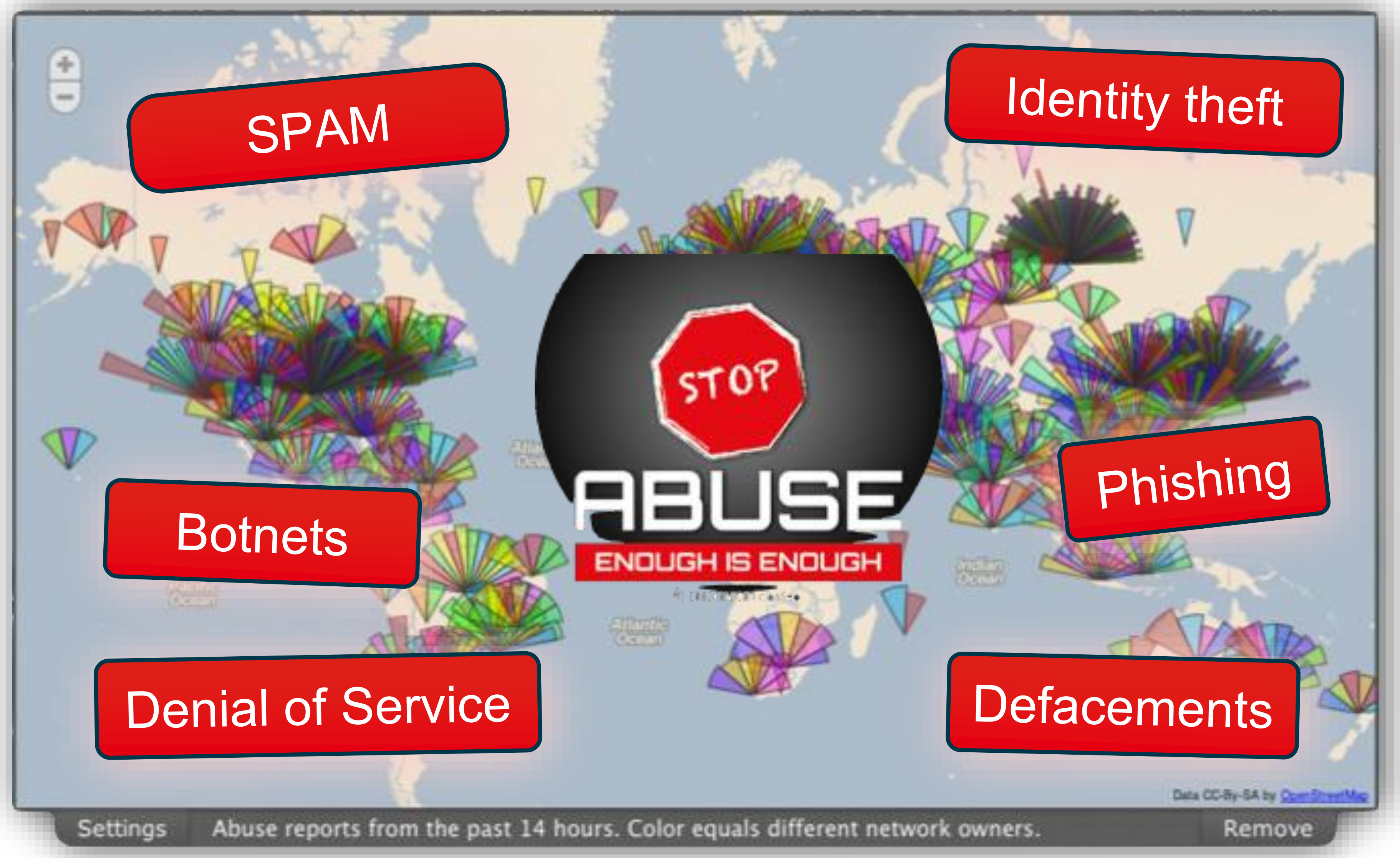
codenomicon

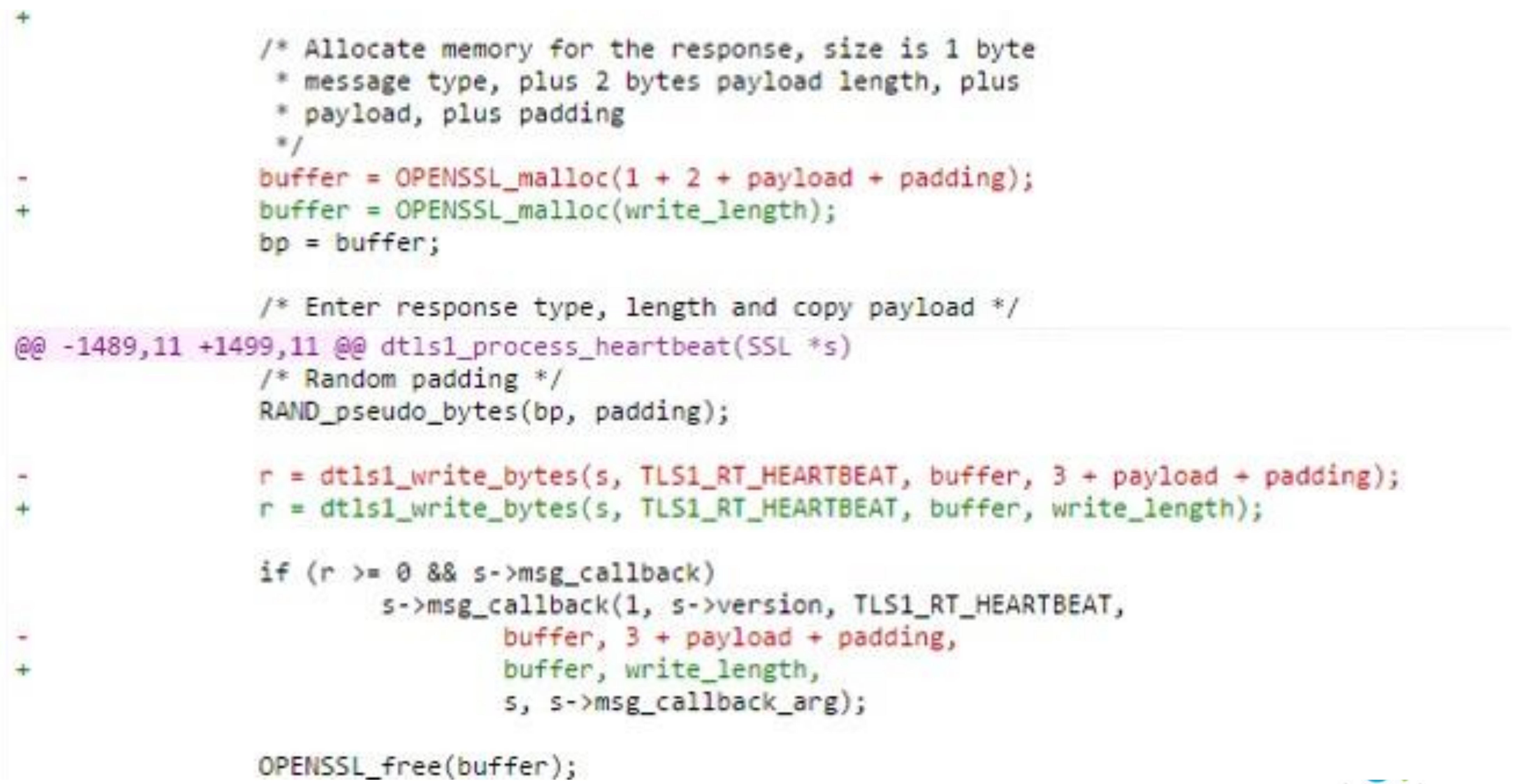
FINNISH APPROACH

Collaborative, threat-indicator based cyber defence.



Abuse reports from the past 14 hours. Color equals different network owners.

@codenomicon

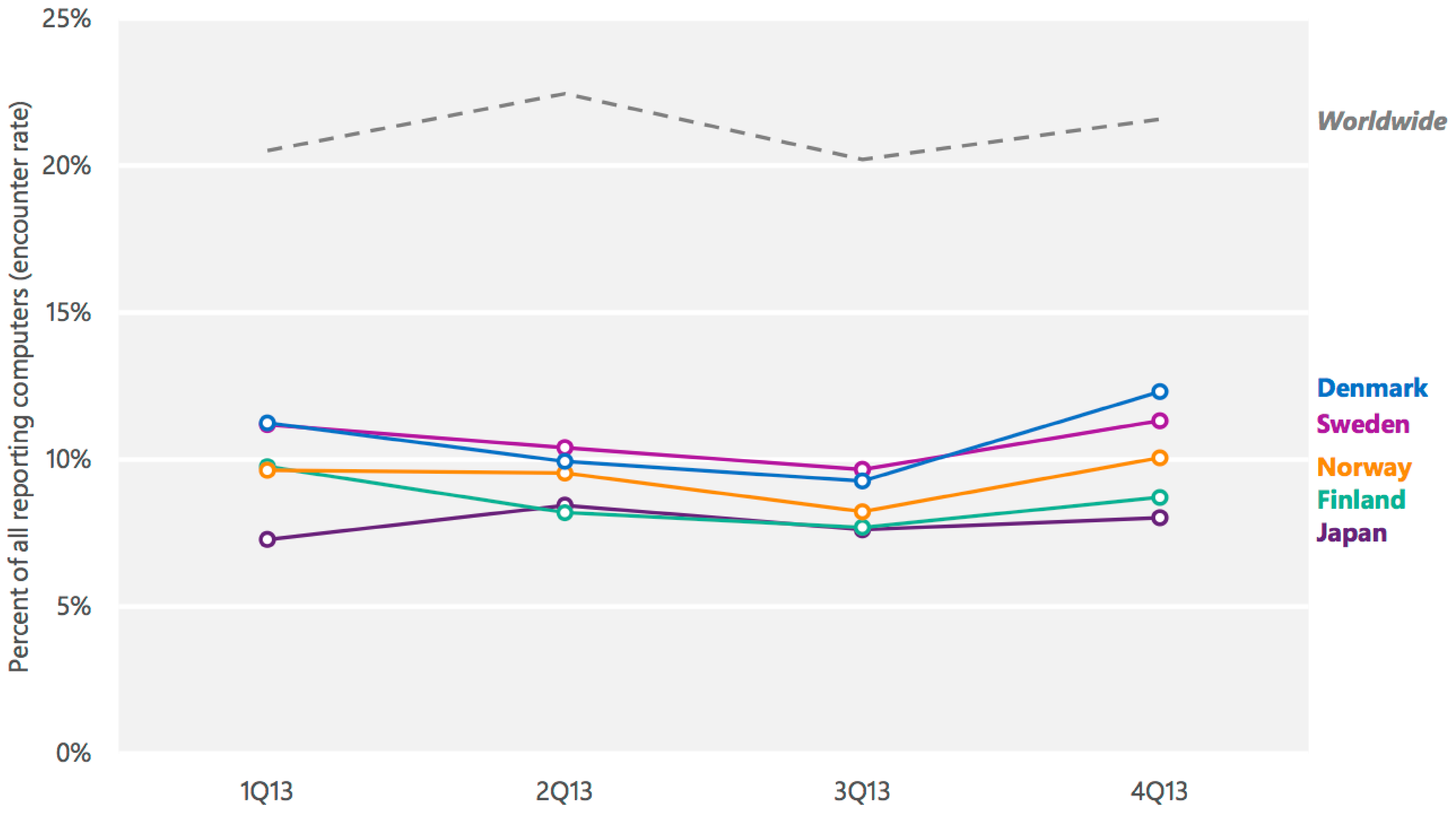


```
+
                /* Allocate memory for the response, size is 1 byte
                 * message type, plus 2 bytes payload length, plus
                 * payload, plus padding
                 */
-               buffer = OPENSSL_malloc(1 + 2 + payload + padding);
+               buffer = OPENSSL_malloc(write_length);
                bp = buffer;

                /* Enter response type, length and copy payload */
@@ -1489,11 +1499,11 @@ dtls1_process_heartbeat(SSL *s)
                /* Random padding */
                RAND_pseudo_bytes(bp, padding);

-               r = dtls1_write_bytes(s, TLS1_RT_HEARTBEAT, buffer, 3 + payload + padding);
+               r = dtls1_write_bytes(s, TLS1_RT_HEARTBEAT, buffer, write_length);

                if (r >= 0 && s->msg_callback)
                        s->msg_callback(1, s->version, TLS1_RT_HEARTBEAT,
-                               buffer, 3 + payload + padding,
+                               buffer, write_length,
                                s, s->msg_callback_arg);

                OPENSSL_free(buffer);
```

