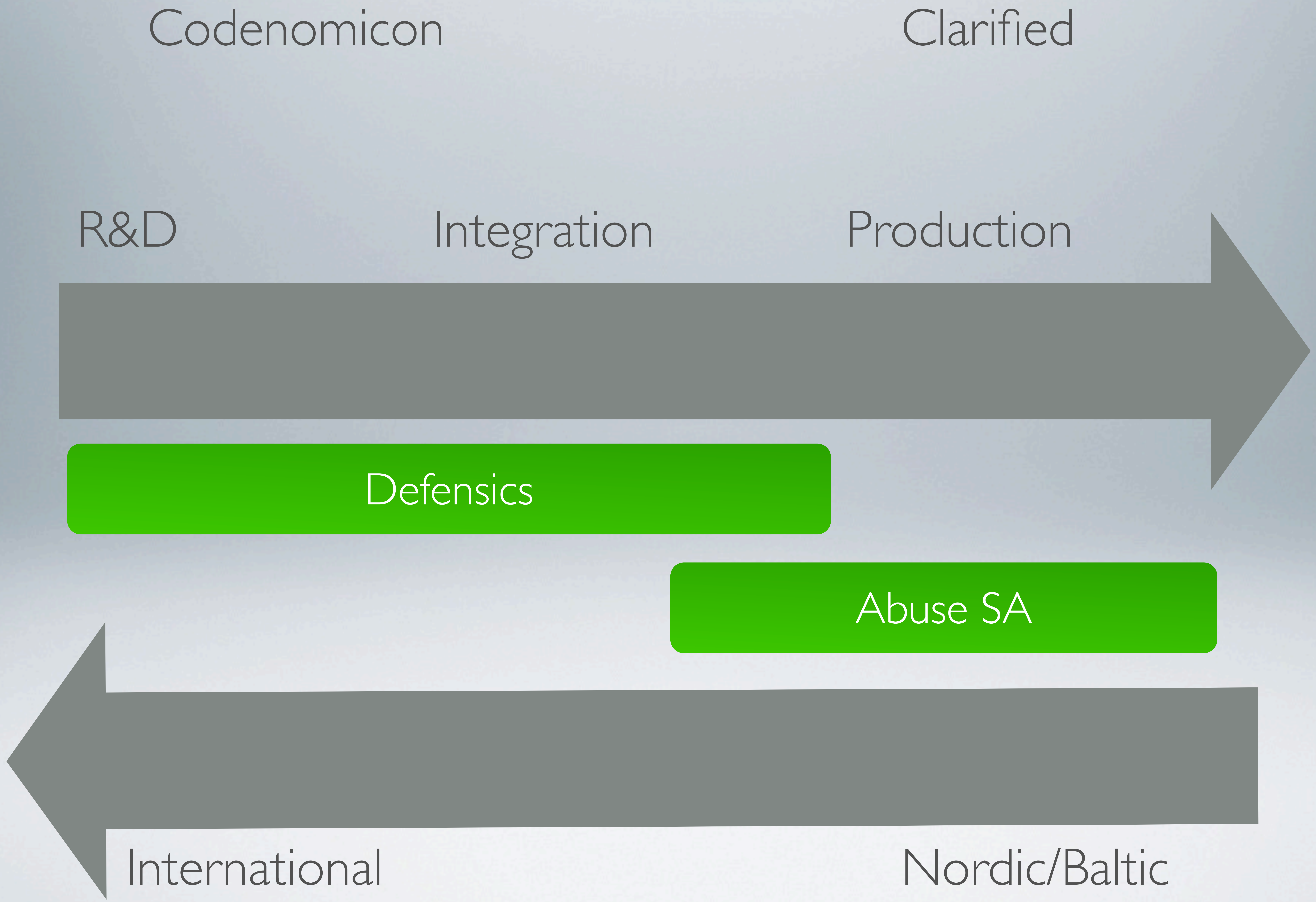


Codenomicon

Clarified

R&D

Integration

Production

Defensics

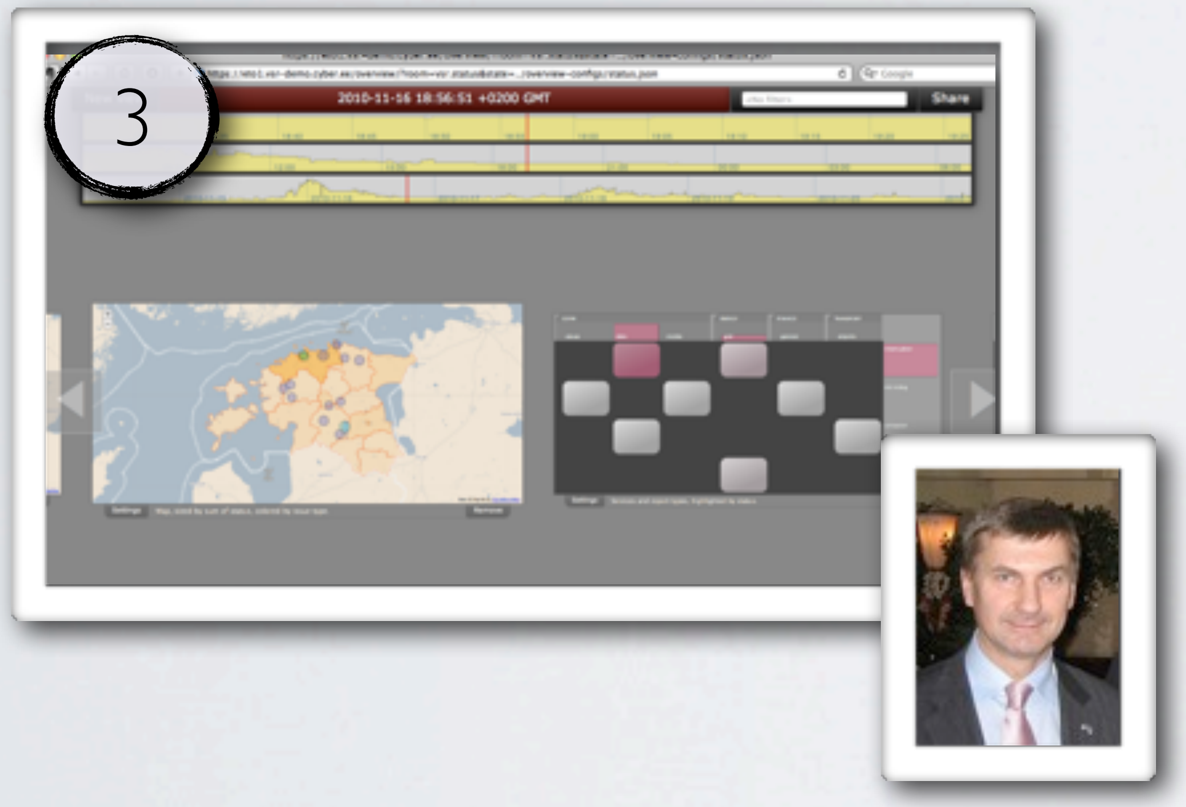
Abuse SA

International

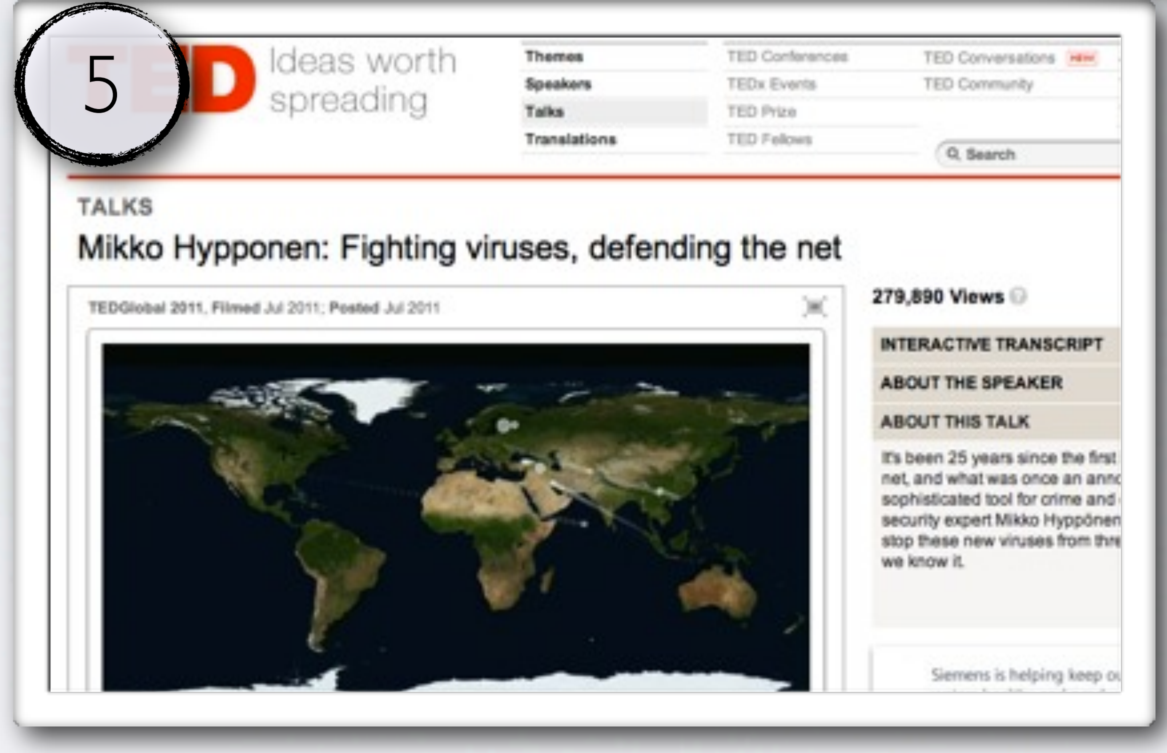
Nordic/Baltic

US IN NUMBERS

- **Clarified 2010:**
  - Estonia (gov & NATO CCDCOE), Russia, Finland, Sweden
  - CERTs, Banks, Large teleoperators, Large enterprises, other gov orgs.
  - 1.5x growth, profitable, AAA-rating
- **Clarified 2011- Joining forces with Codenomicon**, sales rep now includes:
  - UK, Canada, Japan, Sweden, Netherlands, US
- Operating in US/European/APAC market
- As a whole: 70 person R&D community producing innovative solutions to protect you and your constituencies



Övar sig att mota en cyberattack



TALKS

Mikko Hypponen: Fighting viruses, defending the net

TEDGlobal 2011. Filmed Jul 2011; Posted Jul 2011

279,890 Views

It's been 25 years since the first net, and what was once an ann sophisticated tool for crime and security expert Mikko Hyppönen stop these new viruses from thr we know it.

