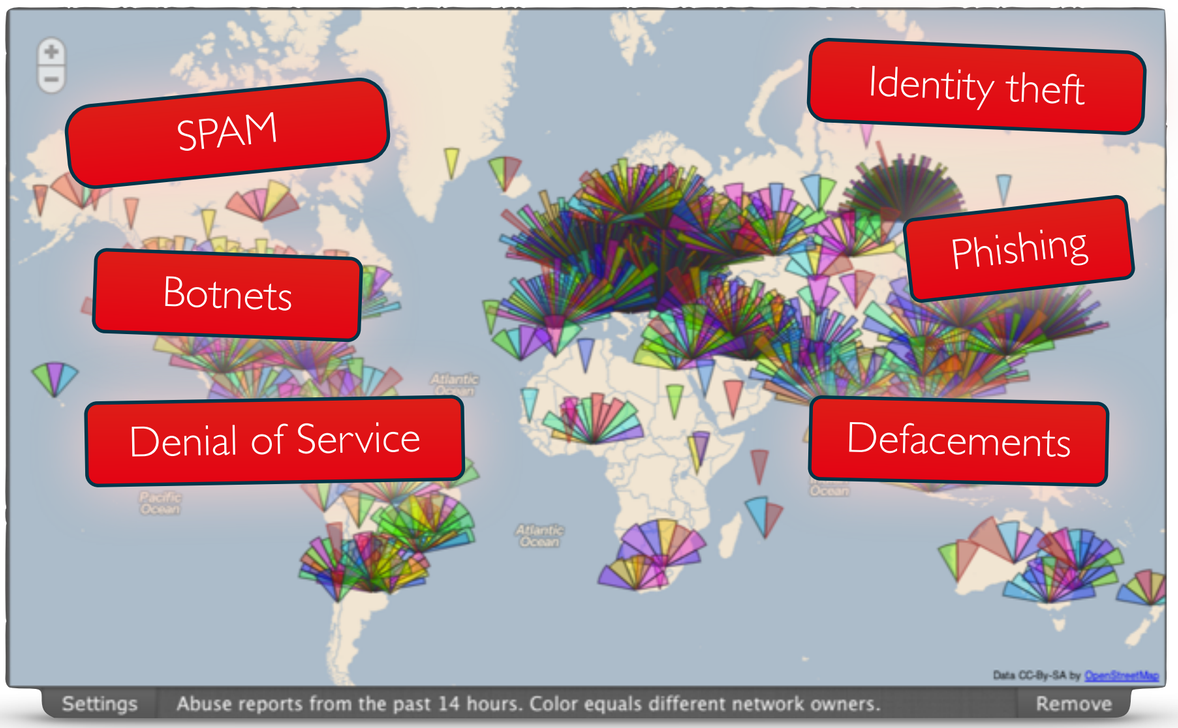
codenomicon

FINNISH CYBER DEFENSE MODEL

GUIDED TOUR



4th SEE RIPE NCC REGIONAL MEETING

@codenomicon

BACKGROUND

- Sindri Bjarnason - sindri@codenomicon.com
- Senior Solution Engineer at Codenomicon
- 3+ years founding the national CSIRT in Iceland (2011 - 2014)
- Currently working with various CSIRTs on topics related to abuse handling

OVERVIEW

- Finland’s National Cyber Security Strategy
- Meanwhile in Finland …
- NCSC-FI as the common denominator of success
- Examining the key components of NCSC-FI / NCSS
- Applicability of the Finnish model

NATIONAL CYBER SECURITY STRATEGIES

- Extensive NCSS documentation available on the ENISA website: https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/national-cyber-security-strategies-in-the-world
- The Finnish NCSS published in 2013 is located there: https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/FinlandsCyberSecurityStrategy.pdf

THE FINNISH NCSS

- The principles of “Cyber Security Management” on a national level
- Provides current state and future vision for the evolution of cyber security within Finland
- 10 “Strategic Guidelines” that encapsulate the primary components of the NCSS
- Is the Finnish NCSS <=> Finnish Defense Model?

NCSS <=> FINNISH DEFENSE MODEL?

- The NCSS can be seen as a focal document of the national cyber security framework
- However! The Finnish NCSS reflects heavily on the maturity of the IT ecosystem within Finland
- It does not provide an insight into the past/present evolution of its individual component
- *“These individual components are what makes the NCSS viable”*

MEANWHILE IN FINLAND ...

AREAS OF NOTEWORTHY SUCCESS

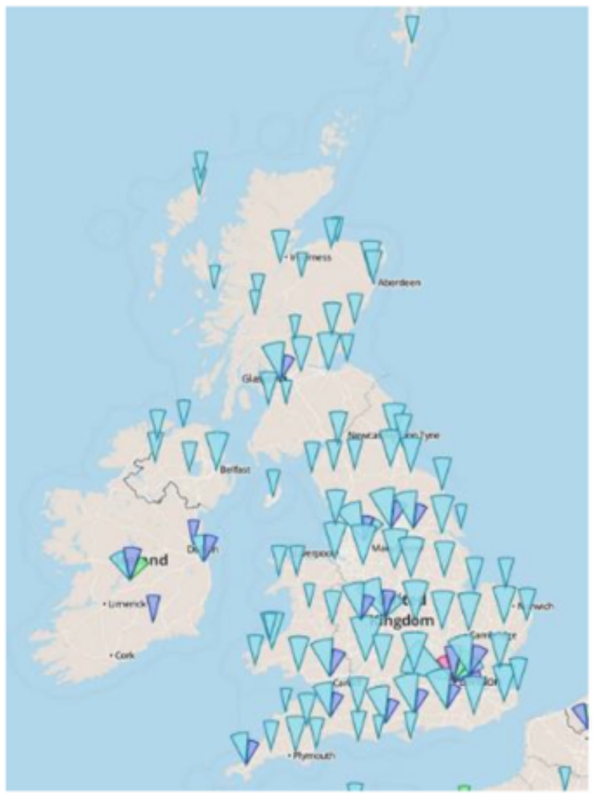
- Finland is ranked as the “cleanest” nation in terms of network abuse
- Mature IT / IT-SEC ecosystem
- International level:
  - Threat intelligence sharing across national borders
  - Multi-national network abuse response
- Active engagement with actors on the cyber security scene
  - National and international collaboration
  - Active dialog with the research / academic community
  - Established as a trusted source for information exchange

CERT-UK IN ACTION - INCIDENTS & VULNERABILITIES

CERT-UK

QUARTERLY REPORT

CERT-UK processes over 250,000 reports of 'abuse' every day



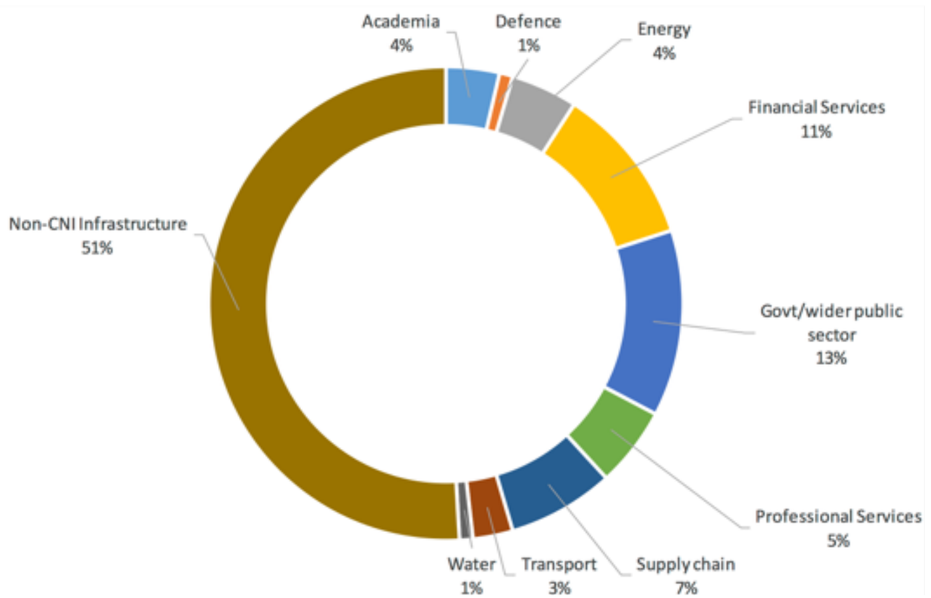
On CiSP, CERT-UK routinely publishes a list of the 'command and control' (C2) servers that we see being used by malware. This list is produced by the Fusion Cell and is aggregated from all of our feeds of commercial and non-commercial information. Using a specialist tool, we are able to take in over 250,000 reports of 'abuse' information that has been traced to the UK, every day. The 'abuse' could be anything from a botnet infected client to an IP address in the UK launching automated scans across the internet.