codenomicon

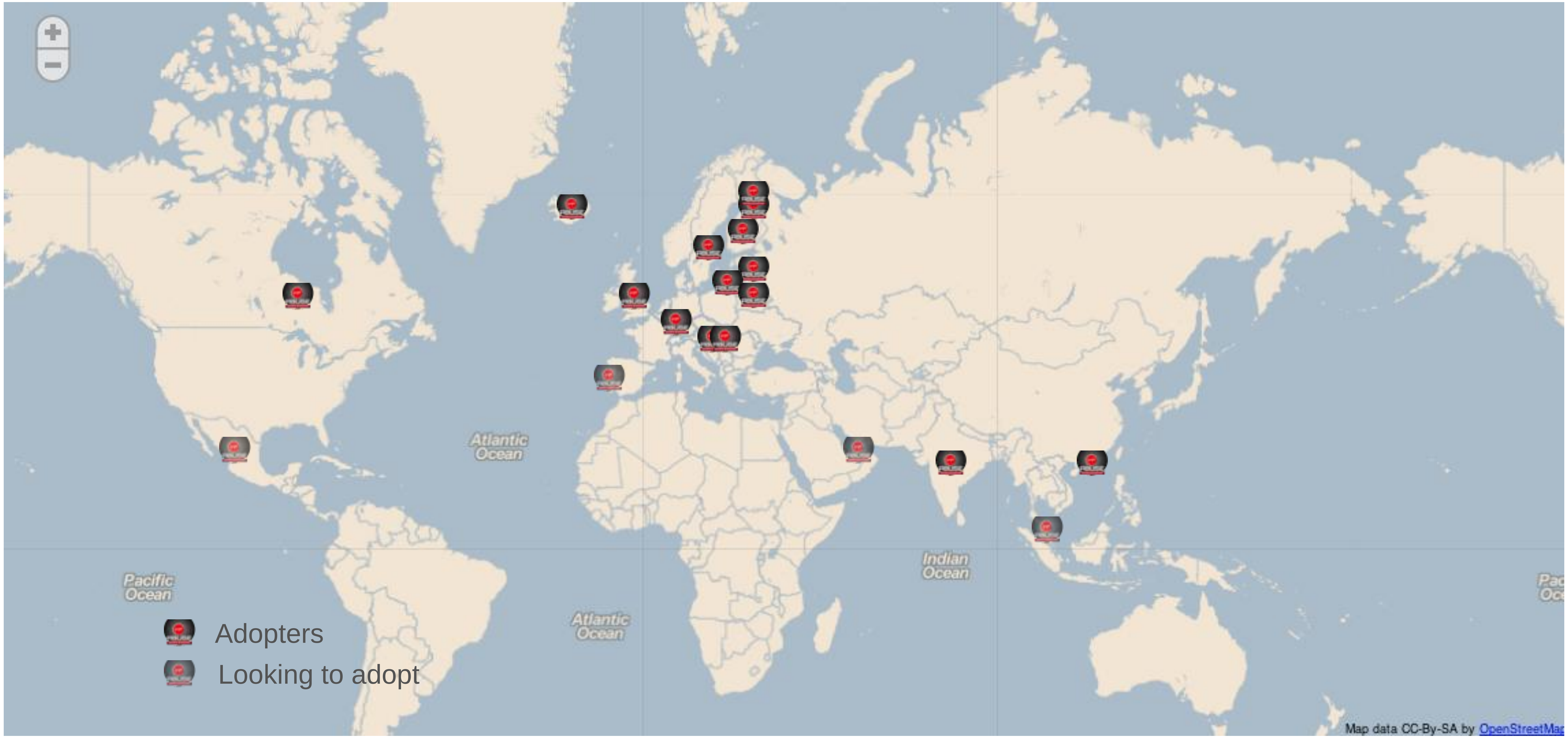
TODAY, FINLAND IS ONE OF THE CLEANEST COUNTRIES IN THE WORLD

Figure 34. Trends for locations with low malware encounter rates in 2H13 (100,000 reporting computers minimum)



Microsoft Security Intelligence Report Vol 16.

APPROACH GETTING POPULAR!

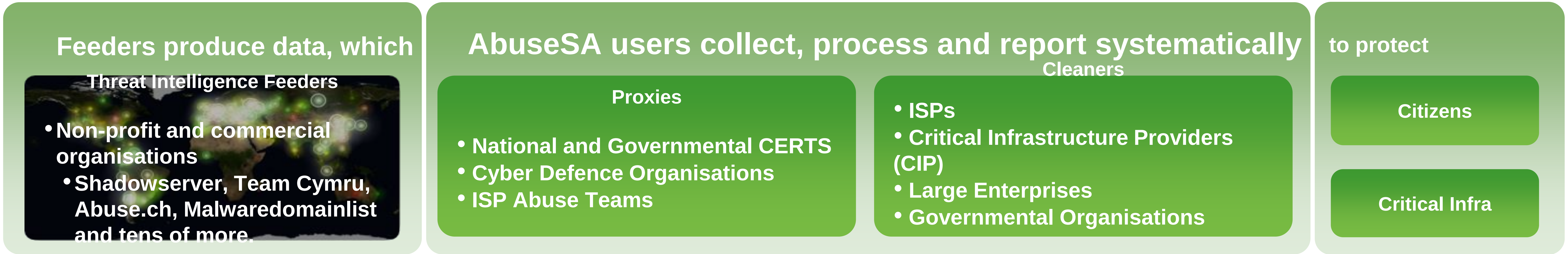


codenomicon

How does it work?