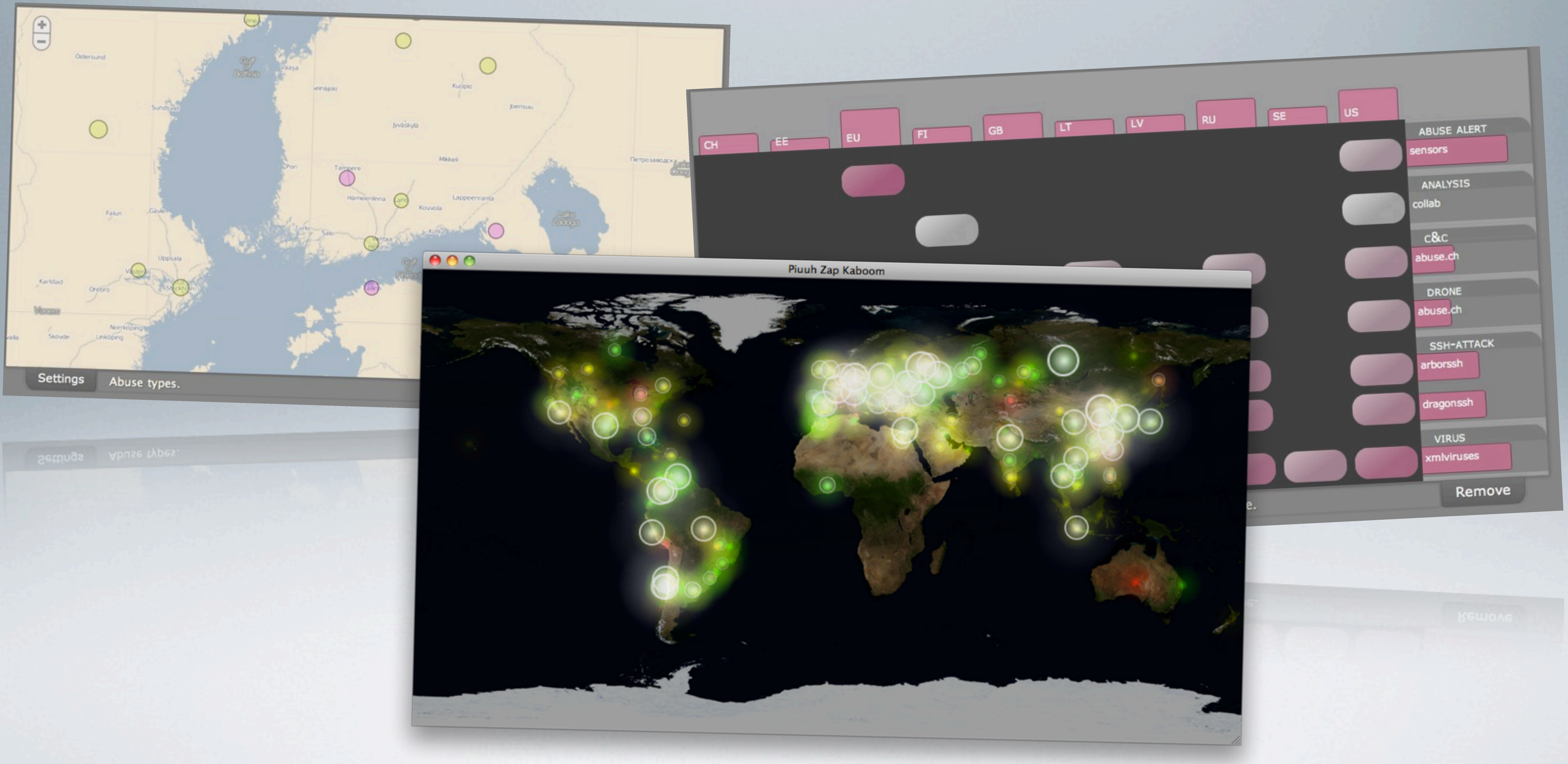
Siemens is helping keep o

CHRISTIAN VAN HEURCK
Coordinateur - CERT.be
Computer Emergency Response Team

1. Analyzer used in Bredolab botnet takedown, Dutch TV-channel covers
2. White House still remembers our research results from 2002, Chief of Defense Command Finland tweets about it after his visit. (Clarified Networks and Codenomicon are spin-offs from Oulu University Secure Programming Group).
3. Virtual Situation Room deployment for Estonian Government
4. Situation rooms for NATO Baltic Cyber Shield exercise, covered by Swedish national TV (SVT)
5. Clarified Visualization in Mikko Hyppönen's TED talk, 300 000 views as of 2011-09
6. News coverage of CERT.be fighting against website hacks, AbuseHelper's TV-premiere.