In addition to using this information to produce a list of C2 servers that businesses can use to identify malicious activity on their networks, CERT-UK provides an automated alerting system

Case Study: Heartbleed

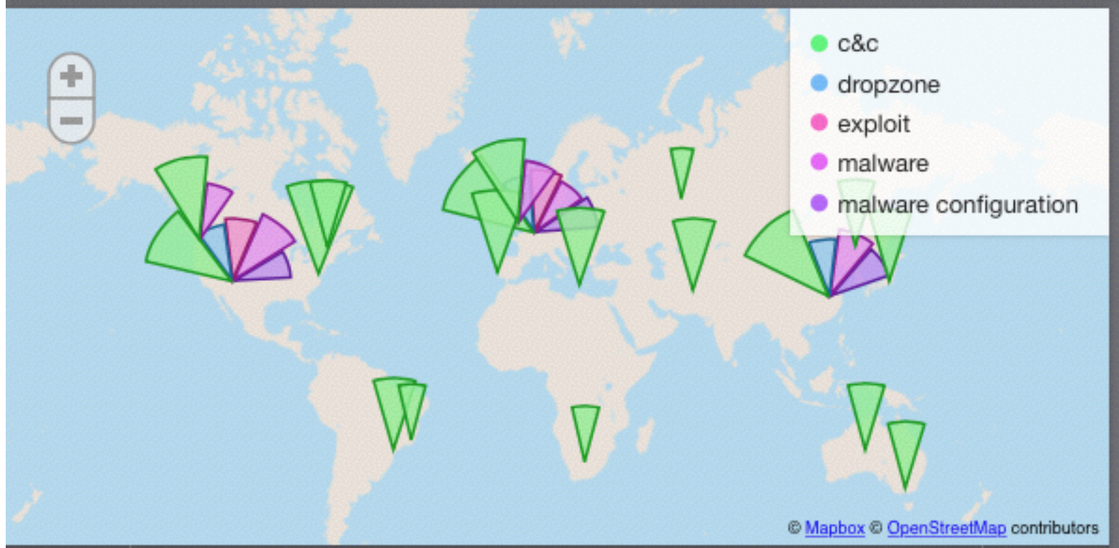
On 7 April a vulnerability disclosure by the OpenSSL team quickly gained worldwide attention in the technical press as well as significant coverage in the mainstream media. What made Heartbleed garner such widespread attention, and was it justified?

Trends per Sector

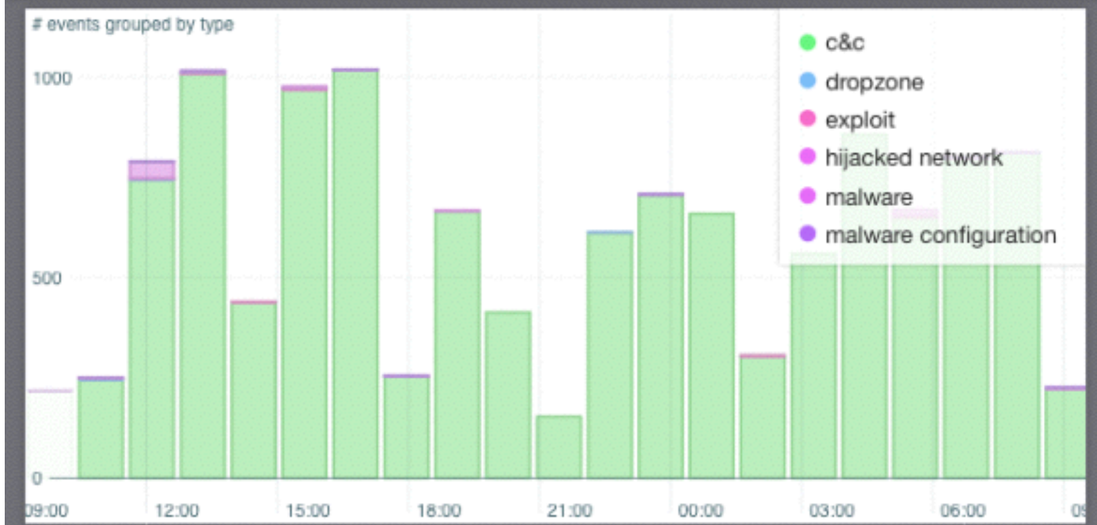


codenomicon

New view | Last 1 day | CODENOMICON | <No filter> | Share



Settings | <Unnamed view> | Remove



Settings | <Unnamed view> | Remove

# events	type	feed	description
12258	c&c	sandboxioc	This host is mos
17	c&c	abuse.ch	This host is mos
10	dropzone	abuse.ch	This host is mos
17	malware configuration	abuse.ch	This host is mos
1	hijacked network	spamhaus drop list	103.19.0.0/22 is
1	hijacked network	spamhaus drop list	103.18.248.0/22
14	c&c	abuse.ch	This host is mos
2	malware	abuse.ch	This host is mos
10	c&c	abuse.ch	The malicious se
17	exploit	autoshun	This host has tri
49	malware	malc0de	This host is mos
11	malware	vxvault	This host is mos
2	malware	mdl	This host is mos

Settings | Export | Incidence per Type | Remove

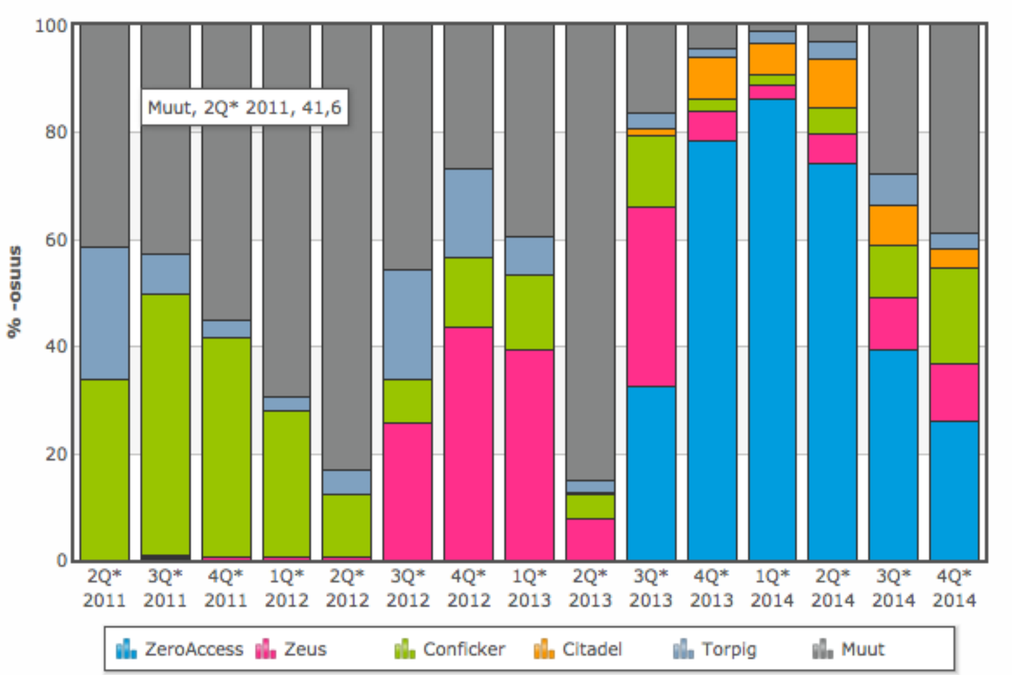
THE COMMON DENOMINATOR?

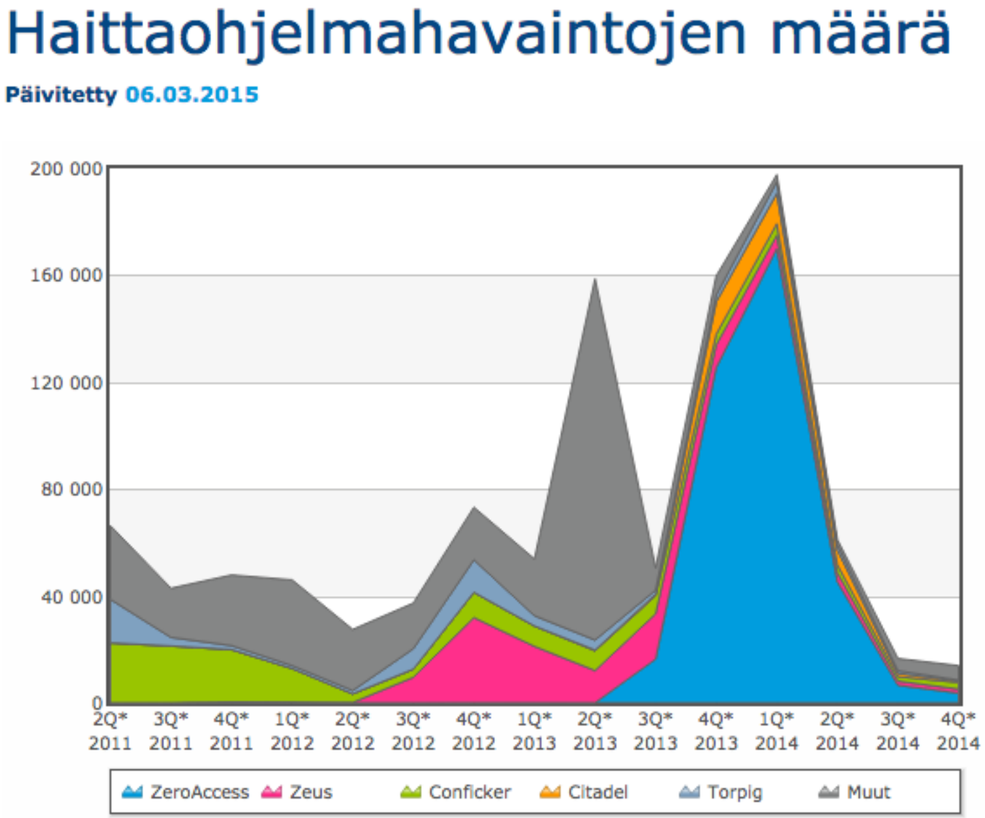
NCSC-FI, THE FINNISH NATIONAL CSIRT

- Established in 2001, “officially” operational in 2002
- Mostly ISP focused throughout 2005
- Early adopter of automated abuse handling (2006)
- Constituency expansion to CII (2006)
- Active CII protection role (~2013)
- Extensive service portfolio for its constituency and outside actors
- High maturity level

NCSC-FI: OPERATIONAL STATS

Kuvio A: Havaintojen kokonaismäärä





codenomicon

SUITABLE ROLE MODEL?