ACTORS

WHICH ONE ARE YOU?



Feeders produce data, which

Threat Intelligence Feeders

- Non-profit and commercial organisations
  - Shadowserver, Team Cymru, Abuse.ch, Malwaredomainlist and tens of more.

AbuseSA users collect, process and report systematically

Proxies

- National and Governmental CERTS
- Cyber Defence Organisations
- ISP Abuse Teams

Cleaners

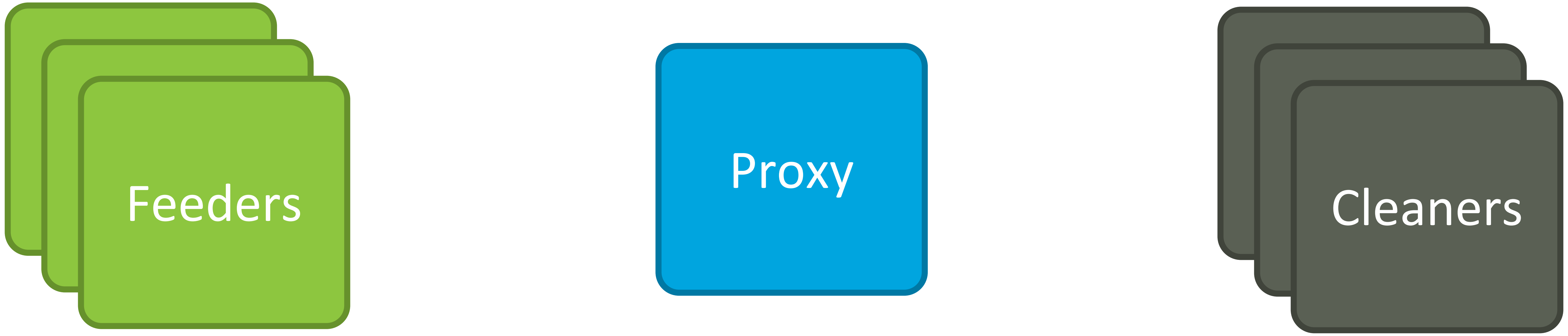
- ISPs
- Critical Infrastructure Providers (CIP)
- Large Enterprises
- Governmental Organisations