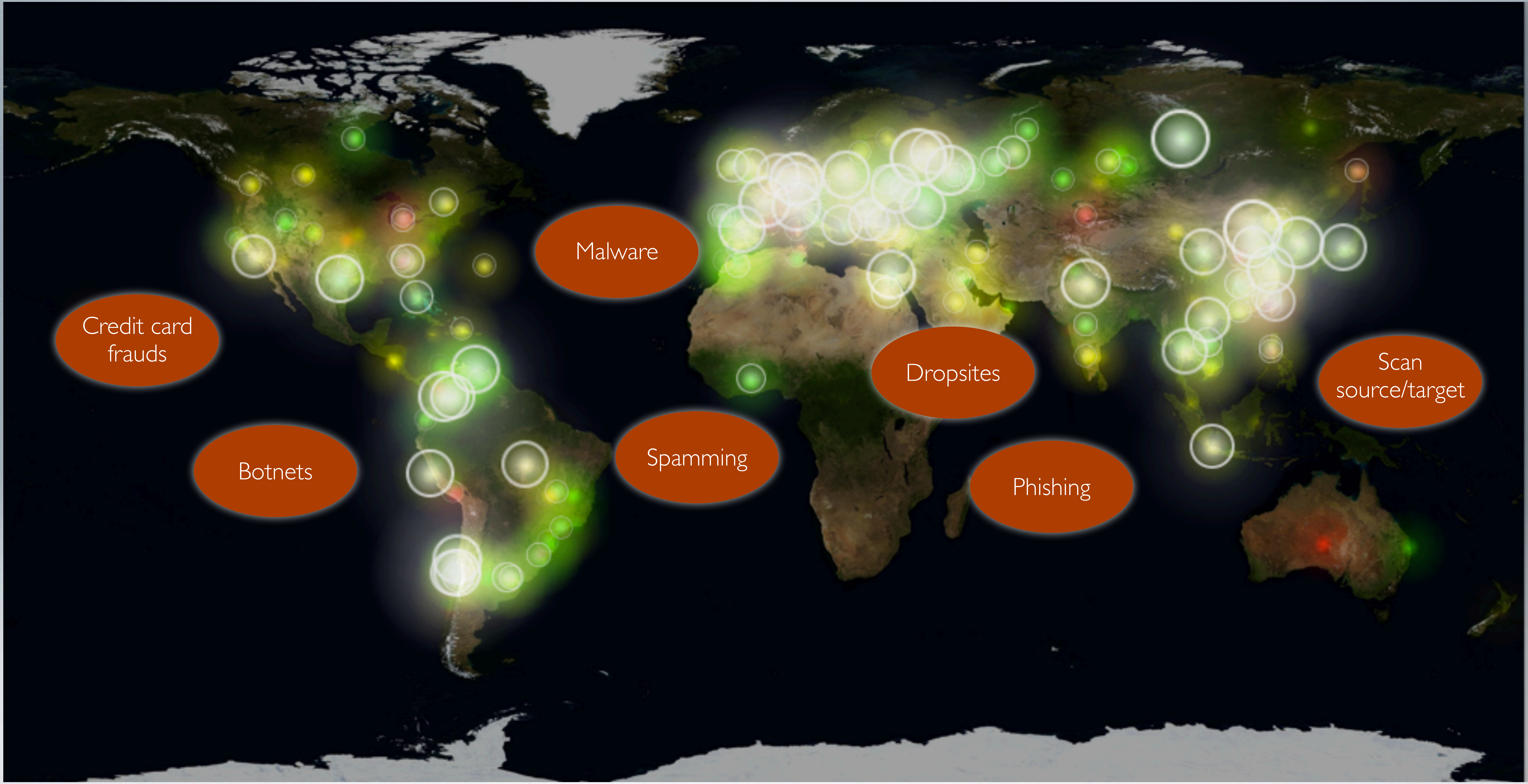
RECENT (PUBLIC) EVENTS

ABUSE SITUATION AWARENESS



Jani Kenttälä, Clarified Networks Oy, part of Codenomicon Group

CHALLENGE: ABUSE IS REALITY

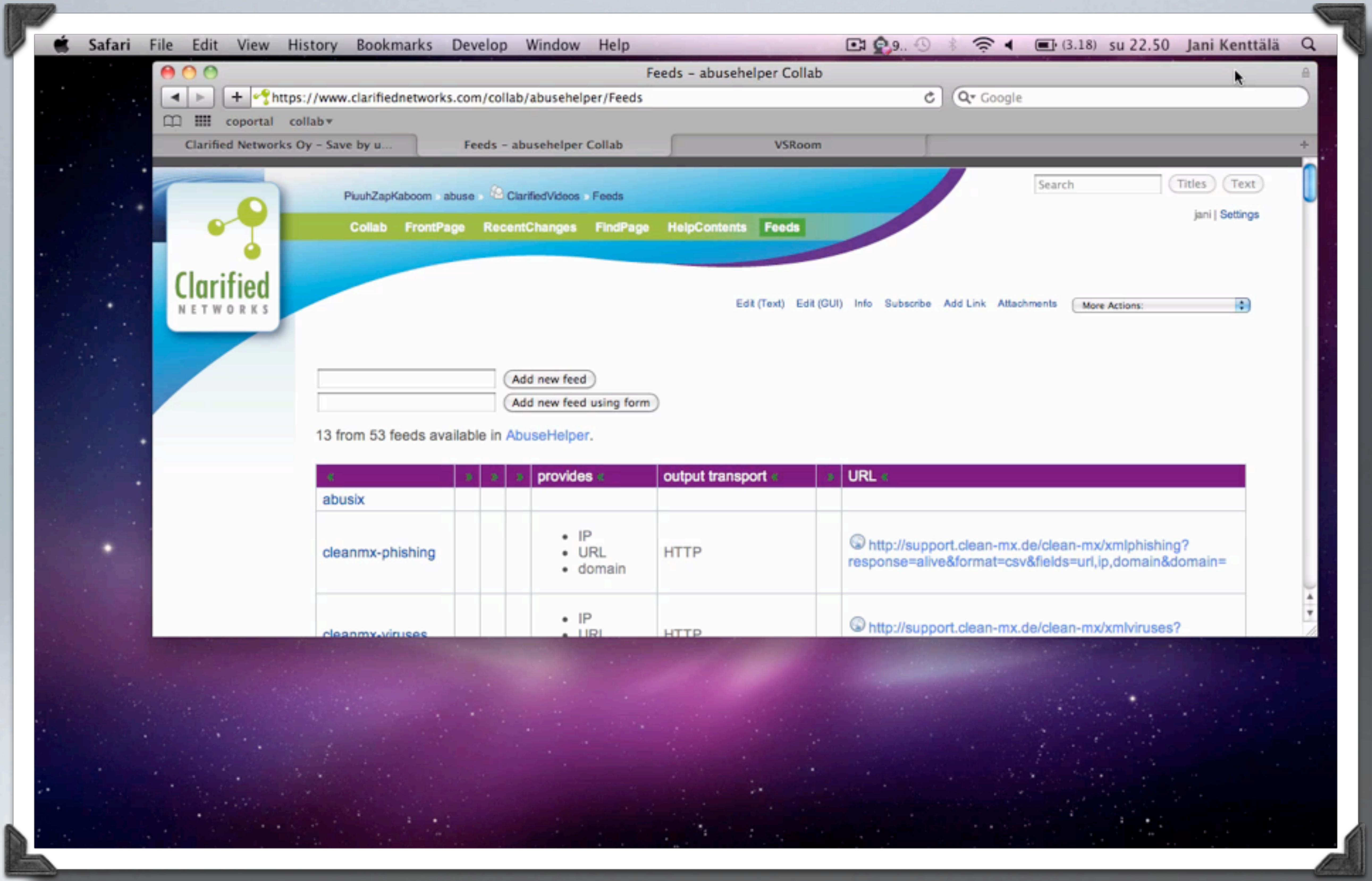


Screenshot of a real-time visualization showing abuse events.

AID, AND A NEW CHALLENGE: A LOT OF FEEDS TELLS US ABOUT IT

ShadowServer
Spamhaus Drop & SBL
Zone-H
Team Cymru Bogons
Dshield
ZeusTracker
Malwaredomainlist

AID, AND A NEW CHALLENGE: A LOT OF FEEDS TELLS US ABOUT IT


Safari File Edit View History Bookmarks Develop Window Help
(3.18) su 22.50 Jani Kenttälä
Feeds – abusehelper Collab
https://www.clarifiednetworks.com/collab/abusehelper/Feeds
Google
coportal collab
Clarified Networks Oy – Save by u…
Feeds – abusehelper Collab
VSRoom
Clarified NETWORKS
PiuuhZapKaboom abuse ClarifiedVideos Feeds
Collab FrontPage RecentChanges FindPage HelpContents Feeds
Search Titles Text
jani | Settings
Edit (Text) Edit (GUI) Info Subscribe Add Link Attachments More Actions:
Add new feed
Add new feed using form

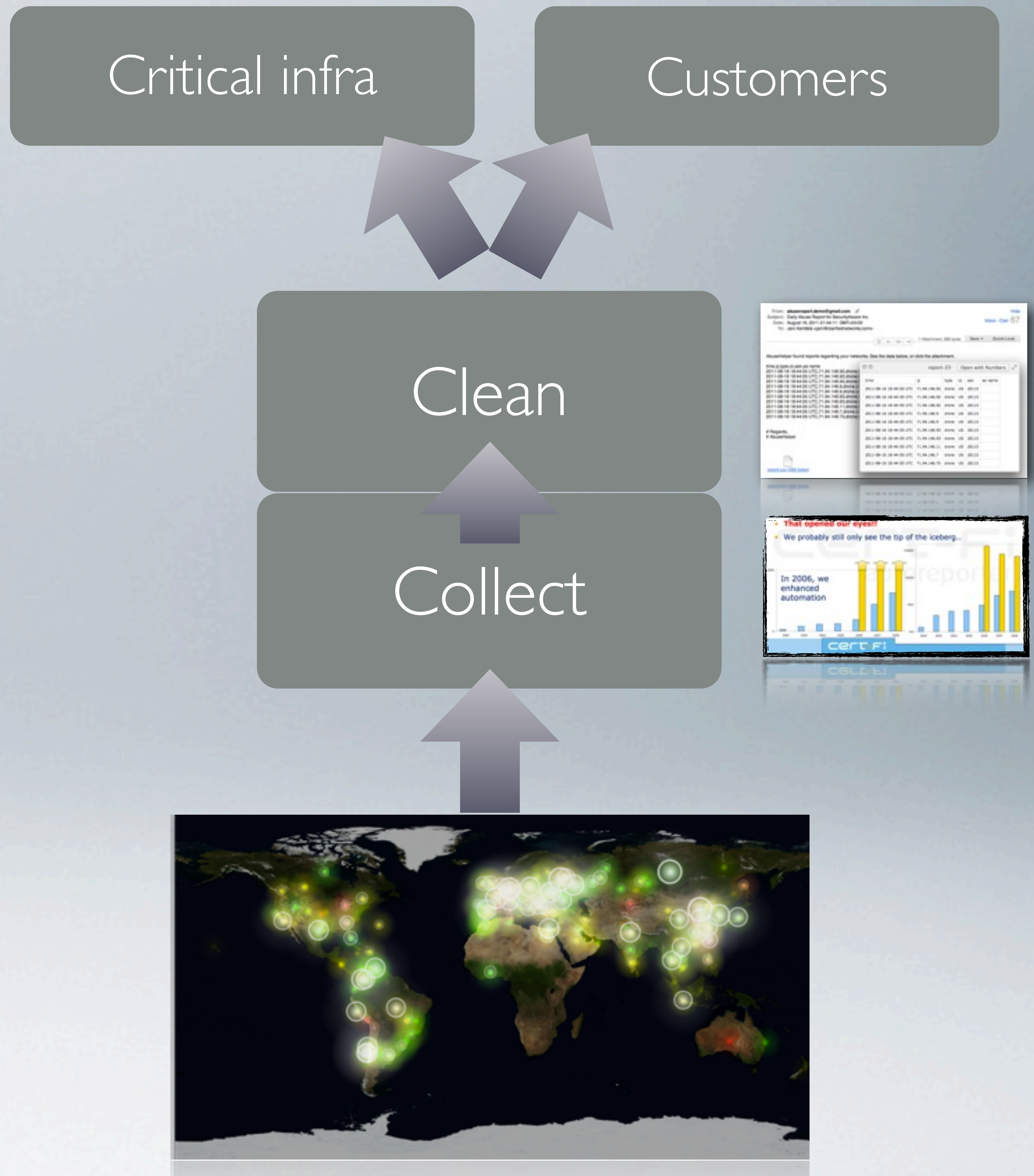
13 from 53 feeds available in AbuseHelper.

«	»	»	»	provides «	output transport «	»	URL «
abusix							
cleanmx-phishing				• IP • URL • domain	HTTP		http://support.clean-mx.de/clean-mx/xmlphishing?response=alive&format=csv&fields=url,ip,domain&domain=
cleanmx-viruses				• IP • URL	HTTP		http://support.clean-mx.de/clean-mx/xmlviruses?

THE PROCESS

We help our customers to deal with Cyber threats (malware, spam, botnets etc) by:

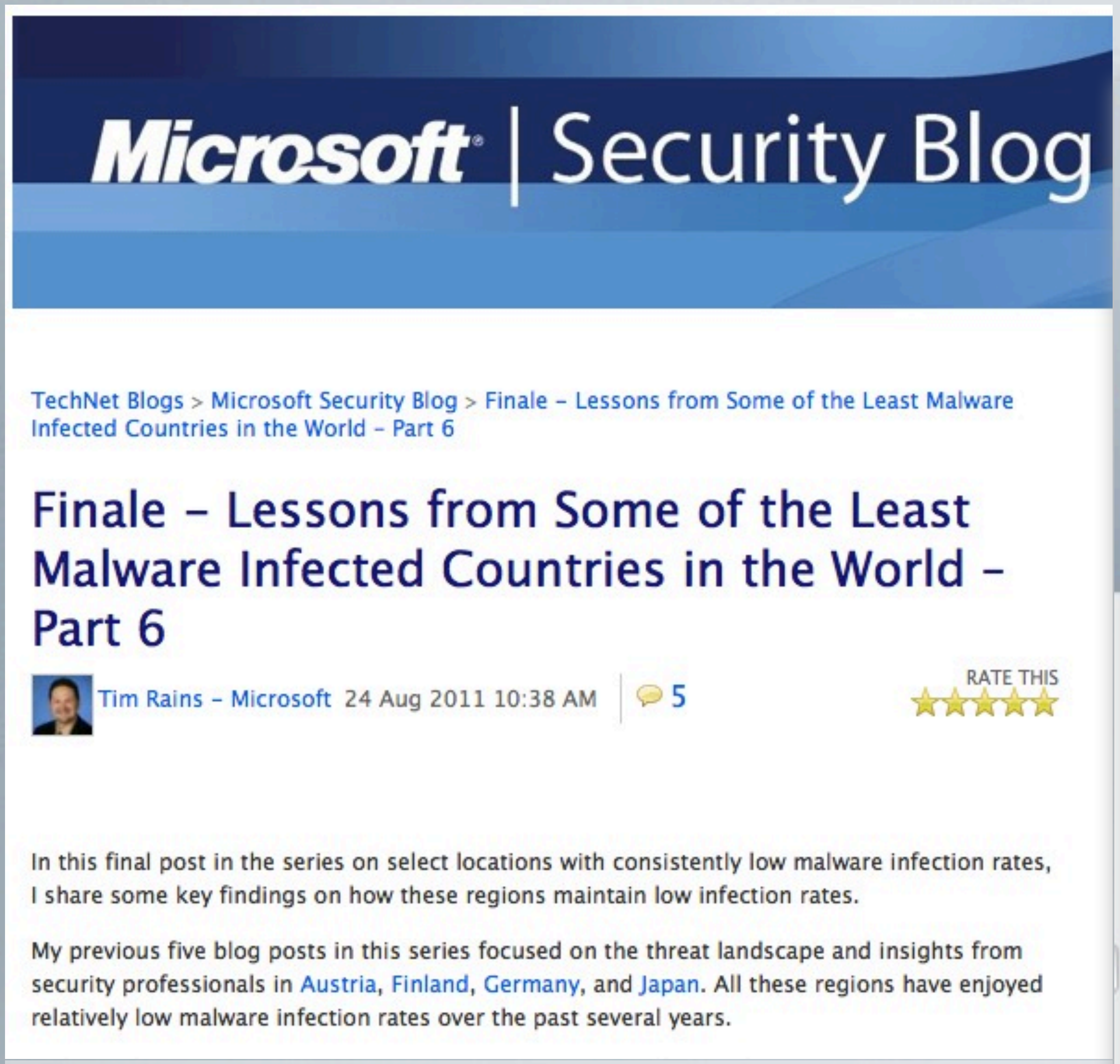
- fully automating the data collection from external sources,
- enabling **actionable reporting** to stakeholders, and
- **visualizing** the collected information for risk management and decision support
- Additionally we enable cross-organizational collaboration