- By observing the evolution of NCSC-FI we can identify the components that play a key role in its current success
- Even with its civil scope, it is the entity in Finland with the highest rate of exposure to the challenges related to network abuse
- It stands to reason that these components will (with high probability) be contributing factors to the initial success of NCSS implementation
  - making sure these components are evaluated in the context of todays technical environment

KEY COMPONENTS

COLLABORATION
AUTOMATION
SITUATIONAL AWARENESS

COLLABORATION

CHALLENGE:

CREATE AND MAINTAIN AN ENVIRONMENT THAT SUPPORTS AND ENCOURAGES ACTIVE COLLABORATION BETWEEN NATIONAL ACTORS (AND LATER INTERNATIONAL ACTORS)

APPROACH:

IDENTIFY ACTIVE COLLABORATION SCENARIOS WITHIN THE IT-ECOSYSTEM AND INTEGRATE WITH IT. ESTABLISH SECTOR/ THREAT SPECIFIC WORKGROUPS. ACTIVE NETWORKING

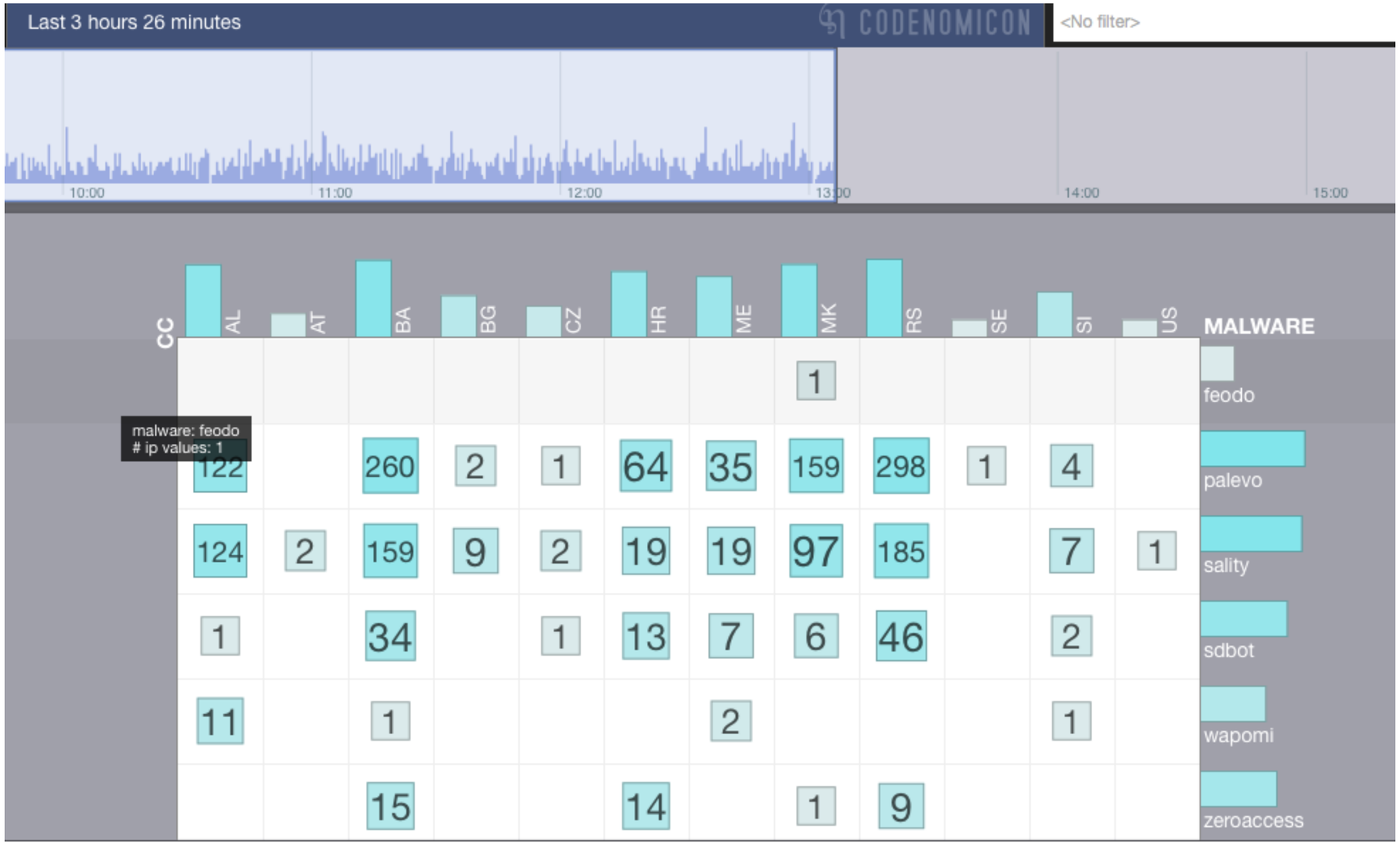
GOAL:

A TRUSTED COMMUNICATION NETWORK BETWEEN DIFFERENT ACTORS THAT ENABLES INTERNAL COMMUNICATION AS WELL AS COLLECTIVE RESPONSE

OBSERVATION:

A NEW ACTOR/AUTHORITY WILL START WITH LIMITED TRUST, BEING ABLE TO CONTRIBUTE INTERESTING DATA/INSIGHTS HELPS INITIALLY (NATIONAL SITUATIONAL AWARENESS)

NATIONAL SITUATIONAL AWARENESS



codenomicon

AUTOMATION

codenomicon

CHALLENGE:

OVER TIME THE AMOUNT OF REPORTED / OBSERVED NETWORK ABUSE WILL INCREASE DRASTICALLY AND RAPIDLY DECREASE THE UTILIZATION OF RESOURCES

APPROACH:

NCSC-FI WAS AN EARLY ADOPTER OF AUTOMATION BACK IN 2006. AT THE PRESENT VAST MAJORITY OF NETWORK ABUSE IS DEALT WITH THROUGH AUTOMATED PROCESSES

GOAL:

DEPLOY A FLEXIBLE FRAMEWORK THAT AUTOMATES FULLY THE FETCH-PROCESS-REPORT CYCLE OF ABUSE HANDLING

OBSERVATION:

THE EFFECTIVENESS OF AUTOMATION WILL ULTIMATELY BE IN RELATION TO THE ACTIVE COLLABORATION BETWEEN ACTORS

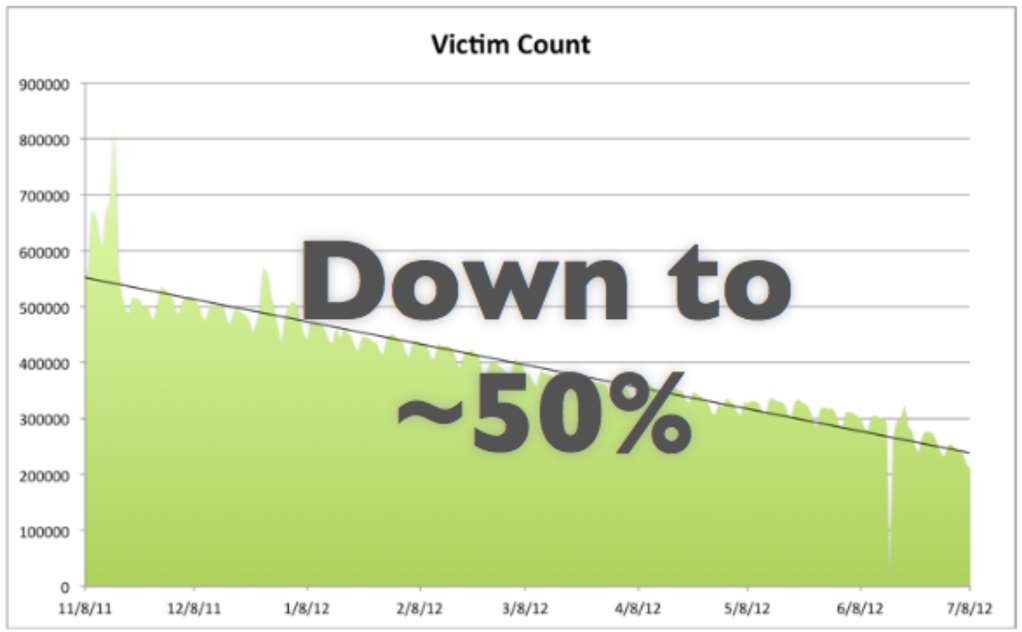
AUTOMATION

- Following the initial automation in 2006, NCSC-FI went from processing 1.000 incidents to 100.000 incidents that year
- On average NCSC-FI automatically handles ~200.000 incidents per year
- This allows them to focus their resources on more serious incidents requiring a managed approach
- The situational awareness will also benefit through automation, extending normal operations to campaigns
- Abuse automation has come a long way since 2006