to protect

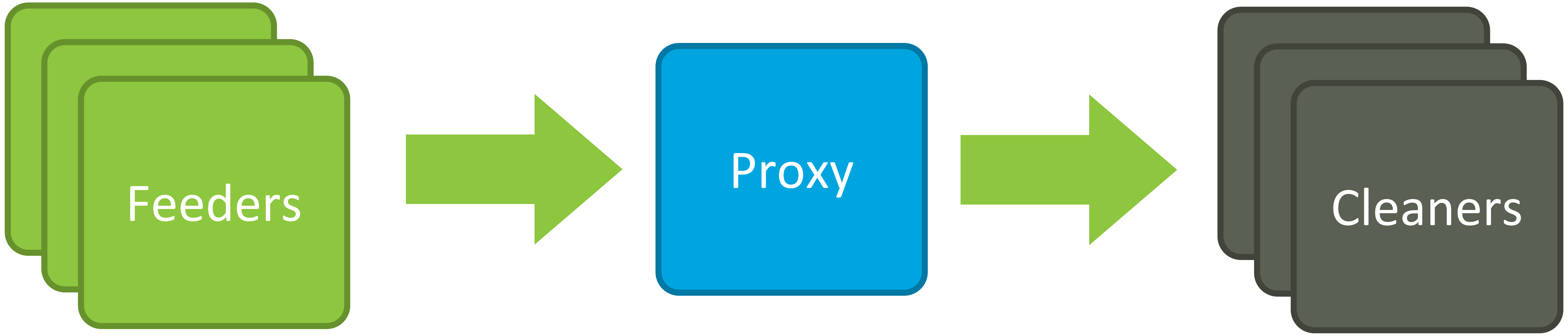
Citizens

Critical Infra

Level 1:
Assets being identified,
useful feeds known



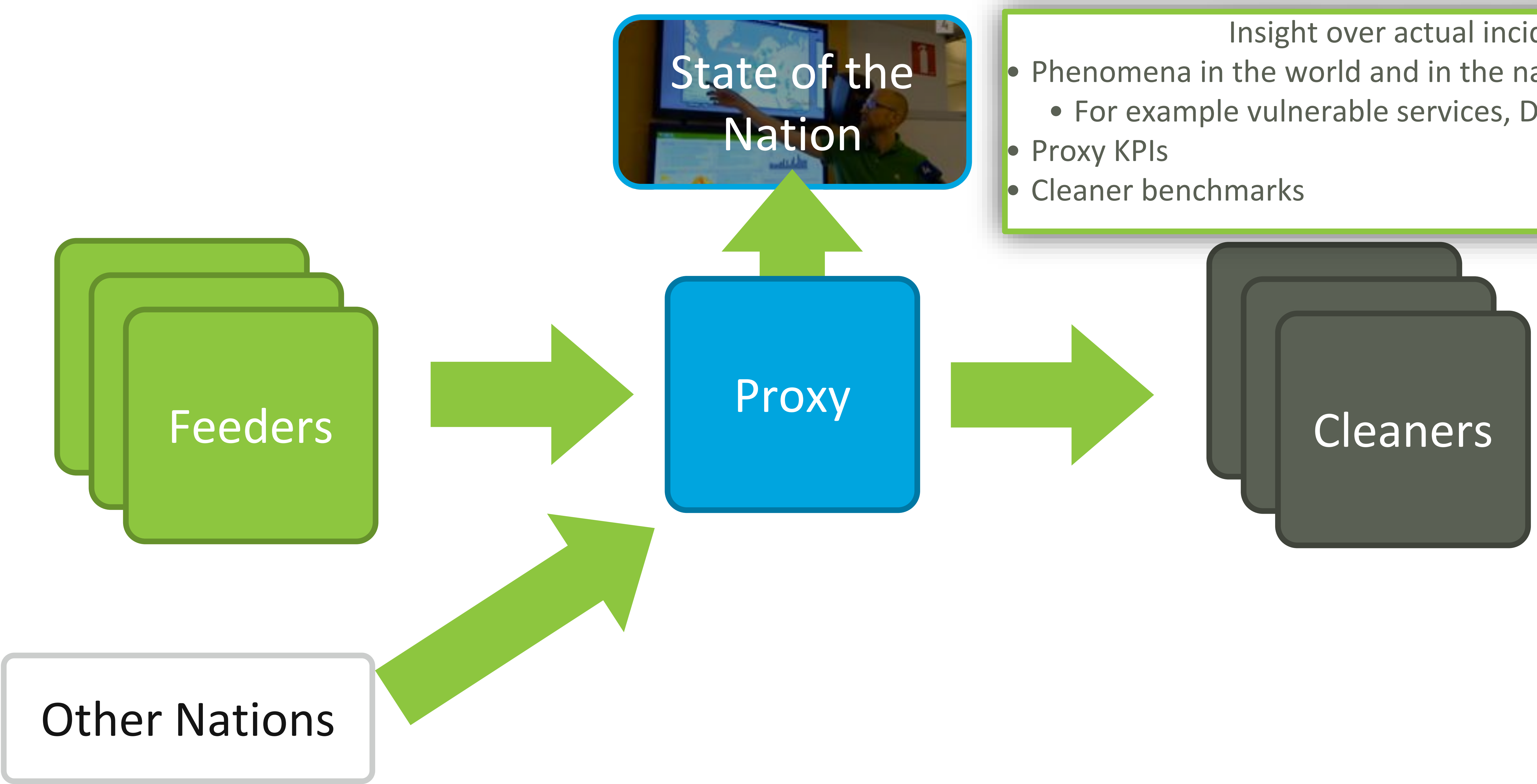
Level 1:	**Level 2:**
Assets being identified, useful feeds known	Automated 24/7 abuse handling with common tools