Critical infra
Customers
Clean
Collect
That opened our eyes!!
We probably still only see the tip of the iceberg...
In 2006, we enhanced automation
cert fi

RAISING THE MATURITY OF ABUSE HANDLING

UP TO THE FULL AUTOMATION

- Manual
- Ad hoc (in-house) scripts
- Hands on automata (abuse specific ticketing systems)
- **Hands off automata**
- Investigative capability



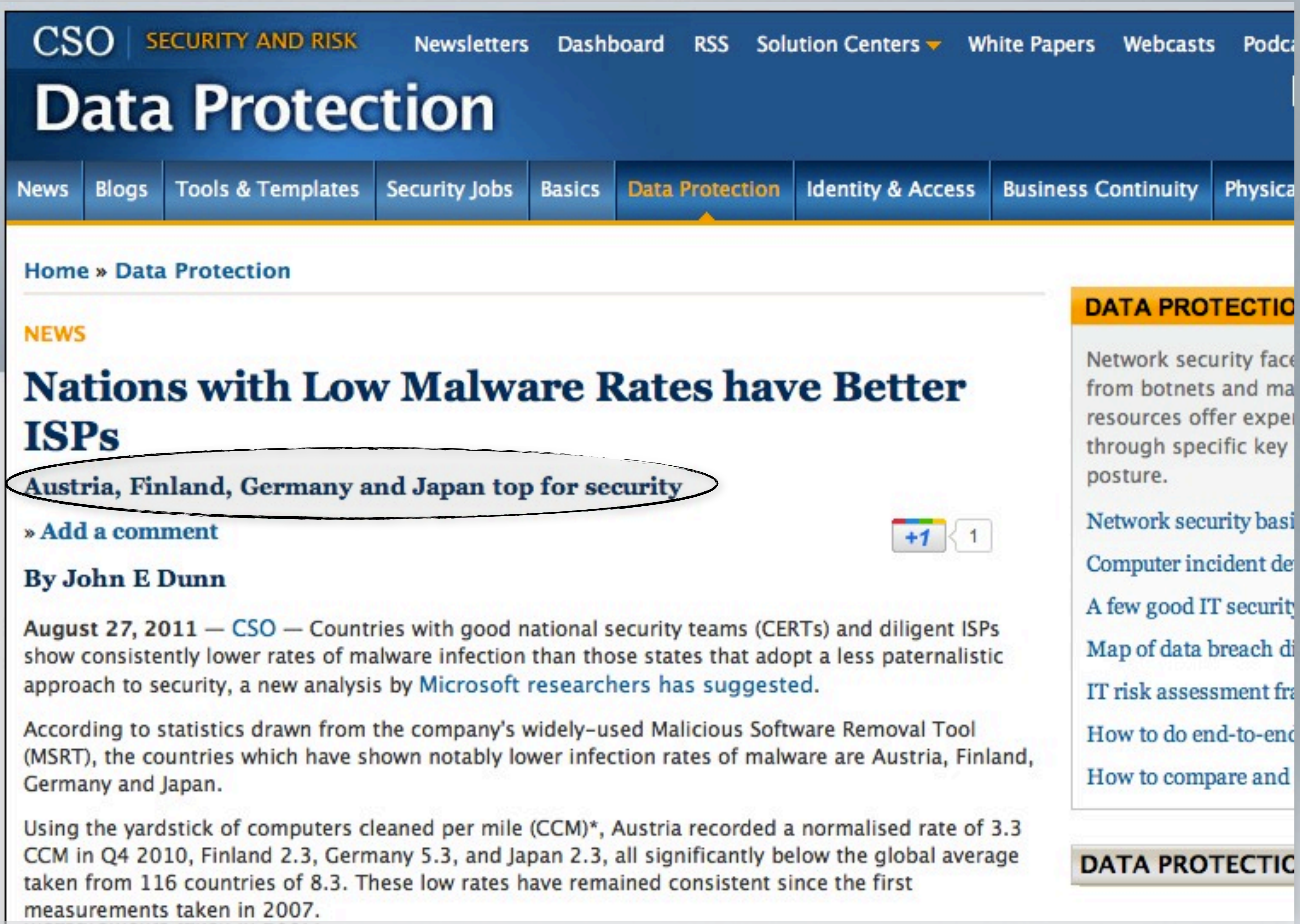
TechNet Blogs > Microsoft Security Blog > Finale – Lessons from Some of the Least Malware Infected Countries in the World – Part 6

Finale – Lessons from Some of the Least Malware Infected Countries in the World – Part 6

Tim Rains - Microsoft 24 Aug 2011 10:38 AM 5 RATE THIS ★★★★★

In this final post in the series on select locations with consistently low malware infection rates, I share some key findings on how these regions maintain low infection rates.

My previous five blog posts in this series focused on the threat landscape and insights from security professionals in Austria, Finland, Germany, and Japan. All these regions have enjoyed relatively low malware infection rates over the past several years.



Home » Data Protection

NEWS

Nations with Low Malware Rates have Better ISPs

Austria, Finland, Germany and Japan top for security

» Add a comment

By John E Dunn

August 27, 2011 — CSO — Countries with good national security teams (CERTs) and diligent ISPs show consistently lower rates of malware infection than those states that adopt a less paternalistic approach to security, a new analysis by Microsoft researchers has suggested.

According to statistics drawn from the company's widely-used Malicious Software Removal Tool (MSRT), the countries which have shown notably lower infection rates of malware are Austria, Finland, Germany and Japan.

Using the yardstick of computers cleaned per mile (CCM)*, Austria recorded a normalised rate of 3.3 CCM in Q4 2010, Finland 2.3, Germany 5.3, and Japan 2.3, all significantly below the global average taken from 116 countries of 8.3. These low rates have remained consistent since the first measurements taken in 2007.

DATA PROTECTIO

Network security face from botnets and ma resources offer exper through specific key posture.

Network security basi
Computer incident de
A few good IT security
Map of data breach di
IT risk assessment fra
How to do end-to-end
How to compare and

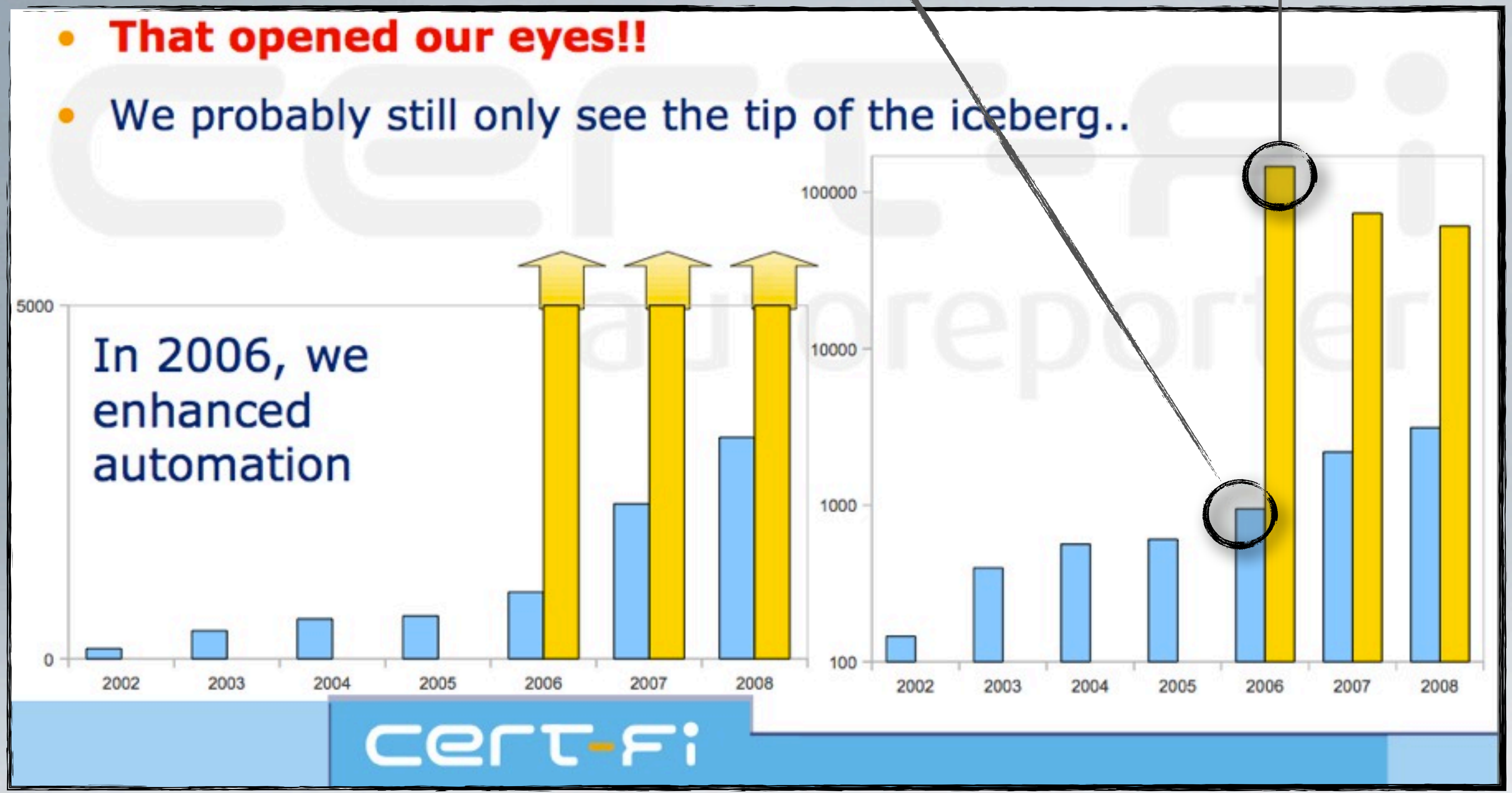
DATA PROTECTIO

> “The infection rates and other metrics for Finland have consistently been below the world-wide averages, and we have often wondered ourselves what the reason is for this”
>
> – Kimmo Bergius, Microsoft’s Chief Security Advisor

HOW DID IT WORK FOR CERT-FI?