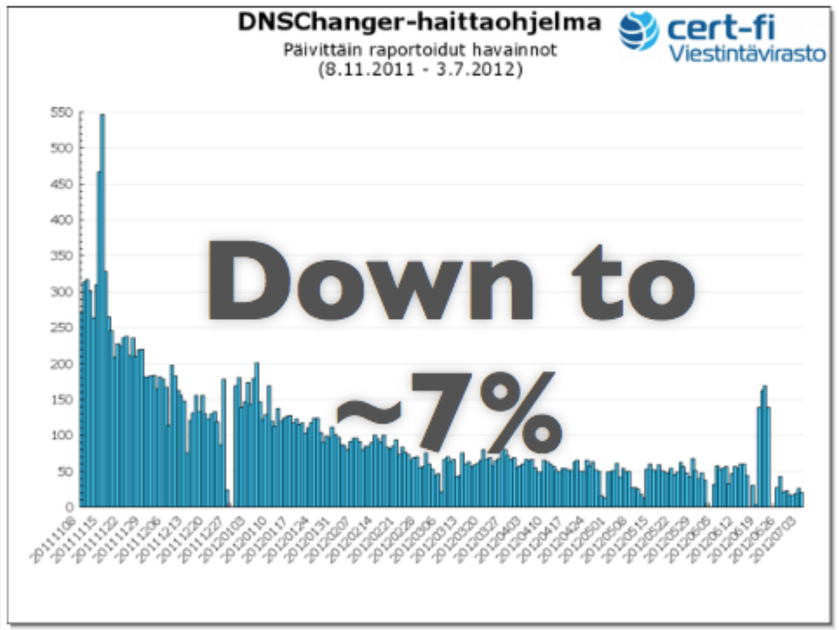
CAMPAIGNS THROUGH AUTOMATION

ALSO HIGH-PROFILE CASES DEALT EFFICIENTLY - CASE DNSCHANGER

World



Finland

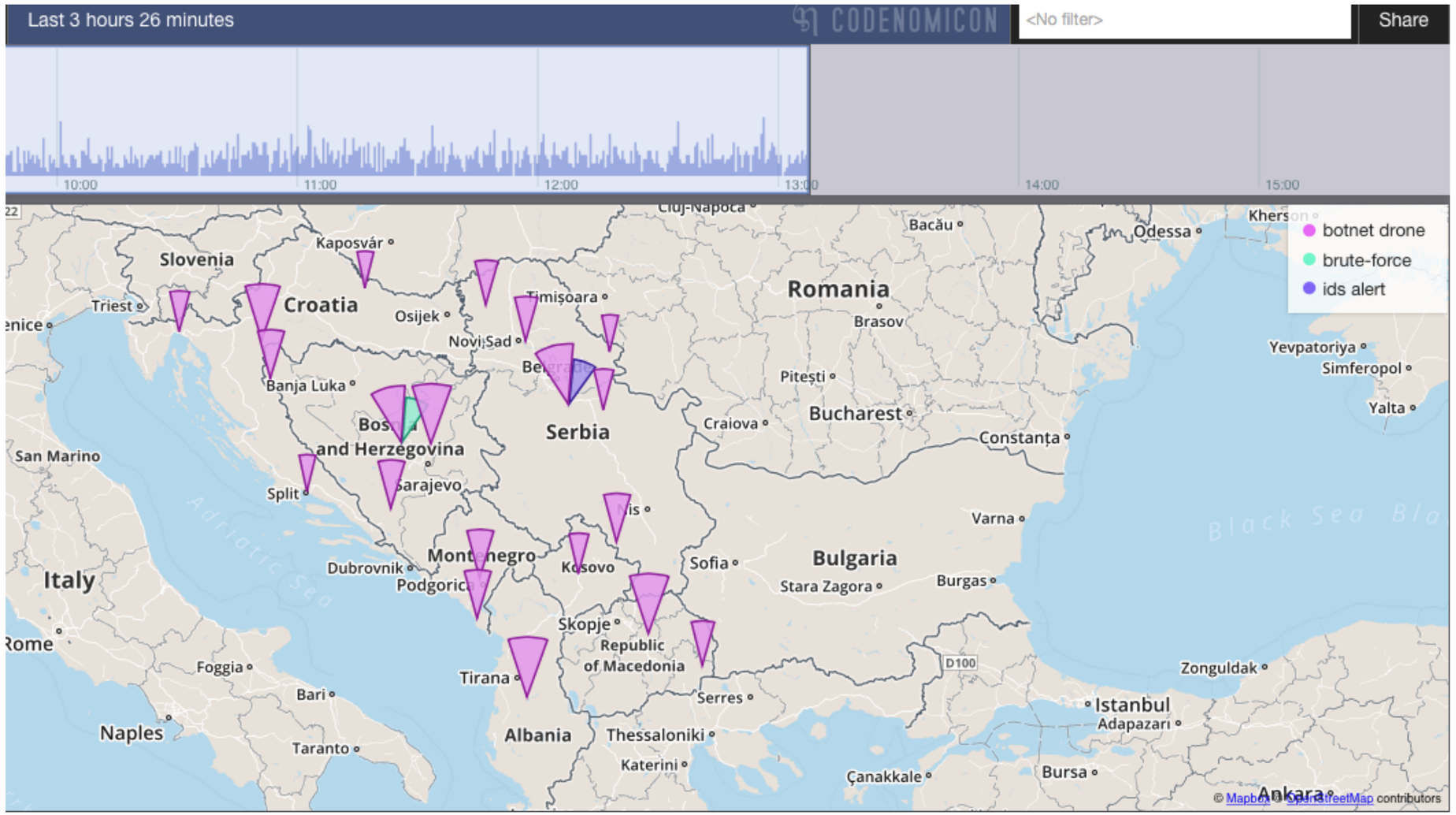


codenomicon

SITUATIONAL AWARENESS

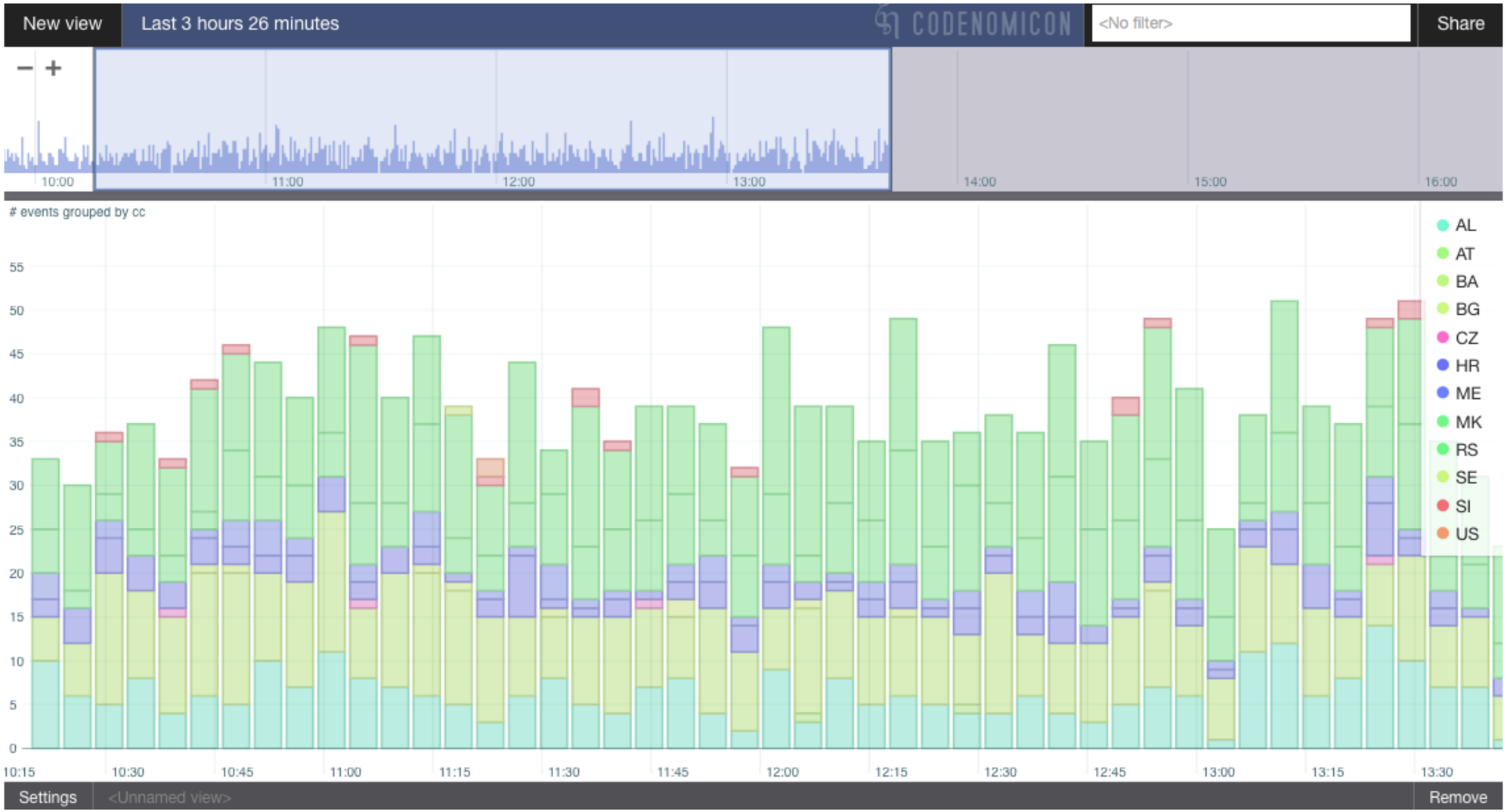
codenomicon

NATIONAL SITUATIONAL AWARENESS



codenomicon

NATIONAL SITUATIONAL AWARENESS

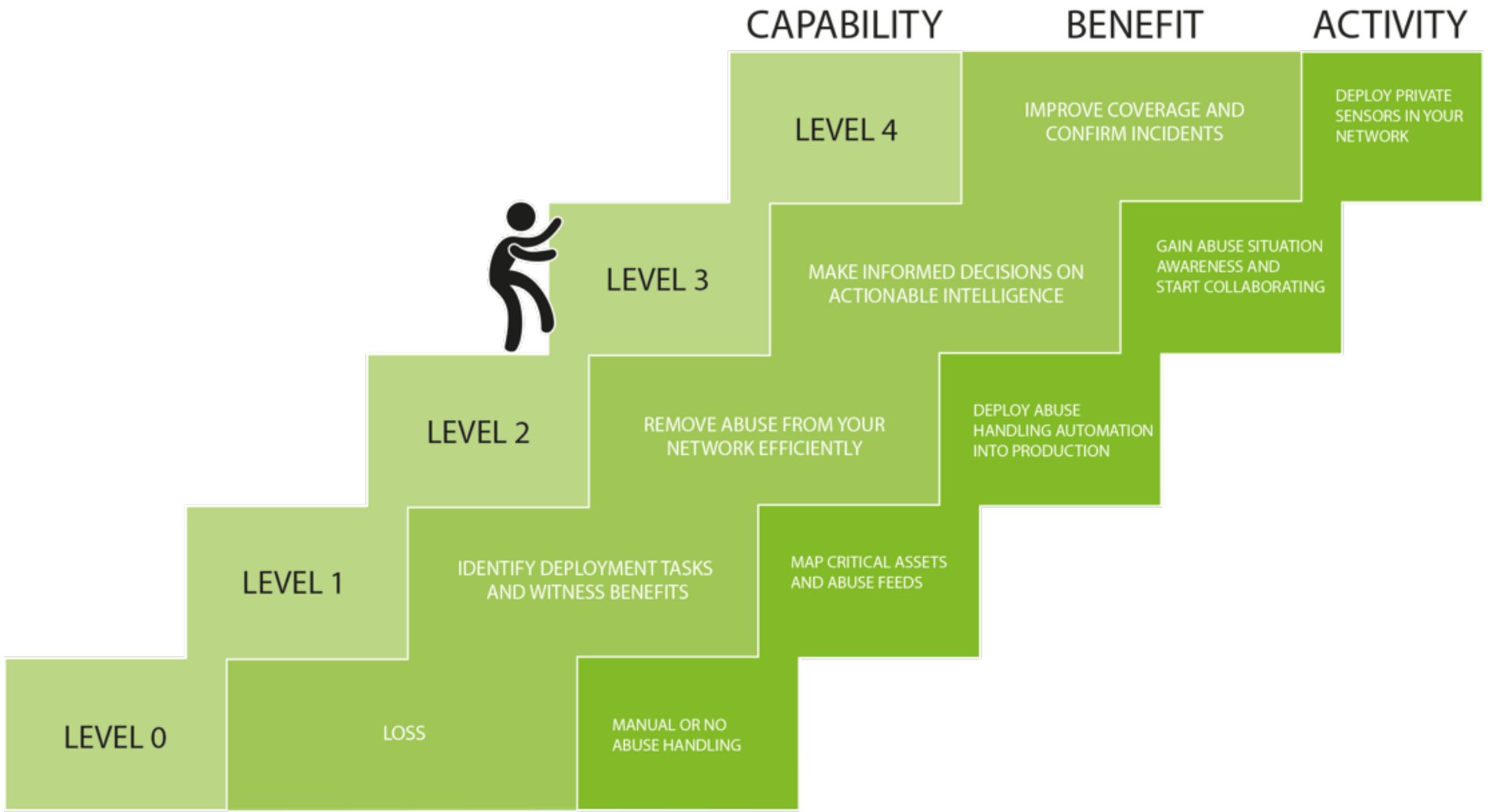


codenomicon

THOSE THREE COMPONENTS AND THEIR DERIVATIVES ARE THE FOUNDATION FOR 4 OF THE 10 NCSS STRATEGIC GUIDELINES

APPLICABILITY

THE STAIRWAY TO AWARENESS



codenomicon


codenomicon

REFERENCES

- AbuseHelper - automation framework for abuse handling:
  http://en.wikipedia.org/wiki/AbuseHelper
  http://www.codenomicon.com/products/abusesa/
- Establishing national CSIRT (CERT-CC):
  https://www.cert.org/incident-management/national-csirts/
- ENISA:
  https://www.enisa.europa.eu/activities/cert/support

ADDITIONAL SLIDES

START ON LEVEL 1 ...

Level 1:
Assets being identified, useful feeds known

codenomicon

Level 1: Assets being identified, useful feeds known	**Level 2:** Automated 24/7 abuse handling with common tools

Level 1: Assets being identified, useful feeds known	Level 2: Automated 24/7 abuse handling with common tools	Level 3: Situation Awareness

Insight over actual incidents
- Phenomena in the world and in the nation
  - For example vulnerable services, DDoS potential
- Proxy KPIs
- Cleaner benchmarks

Feeders

Proxy

Cleaners

Other Nations

codenomicon

Level 1: Assets being identified, useful feeds known	Level 2: Automated 24/7 abuse handling with common tools	Level 3: Situation Awareness	Level 4: Abuse Handling Expanded with sensors