Level 1:
Assets being identified, useful feeds known

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

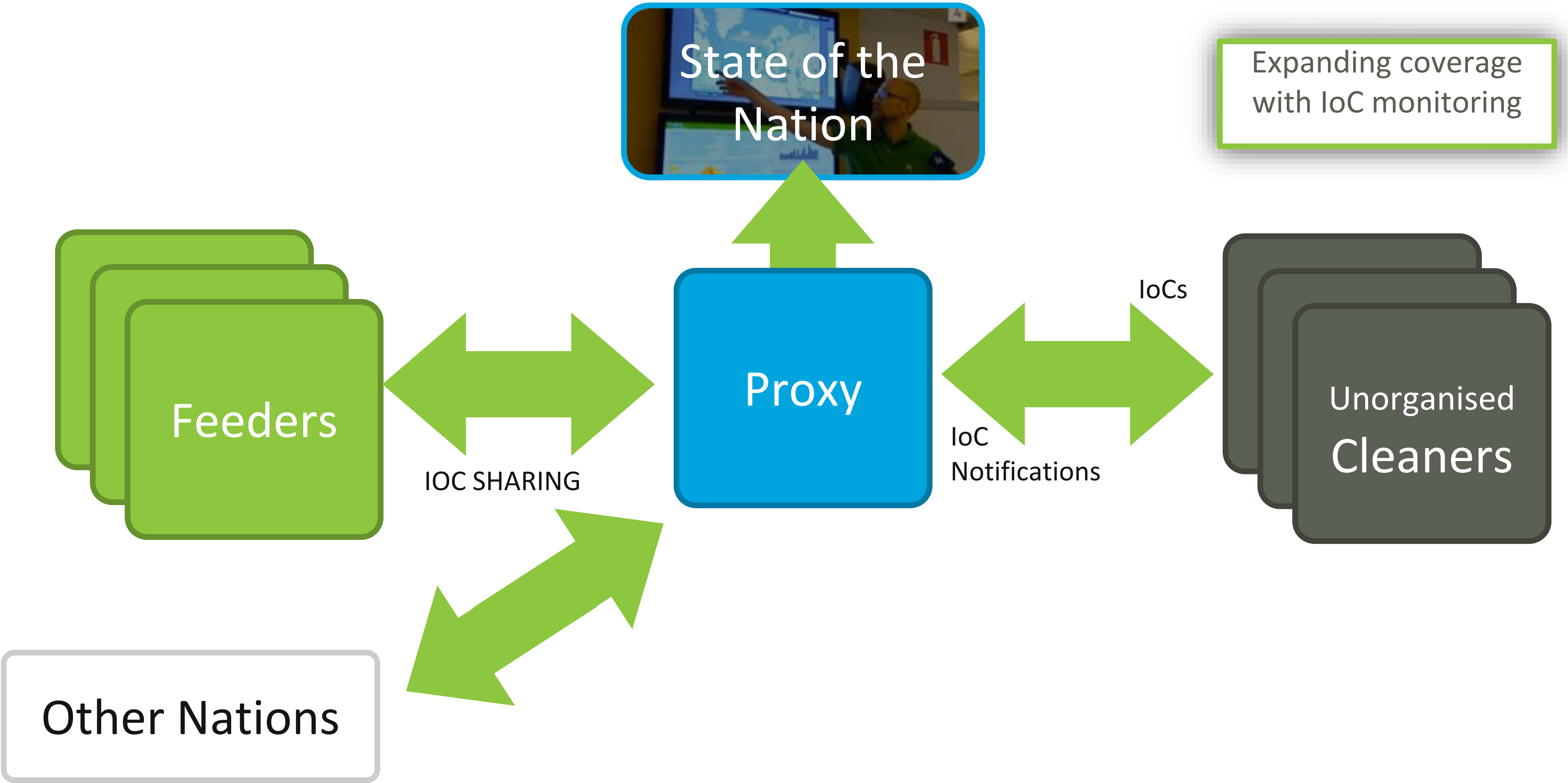
Level 3:
Situation Awareness



Insight over actual incidents

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

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



State of the Nation

Expanding coverage with IoC monitoring

Feeders

IOC SHARING