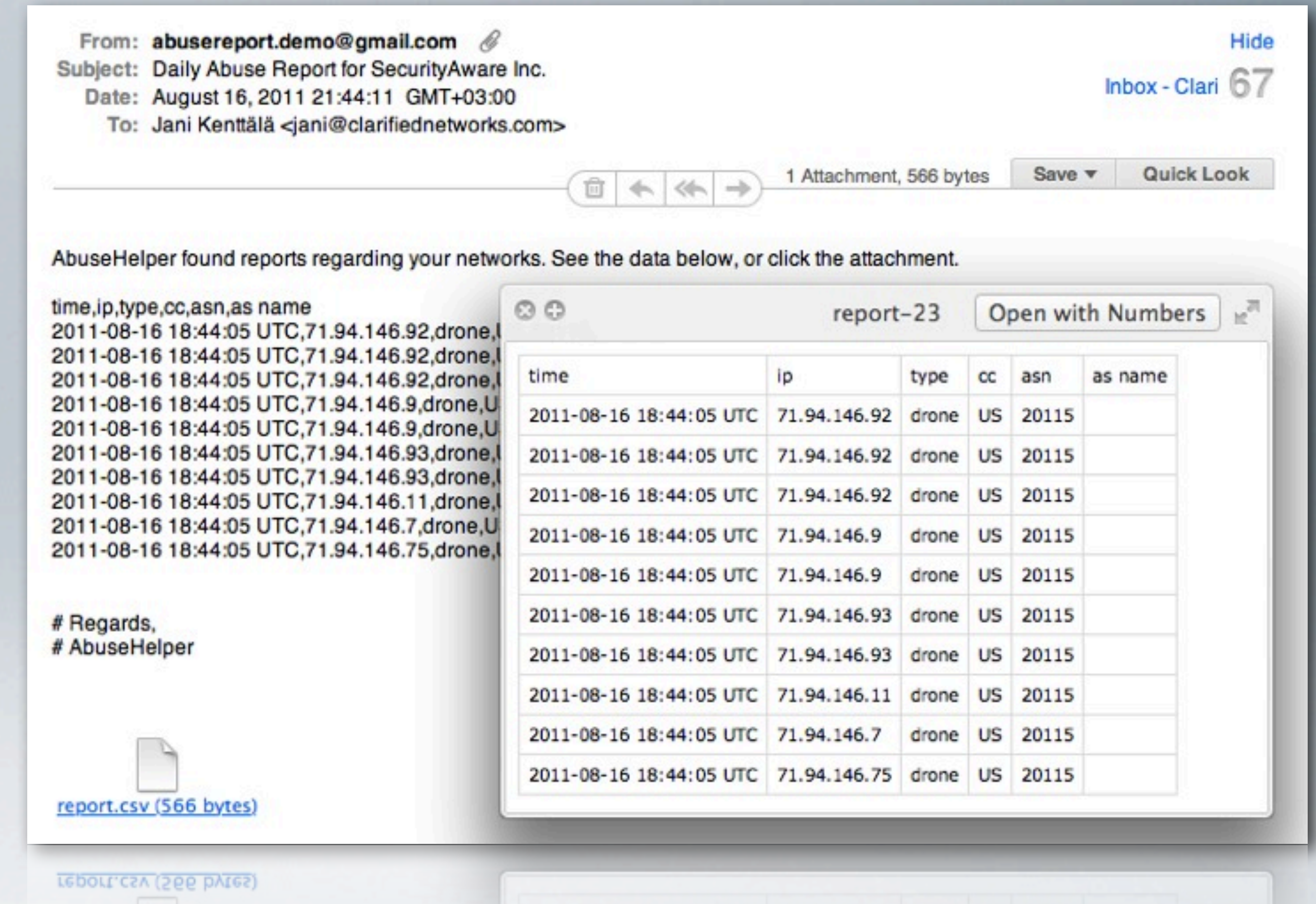
1000 manually handled cases

100 000 automatically handled cases



- **That opened our eyes!!**
- We probably still only see the tip of the iceberg..

In 2006, we enhanced automation



From: **abusereport.demo@gmail.com**
Subject: Daily Abuse Report for SecurityAware Inc.
Date: August 16, 2011 21:44:11 GMT+03:00
To: Jani Kenttälä <jani@clarifiednetworks.com>

AbuseHelper found reports regarding your networks. See the data below, or click the attachment.

```
time,ip,type,cc,asn,as name
2011-08-16 18:44:05 UTC,71.94.146.92,drone,U
2011-08-16 18:44:05 UTC,71.94.146.92,drone,U
2011-08-16 18:44:05 UTC,71.94.146.92,drone,U
2011-08-16 18:44:05 UTC,71.94.146.9,drone,U
2011-08-16 18:44:05 UTC,71.94.146.9,drone,U
2011-08-16 18:44:05 UTC,71.94.146.93,drone,U
2011-08-16 18:44:05 UTC,71.94.146.93,drone,U
2011-08-16 18:44:05 UTC,71.94.146.11,drone,U
2011-08-16 18:44:05 UTC,71.94.146.7,drone,U
2011-08-16 18:44:05 UTC,71.94.146.75,drone,U
```

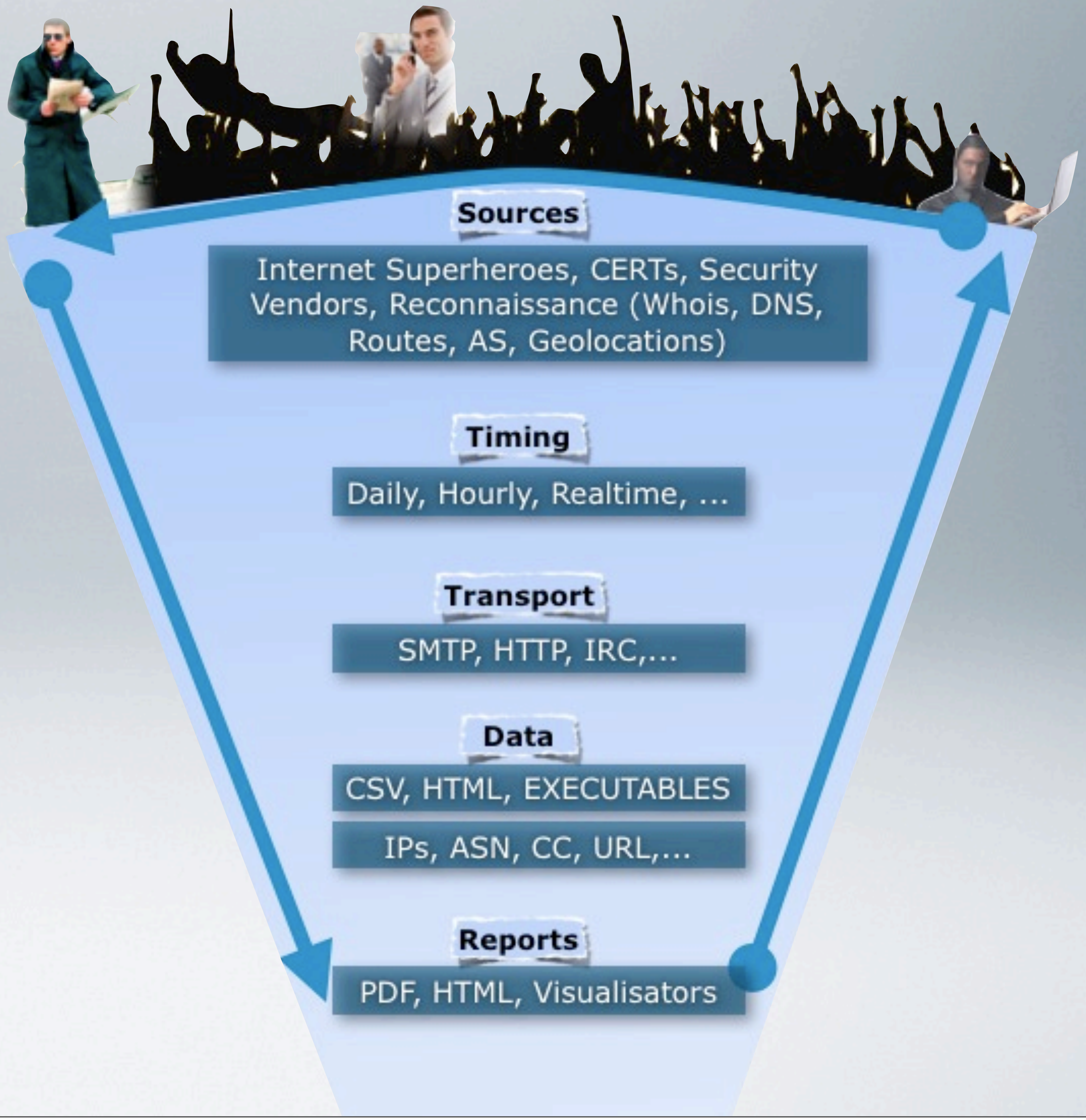
Regards,
AbuseHelper

report.csv (566 bytes)

time	ip	type	cc	asn	as name
2011-08-16 18:44:05 UTC	71.94.146.92	drone	US	20115	
2011-08-16 18:44:05 UTC	71.94.146.92	drone	US	20115	
2011-08-16 18:44:05 UTC	71.94.146.92	drone	US	20115	
2011-08-16 18:44:05 UTC	71.94.146.9	drone	US	20115	
2011-08-16 18:44:05 UTC	71.94.146.9	drone	US	20115	
2011-08-16 18:44:05 UTC	71.94.146.93	drone	US	20115	
2011-08-16 18:44:05 UTC	71.94.146.93	drone	US	20115	
2011-08-16 18:44:05 UTC	71.94.146.11	drone	US	20115	
2011-08-16 18:44:05 UTC	71.94.146.7	drone	US	20115	
2011-08-16 18:44:05 UTC	71.94.146.75	drone	US	20115	

WHY THIS HASN'T BEEN DONE EARLIER?

- Each feed is different in terms of timing, transport, data format, data content etc.
- On the other hand, reporting requirements may be very specific.



Sources

Internet Superheroes, CERTs, Security Vendors, Reconnaissance (Whois, DNS, Routes, AS, Geolocations)

Timing

Daily, Hourly, Realtime, ...

Transport

SMTP, HTTP, IRC,...

Data

CSV, HTML, EXECUTABLES

IPs, ASN, CC, URL,...