Expanding coverage with IoC monitoring

Feeders

IOC SHARING

Proxy

IoCs

IoC Notifications

Unorganised Cleaners

Unorganised = organisations who do not have own sector-specific proxy

Other Nations

codenomicon

Level 1:
Assets being identified, useful feeds known

Level 2:
Automated 24/7 abuse handling with common tools

Level 3:
Situation Awareness

Level 4:
Abuse Handling Expanded with sensors

Feeders

IOC SHARING

Proxy

IoCs

IoC Notifications

Unorganised Cleaners

Other Nations

CI Sector Proxy

IoCs

IoC Notifications

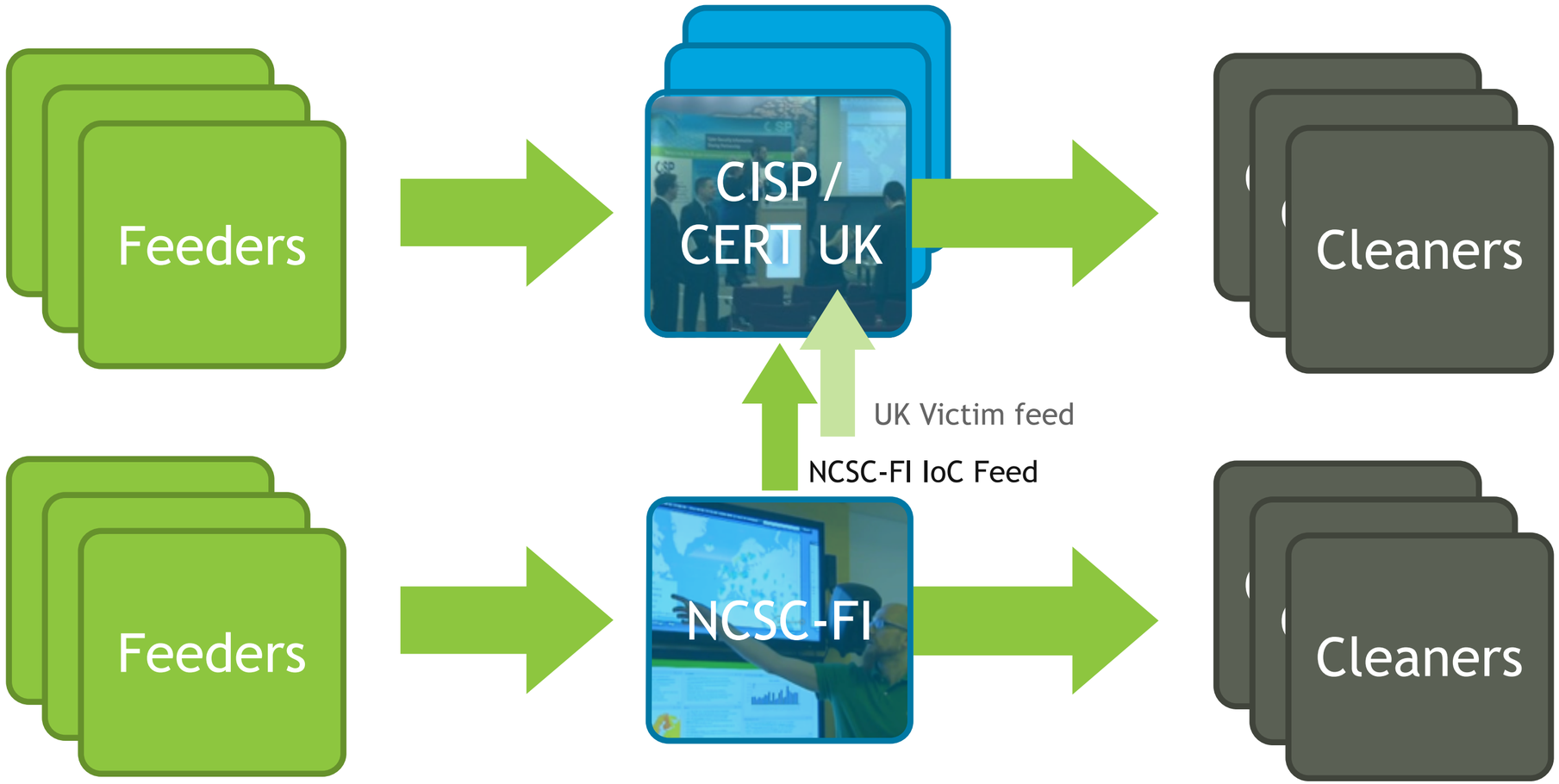