Proxy

IoCs

IoC Notifications

Unorganised Cleaners

Other Nations

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

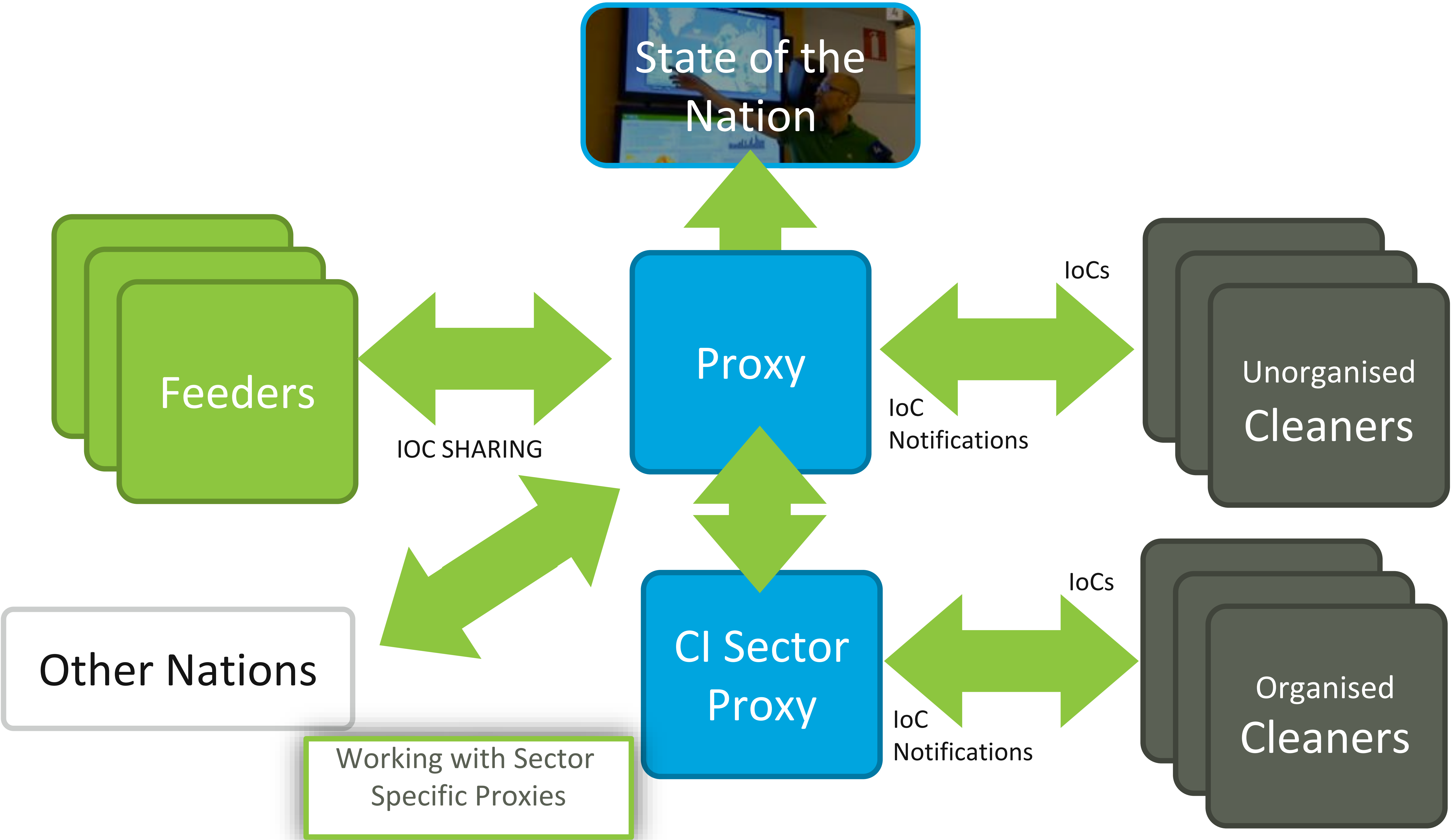
codenomicon

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

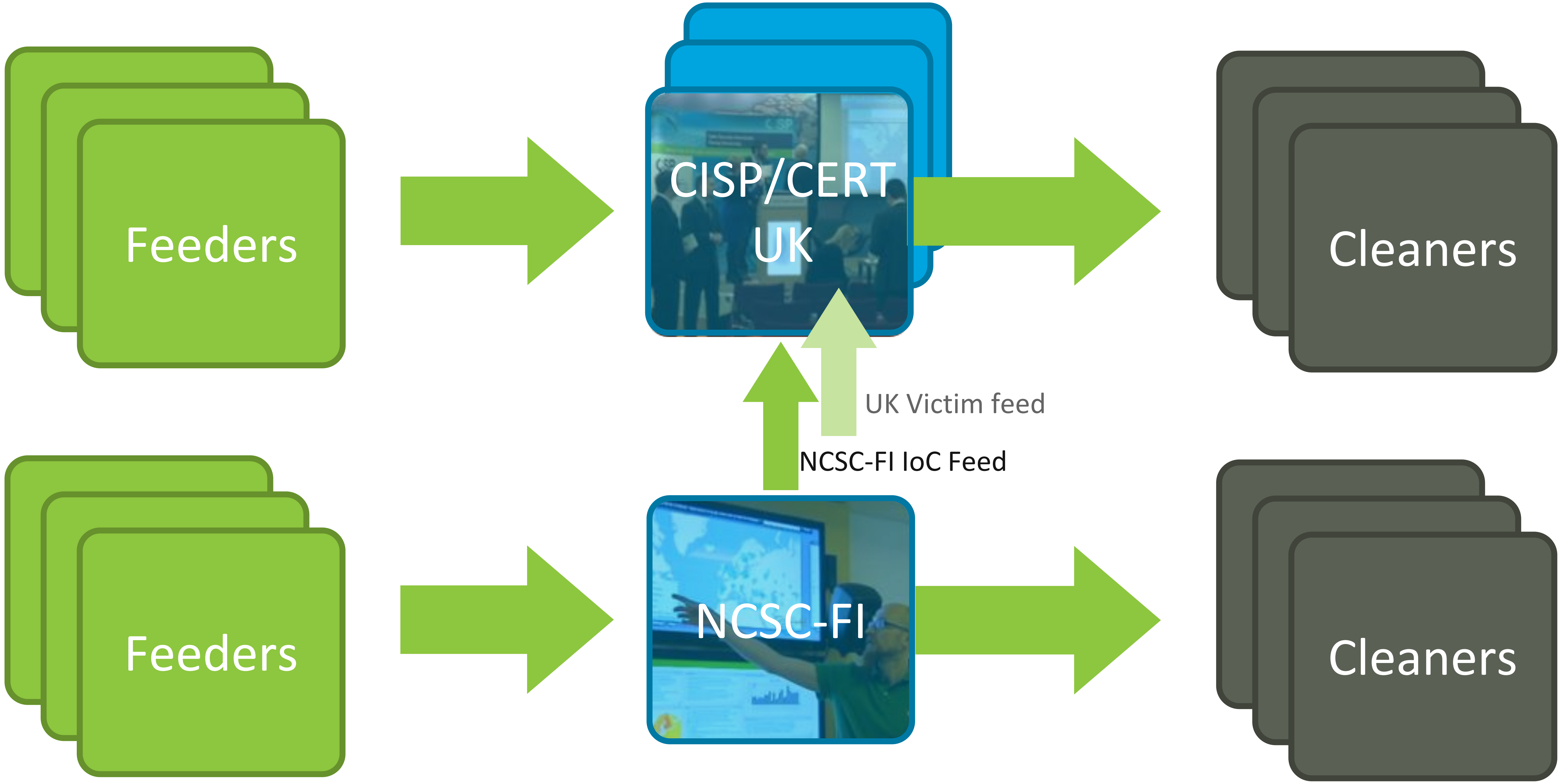


Working with Sector Specific Proxies

codenomicon

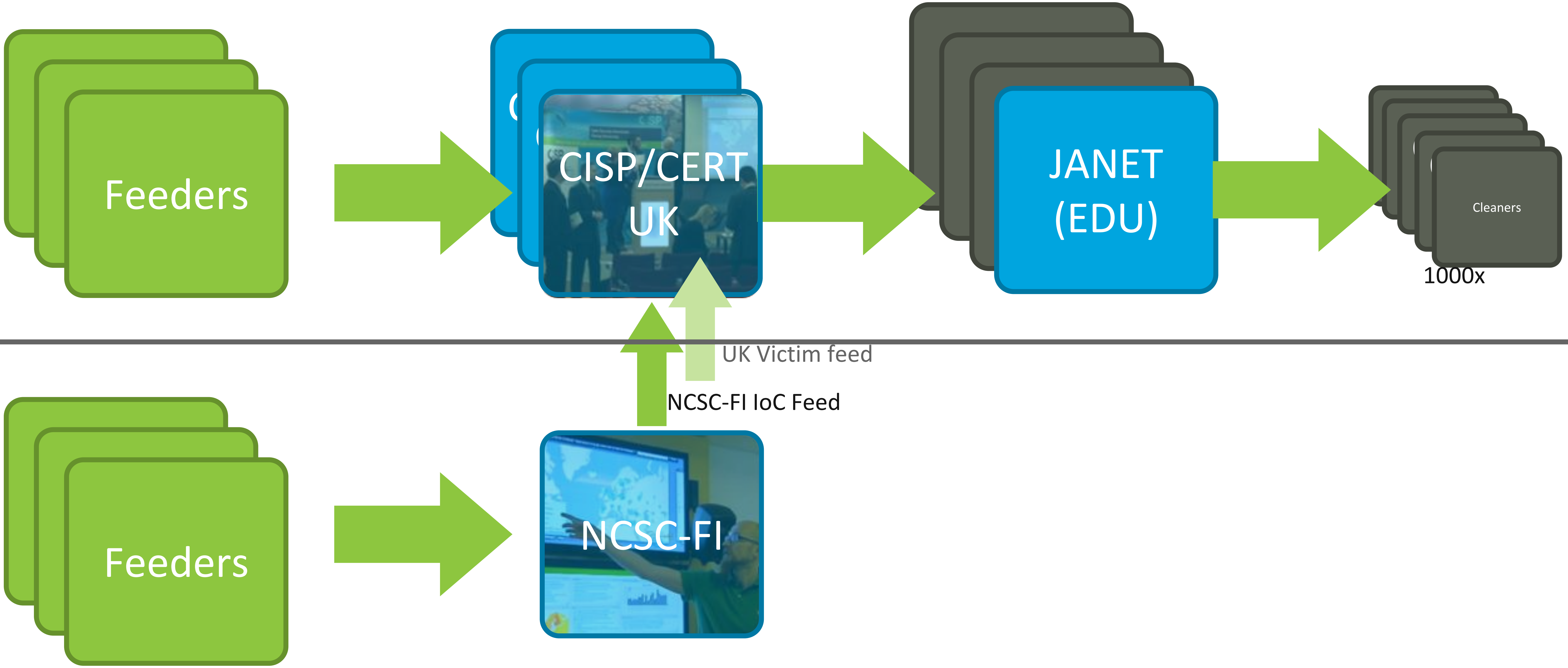
Couldn’t be More Proud of Our Customers!