Reports

PDF, HTML, Visualisators

COMMUNITY HAS CALLED FOR IT

- *Ideally: Security data is collected and either shared or made readily accessible in a trusted community in real time.*
- *Today: Security data is mostly discarded or at least not shared in a common framework.*

-- Paul Vixie, Andrew Fried, Dr. Chris Lee - Stalking Badness Through Data Mining
presented at Black Hat USA -09

Internet Special Ops

Stalking Badness Through Data Mining

Paul Vixie

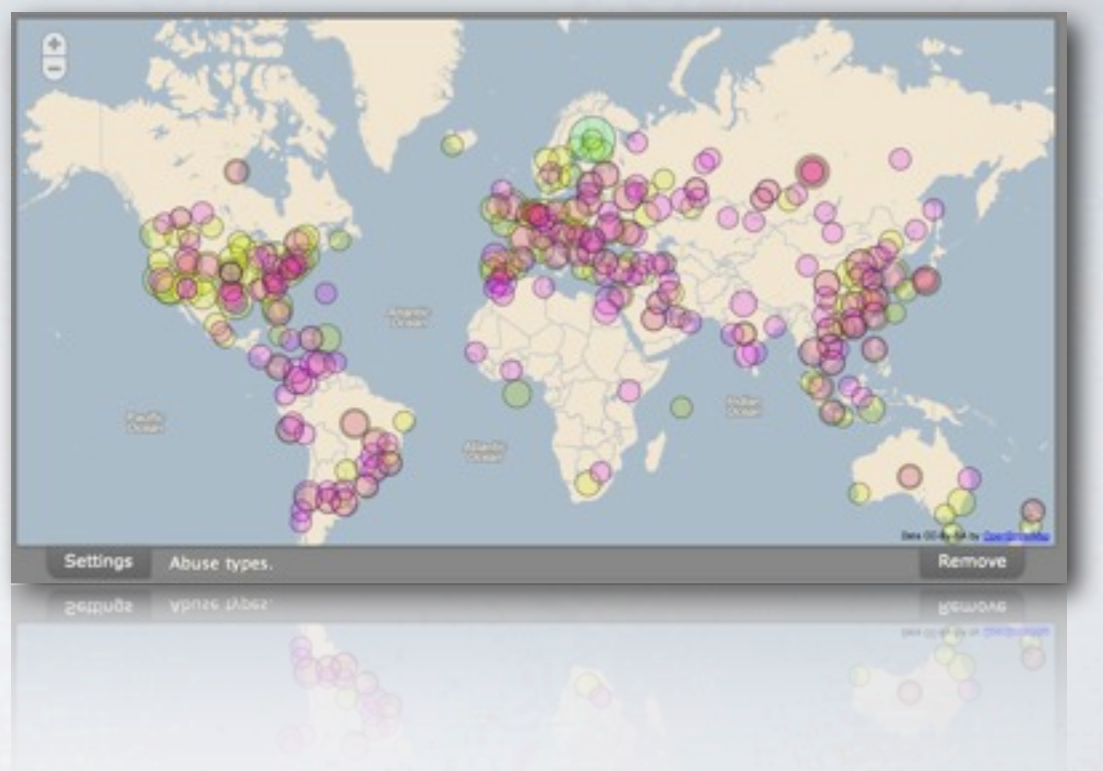
Andrew Fried

Dr. Chris Lee

TOOLS FOR DEALING WITH ABUSE

- AbuseHelper
  - A tool for collecting and sharing suspected malicious activity
  - Collect and process Abuse Information
  - Sent out actionable reports

- Virtual Situation Room
  - Gain situational awareness over Abuse Information
  - Real-time visualizations from your perspective



ABUSEHELPER

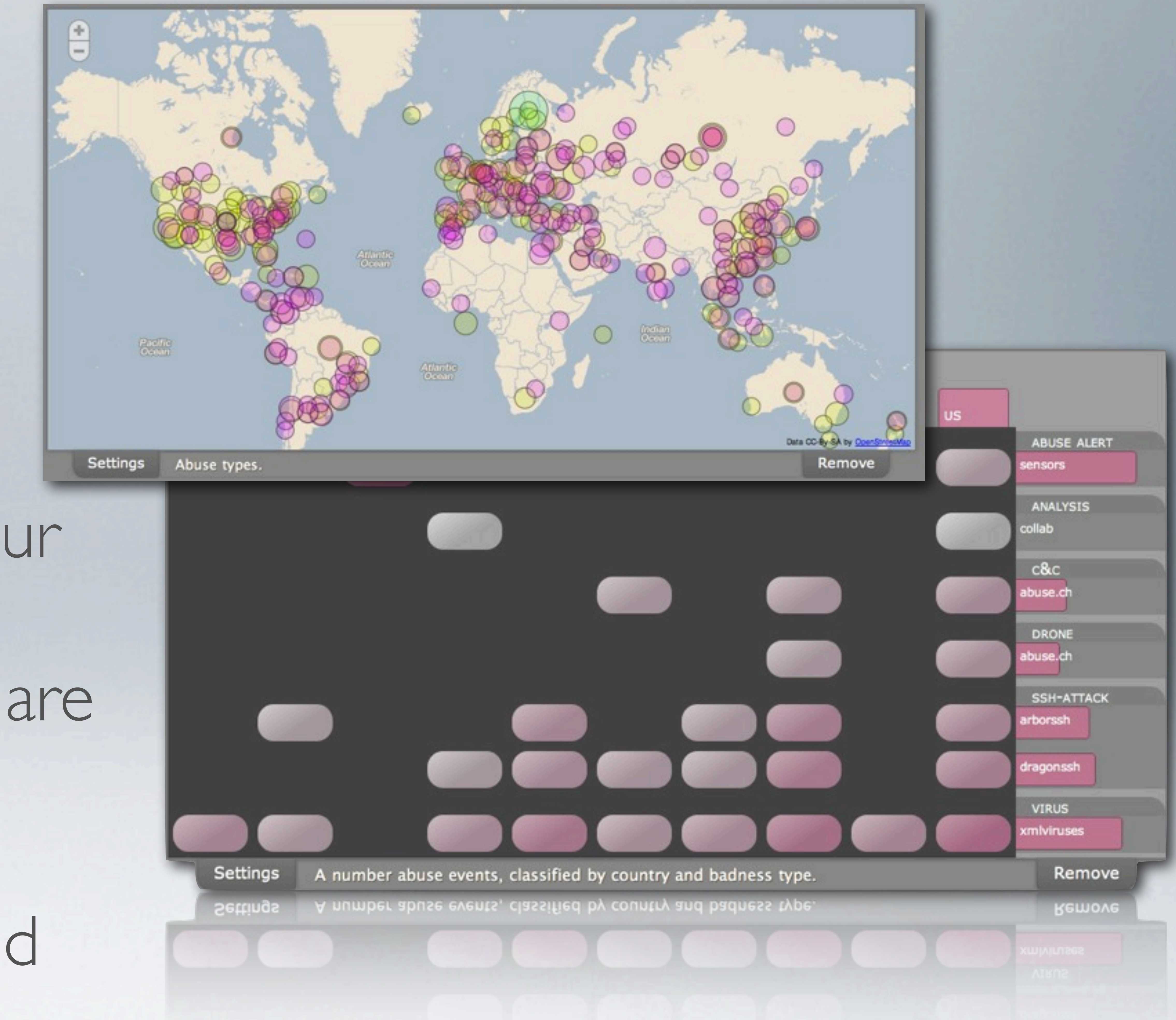
- A tool for collecting and sharing suspected malicious activity
- Botnet inspired architecture
  - Distributed
  - Modular
  - Bot for each specific task
    - Build for various feed formats, download mechanisms, augmenting, sanitizing, normalizing, reporting
- Based on **6** CERT-FI and **2** CERT-EE generations of abuse handling automata
- **Fully automatic**

ABUSEHELPER BENEFITS

- **Handle more Abuse with less effort**:
  - With AbuseHelper you are able to consume more information sources than ever!
- **Stay up to date with newest feeds**:
  - New Abuse Feeds pop up on monthly basis. Some of them are specializing on latest threats, which you want to be aware of. In typical case you have incorporated new feed to your AbuseHelper within a week from discovery.
- **Save time & effort**:
  - Automate mundane tasks, such as abuse & incident data collection and reporting. Skip the bootstrapping time needed to build your own solution from the ground-up.
- **Modularity & extensibility**:
  - Bring together information from sources with wildly varying qualities (e.g. streaming real time data, daily mail reports, periodically polled HTTP resources, different data formats).
- **Robustness & scalability**:
  - With its botnet inspired architecture AbuseHelper is an extremely robust and scalable solution.
- **Sharing & collaboration**:
  - Benefit from the know-how of other similar actors, share yours to benefit them.
- **Open source for a closed community**:
  - Scalable, robust and actively developed open core, while still allowing non-publicly available extensions.

VSROOM

- Taps into stream of events and provides real-time visualizations
- Map based views, classification views, text based views.
- Benefits:
  - See up-to-date situation from your perspective:
    - National: how different nations are coping with abuse
    - Organizational: how large enterprises suborganizations and subcontractors are doing.