Organised Cleaners

Working with Sector Specific Proxies

codenomicon

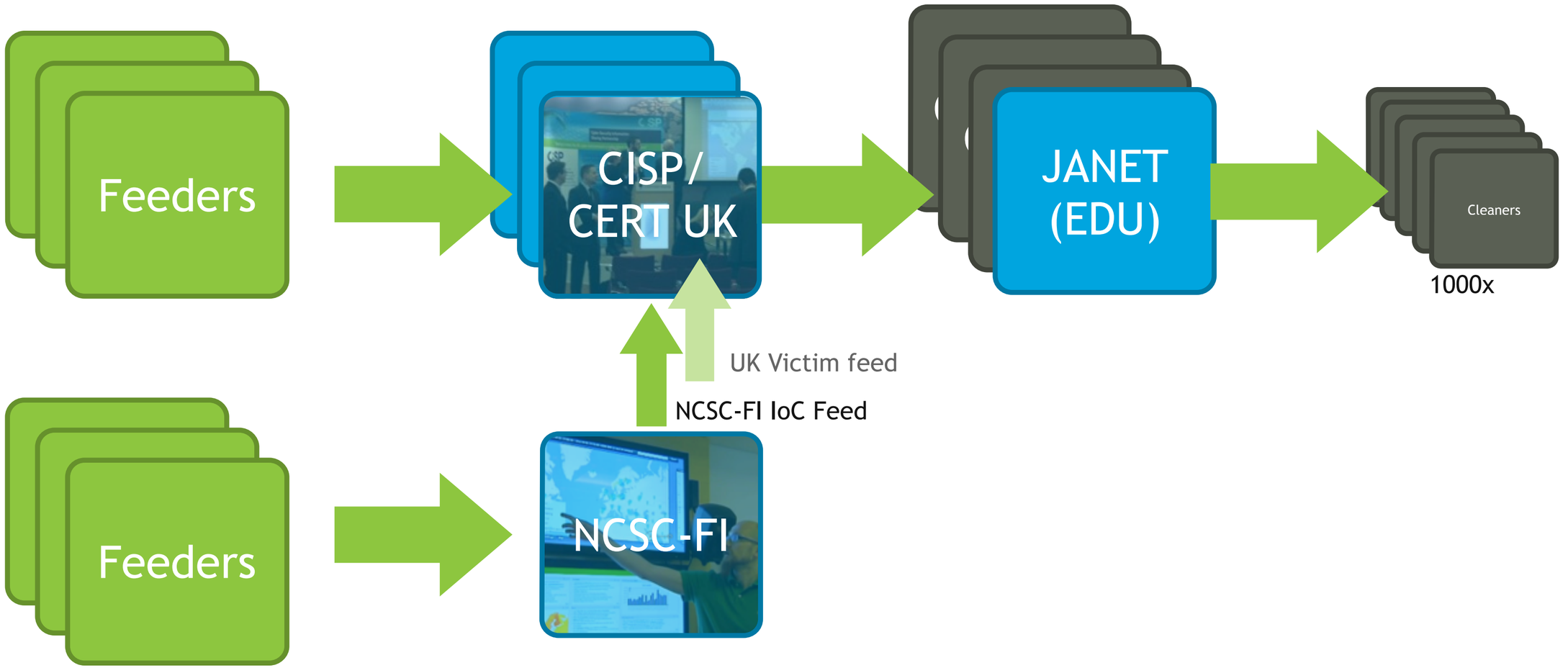
NATURAL GROWTH OF OPERATION

NATION-TO-NATION REALTIME IOC SHARING



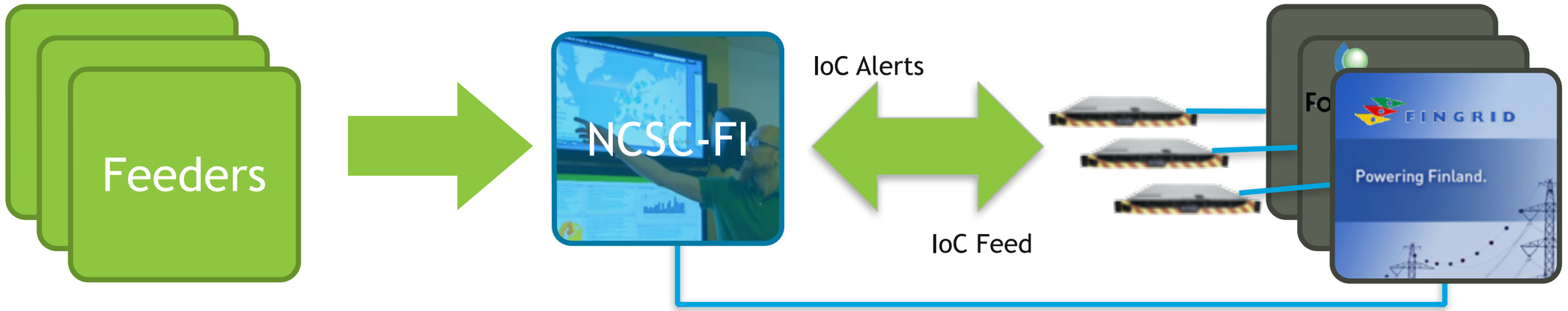
codenomicon

NATIONAL PUBLIC-PRIVATE PARTNERSHIPS

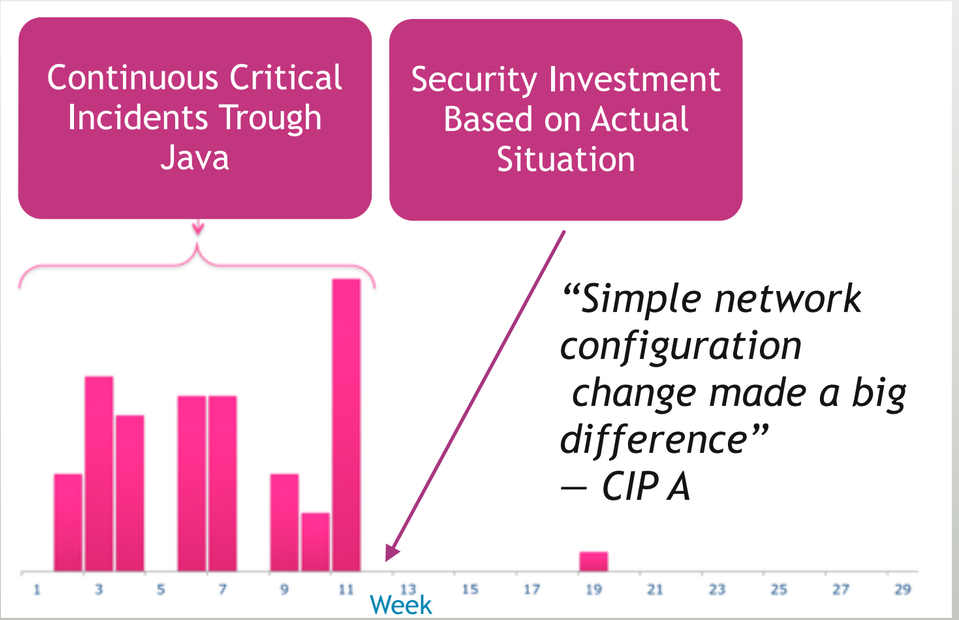


codenomicon

NATIONAL PUBLIC-PRIVATE PARTNERSHIPS

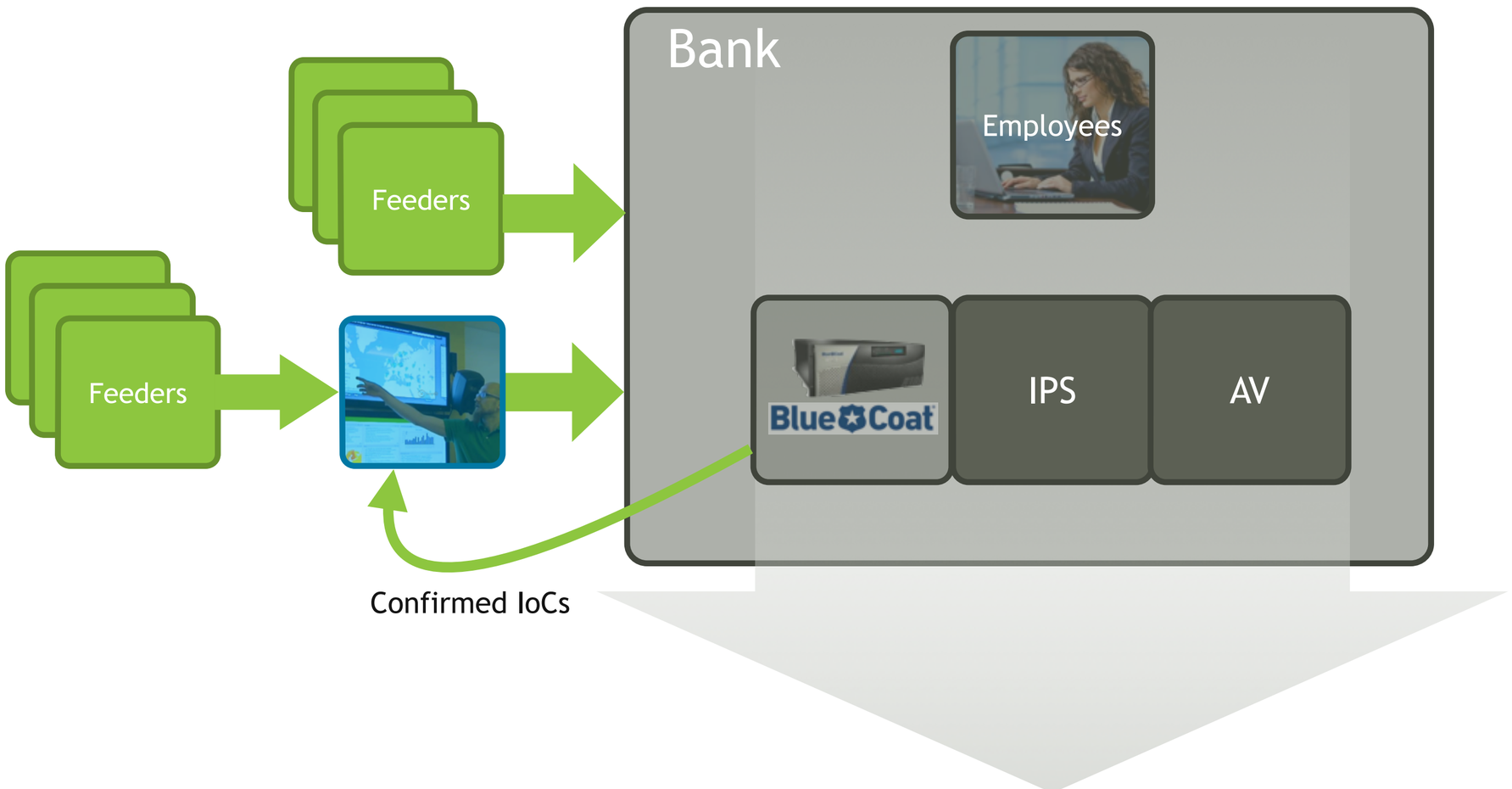


Reports
2013: Handled 15 million events, discovered 622 Critical Incidents



"After seeing actual incidents we decided to fix our incident response capability" — CIP B