NATION-TO-NATION REALTIME IOC SHARING



codenomicon

NATIONAL PUBLIC-PRIVATE PARTNERSHIPS



Feeders

CISP/CERT UK

JANET (EDU)

Cleaners

1000x

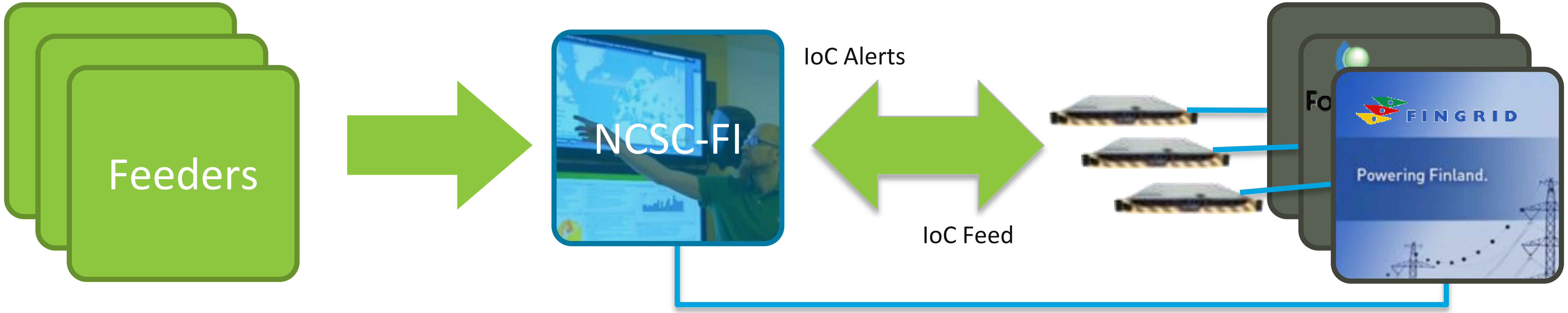
UK Victim feed

NCSC-FI IoC Feed

Feeders

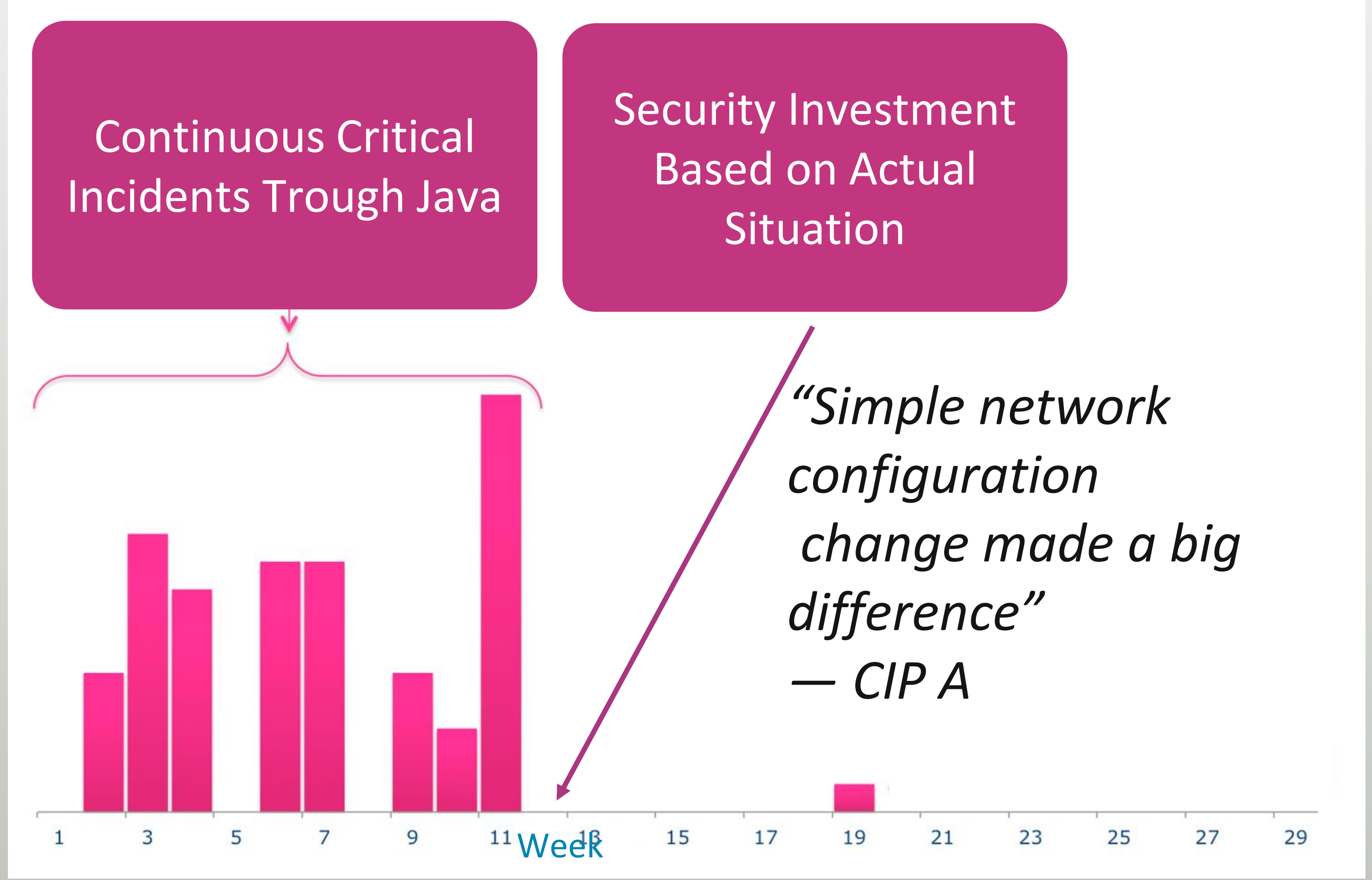
NCSC-FI

NATIONAL PUBLIC-PRIVATE PARTNERSHIPS



Reports

2013: Handled 15 million events, discovered 622 Critical Incidents



Continuous Critical Incidents Trough Java

Security Investment Based on Actual Situation

"Simple network configuration change made a big difference"
— CIP A

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

codenomicon

Ari Knuuti

ari.knuuti@codenomicon.com

Tel: +358405100316