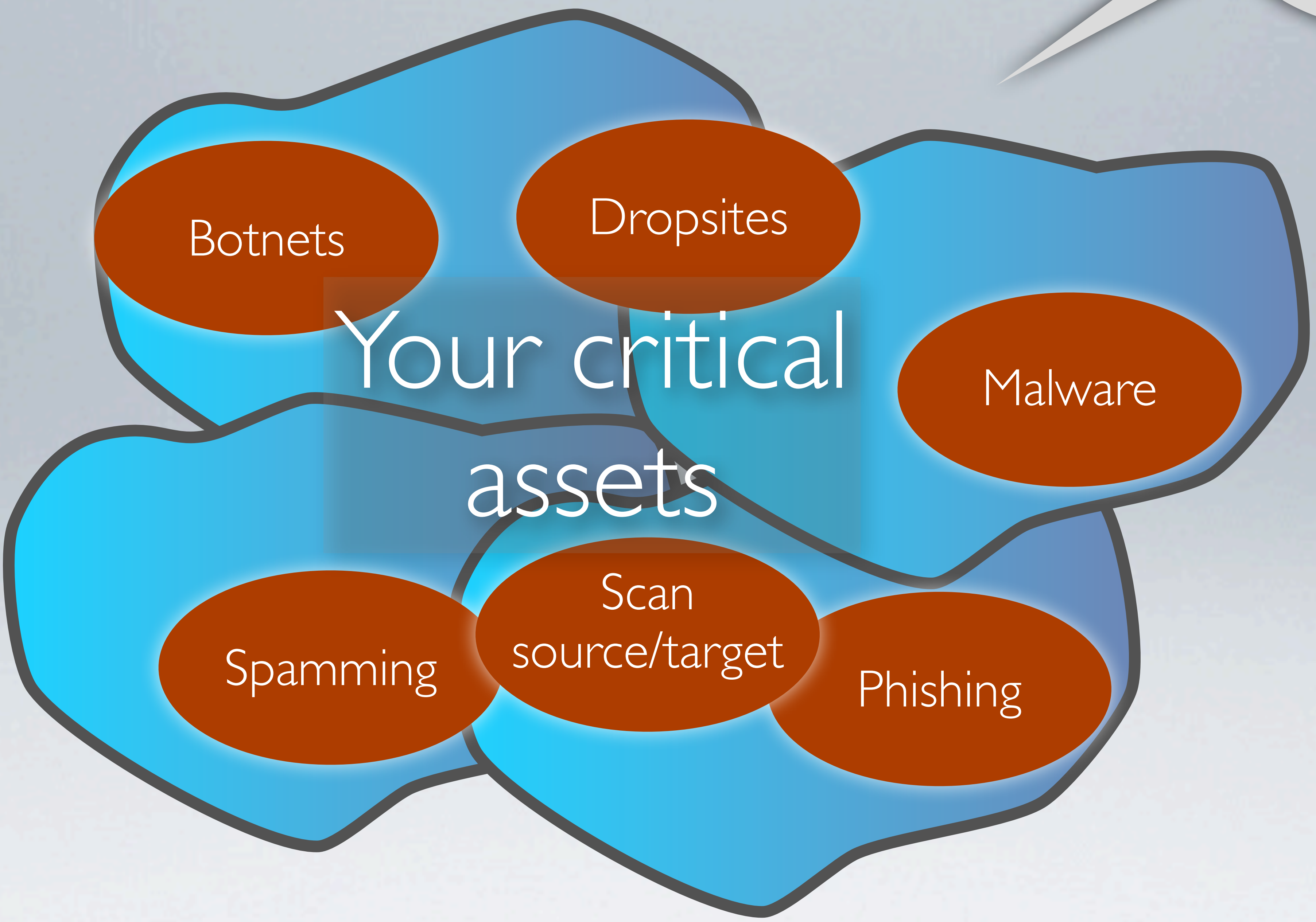


A number abuse events, classified by country and badness type.

HOW IS THIS DIFFERENT FROM IDS/IPS?

The world watches you. AbuseHelper helps you to stay on top of what others know about our security incidents

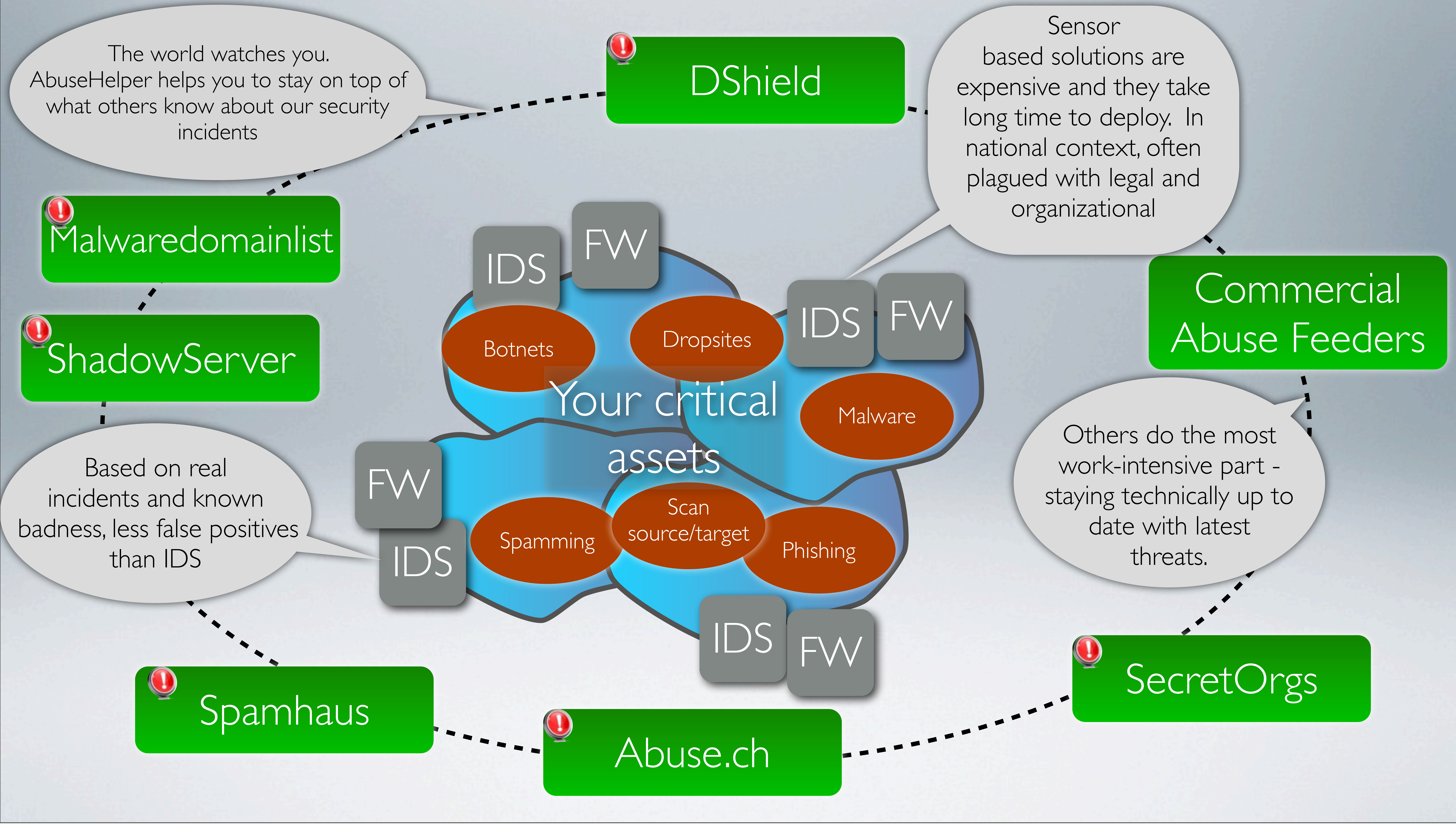
Sensor based solutions are expensive and they take long time to deploy. In national context, often plagued with legal and organizational



Based on real incidents and known badness, less false positives than IDS

Others do the most work-intensive part - staying technically up to date with latest threats.

HOW IS THIS DIFFERENT FROM IDS/IPS?



The world watches you. AbuseHelper helps you to stay on top of what others know about our security incidents

DShield

Sensor based solutions are expensive and they take long time to deploy. In national context, often plagued with legal and organizational

Malwaredomainlist

ShadowServer

Commercial Abuse Feeders

Others do the most work-intensive part - staying technically up to date with latest threats.