PUBLIC-PRIVATE PARTNERSHIPS



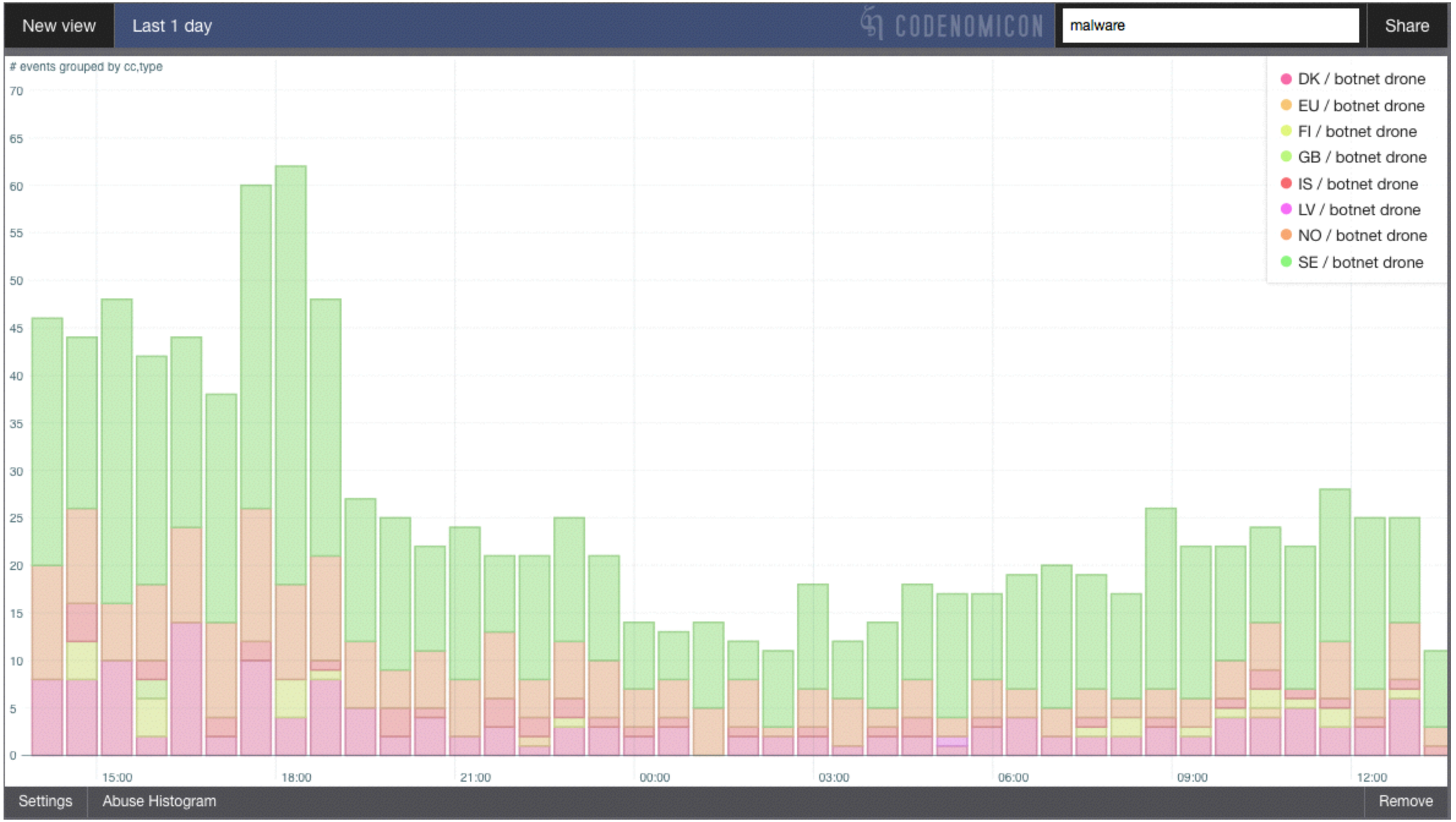
codenomicon

BEHIND THE CORNER …

SHARED SITUATIONAL AWARENESS ACROSS NATIONAL BORDERS

ENABLING LOCALIZED IOC’S TO COMPLEMENT A MULTI-NATIONAL SITUATIONAL AWARENESS

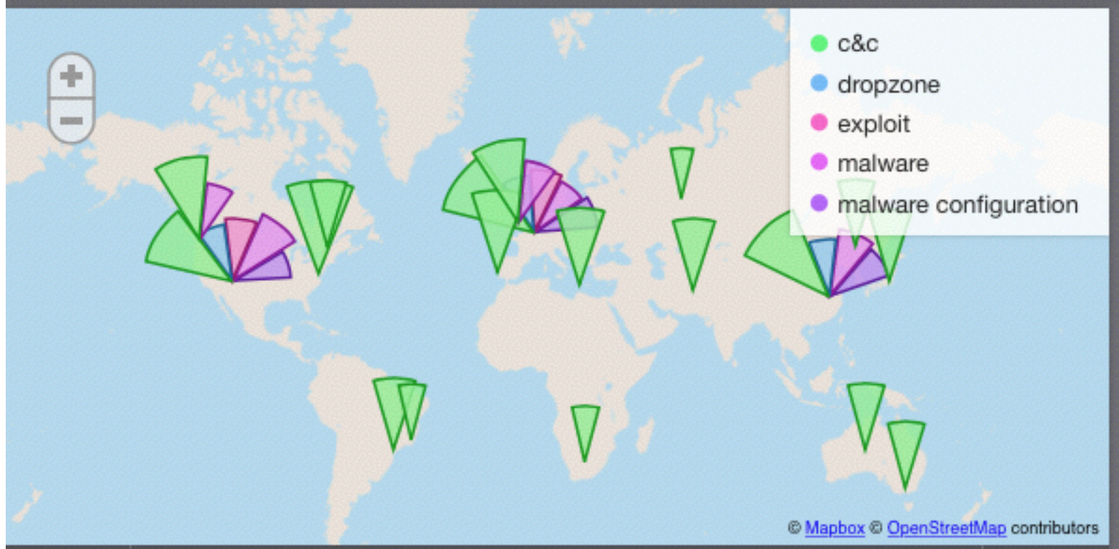
codenomicon


New view
Last 1 day
CODENOMICON
malware
Share
events grouped by cc,type
70
65
60
55
50
45
40
35
30
25
20
15
10
5
0
15:00
18:00
21:00
00:00
03:00
06:00
09:00
12:00
DK / botnet drone
EU / botnet drone
FI / botnet drone
GB / botnet drone
IS / botnet drone
LV / botnet drone
NO / botnet drone
SE / botnet drone
Settings
Abuse Histogram
Remove

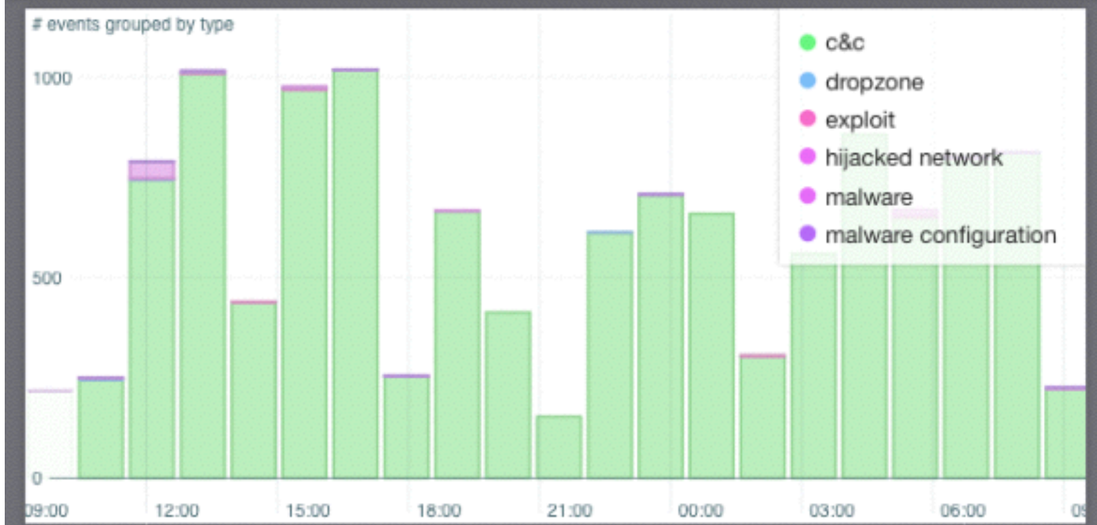
COMMON UNDERSTANDING OF CRIMINAL INFRASTRUCTURE EVOLUTION

COMPLEMENTED BY A FIXED-POINT STATE

New view | Last 1 day | CODENOMICON | <No filter> | Share



Settings | <Unnamed view> | Remove



Settings | <Unnamed view> | Remove

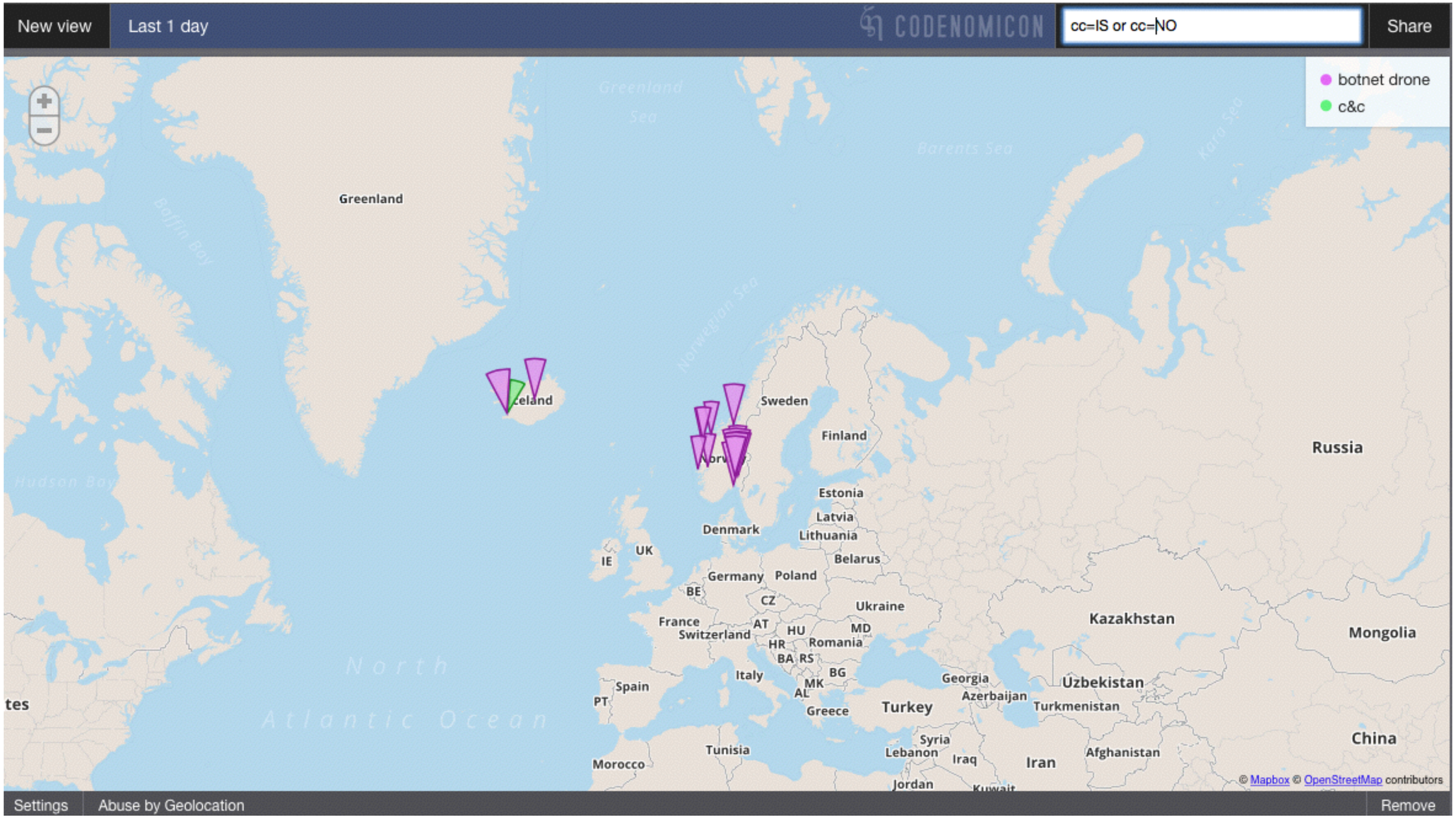
# events	type	feed	description
12258	c&c	sandboxioc	This host is mos
17	c&c	abuse.ch	This host is mos
10	dropzone	abuse.ch	This host is mos
17	malware configuration	abuse.ch	This host is mos
1	hijacked network	spamhaus drop list	103.19.0.0/22 is
1	hijacked network	spamhaus drop list	103.18.248.0/22
14	c&c	abuse.ch	This host is mos
2	malware	abuse.ch	This host is mos
10	c&c	abuse.ch	The malicious se
17	exploit	autoshun	This host has tri
49	malware	malc0de	This host is mos
11	malware	vxvault	This host is mos
2	malware	mdl	This host is mos

Settings | Export | Incidence per Type | Remove

ENABLING REALTIME MITIGATION BETWEEN NATION STATES

ENABLING SHARED MITIGATION THROUGH COMPATIBLE WORKFLOWS

codenomicon



codenomicon


codenomicon