Based on real incidents and known badness, less false positives than IDS

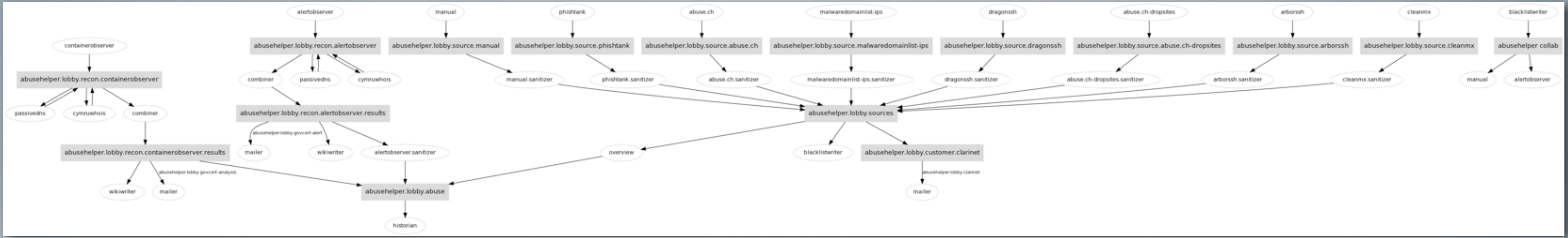
Spamhaus

Abuse.ch

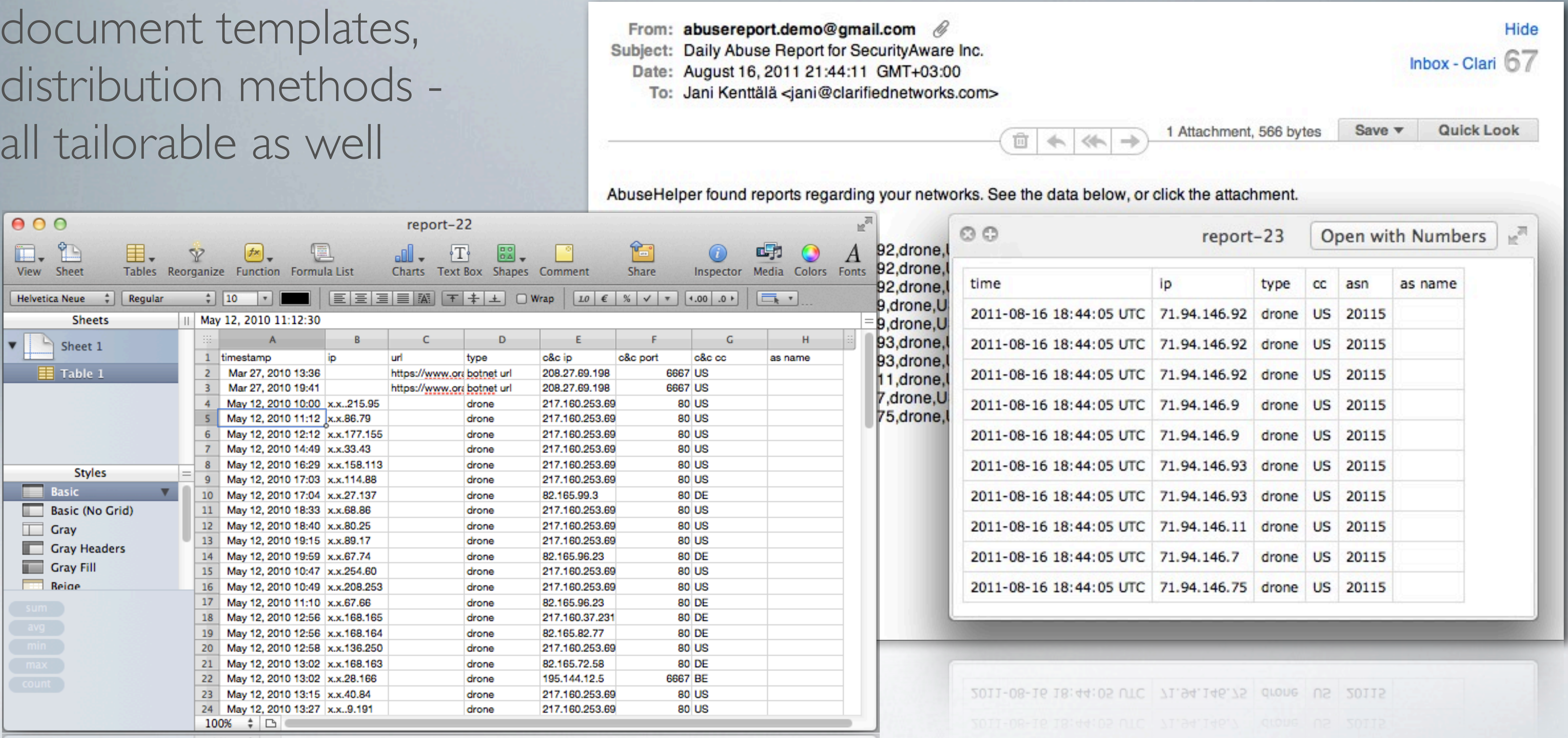
SecretOrgs

Your critical assets

EXAMPLE PROCESSING PIPELINE


containerobserver
abusehelper.lobby.recon.containerobserver
passivedns
cymruwhois
combiner
abusehelper.lobby.recon.containerobserver.results
wikiwriter
mailer
abusehelper.lobby.govcert-analysis
alertobserver
abusehelper.lobby.recon.alertobserver
combiner
passivedns
cymruwhois
abusehelper.lobby.recon.alertobserver.results
abusehelper.lobby.govcert-alert
mailer
wikiwriter
alertobserver.sanitizer
abusehelper.lobby.abuse
historian
manual
abusehelper.lobby.source.manual
manual.sanitizer
phishtank
abusehelper.lobby.source.phishtank
phishtank.sanitizer
abuse.ch
abusehelper.lobby.source.abuse.ch
abuse.ch.sanitizer
malwaredomainlist-ips
abusehelper.lobby.source.malwaredomainlist-ips
malwaredomainlist-ips.sanitizer
dragonssh
abusehelper.lobby.source.dragonssh
dragonssh.sanitizer
abuse.ch-dropsites
abusehelper.lobby.source.abuse.ch-dropsites
abuse.ch-dropsites.sanitizer
arborssh
abusehelper.lobby.source.arborssh
arborssh.sanitizer
cleanmx
abusehelper.lobby.source.cleanmx
cleanmx.sanitizer
abusehelper.lobby.sources
overview
blacklistwriter
abusehelper.lobby.customer.clarinet
abusehelper.lobby.clarinet
mailer
blacklistwriter
abusehelper collab
manual
alertobserver

- Reports are fully tailorable
  - For example add inter-organizational details
- Report timing (real time, periodic), document templates, distribution methods - all tailorable as well



From: abusereport.demo@gmail.com
Subject: Daily Abuse Report for SecurityAware Inc.
Date: August 16, 2011 21:44:11 GMT+03:00
To: Jani Kenttälä <jani@clarifiednetworks.com>

1 Attachment, 566 bytes

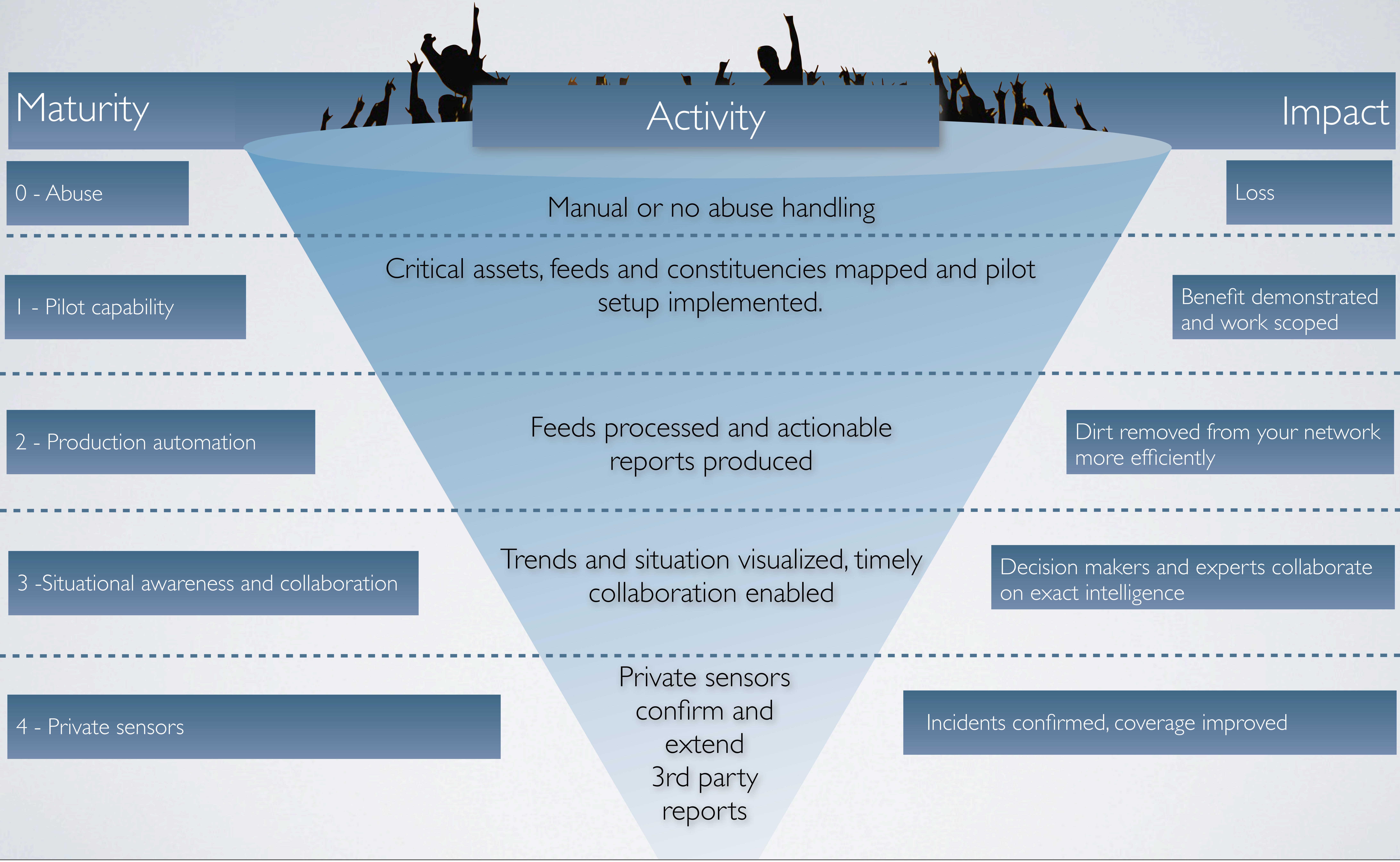
AbuseHelper found reports regarding your networks. See the data below, or click the attachment.

```
92,drone,
92,drone,
92,drone,
9,drone,U
9,drone,U
93,drone,
93,drone,
11,drone,
7,drone,U
75,drone,
```

May 12, 2010 11:12:30

	A	B	C	D	E	F	G	H
1	timestamp	ip	url	type	c&c ip	c&c port	c&c cc	as name
2	Mar 27, 2010 13:36		https://www.ora	botnet url	208.27.69.198	6667	US	
3	Mar 27, 2010 19:41		https://www.ora	botnet url	208.27.69.198	6667	US	
4	May 12, 2010 10:00	x.x..215.95		drone	217.160.253.69	80	US	
5	May 12, 2010 11:12	x.x.86.79		drone	217.160.253.69	80	US	
6	May 12, 2010 12:12	x.x.177.155		drone	217.160.253.69	80	US	
7	May 12, 2010 14:49	x.x.33.43		drone	217.160.253.69	80	US	
8	May 12, 2010 16:29	x.x.158.113		drone	217.160.253.69	80	US	
9	May 12, 2010 17:03	x.x.114.88		drone	217.160.253.69	80	US	
10	May 12, 2010 17:04	x.x.27.137		drone	82.165.99.3	80	DE	
11	May 12, 2010 18:33	x.x.68.86		drone	217.160.253.69	80	US	
12	May 12, 2010 18:40	x.x.80.25		drone	217.160.253.69	80	US	
13	May 12, 2010 19:15	x.x.89.17		drone	217.160.253.69	80	US	
14	May 12, 2010 19:59	x.x.67.74		drone	82.165.96.23	80	DE	
15	May 12, 2010 10:47	x.x.254.60		drone	217.160.253.69	80	US	
16	May 12, 2010 10:49	x.x.208.253		drone	217.160.253.69	80	US	
17	May 12, 2010 11:10	x.x.67.66		drone	82.165.96.23	80	DE	
18	May 12, 2010 12:56	x.x.168.165		drone	217.160.37.231	80	DE	
19	May 12, 2010 12:56	x.x.168.164		drone	82.165.82.77	80	DE	
20	May 12, 2010 12:58	x.x.136.250		drone	217.160.253.69	80	US	
21	May 12, 2010 13:02	x.x.168.163		drone	82.165.72.58	80	DE	
22	May 12, 2010 13:02	x.x.28.166		drone	195.144.12.5	6667	BE	
23	May 12, 2010 13:15	x.x.40.84		drone	217.160.253.69	80	US	
24	May 12, 2010 13:27	x.x..9.191		drone	217.160.253.69	80	US	

time	ip	type	cc	asn	as name
2011-08-16 18:44:05 UTC	71.94.146.92	drone	US	20115	
2011-08-16 18:44:05 UTC	71.94.146.92	drone	US	20115	
2011-08-16 18:44:05 UTC	71.94.146.92	drone	US	20115	
2011-08-16 18:44:05 UTC	71.94.146.9	drone	US	20115	
2011-08-16 18:44:05 UTC	71.94.146.9	drone	US	20115	
2011-08-16 18:44:05 UTC	71.94.146.93	drone	US	20115	
2011-08-16 18:44:05 UTC	71.94.146.93	drone	US	20115	
2011-08-16 18:44:05 UTC	71.94.146.11	drone	US	20115	
2011-08-16 18:44:05 UTC	71.94.146.7	drone	US	20115	
2011-08-16 18:44:05 UTC	71.94.146.75	drone	US	20115	



Maturity	Activity	Impact
0 - Abuse	Manual or no abuse handling	Loss
1 - Pilot capability	Critical assets, feeds and constituencies mapped and pilot setup implemented.	Benefit demonstrated and work scoped
2 - Production automation	Feeds processed and actionable reports produced	Dirt removed from your network more efficiently
3 -Situational awareness and collaboration	Trends and situation visualized, timely collaboration enabled	Decision makers and experts collaborate on exact intelligence
4 - Private sensors	Private sensors confirm and extend 3rd party reports	Incidents confirmed, coverage improved

ROADMAP IN PRACTICE

- Pilot (maturity level 1)
  - sufficient integration to your environment to present tangible results
  - with CSIRT/CERT/Security team and decision makers
- Production (maturity levels 2-4)
  - full integration,
  - 24/7 operation,
  - reaching all stakeholders
- Typically done in 4 sprints