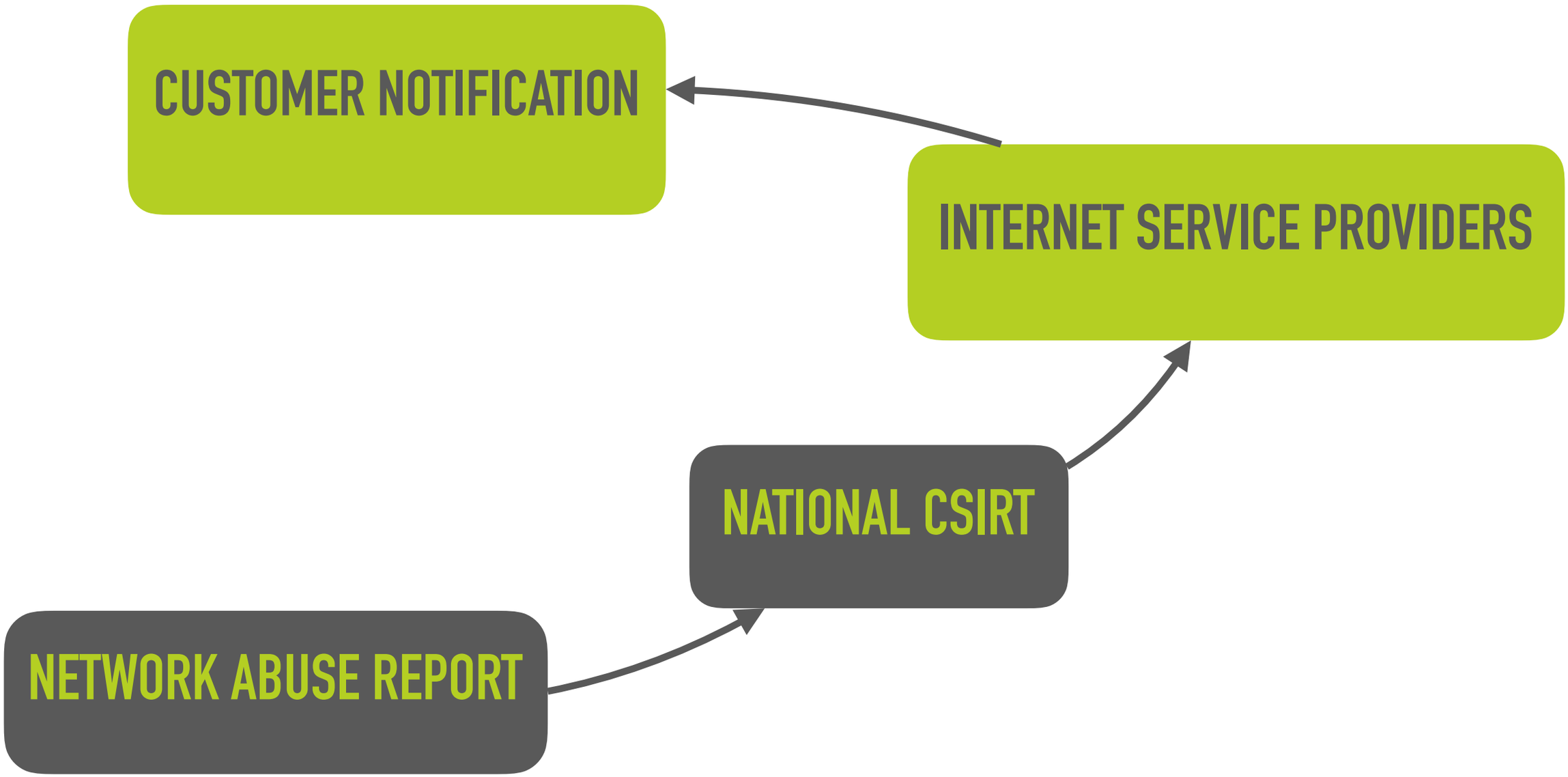
THE LONG TERM EFFECTIVENESS OF A CSIRT OPERATING ON A NATIONAL LEVEL IS TO A LARGE EXTENT, DETERMINED BY THE TEAMS ABILITY TO INCREASE THE RESPONSIVENESS OF INTERNET SERVICE PROVIDERS (ISPS) WITHIN ITS CONSTITUENCY. THIS IS DUE IN PART TO THE ROLE OF ISPS AS THE PRIMARY SOURCE FOR PUBLIC CONNECTIVITY. WHILE ISPS ARE GENERALLY RECOGNIZED AS BEING KEY STAKEHOLDERS BY NATIONAL CSIRTS, FINDING VIABLE METHODS TO INCREASE THEIR RESPONSIVENESS HAS PROVEN TO BE A CHALLENGE. WE WILL EXAMINE THIS CHALLENGE FROM BOTH THE NATIONAL CSIRT AND ISP PERSPECTIVE, BASED ON PRACTICAL EXPERIENCE.

"HOW NATIONAL CERT TEAMS CAN MOTIVATE ISPS TO ENSURE THAT THE VICTIM NOTIFICATIONS ACTUALLY END UP REACHING ALL THE WAY TO THE END USERS"

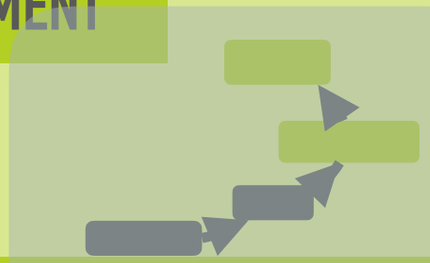


SMALL COG, LARGE MACHINE

DOMESTIC LEVEL

SITUATIONAL AWARENESS

INCIDENT MANAGEMENT



NATIONAL CII PROTECTION

INFORMATION SHARING

CYBER SECURITY STRATEGY

CYBER EXERCISES

PROMOTE IT-SEC COOPERATION

CYBER EXERCISES

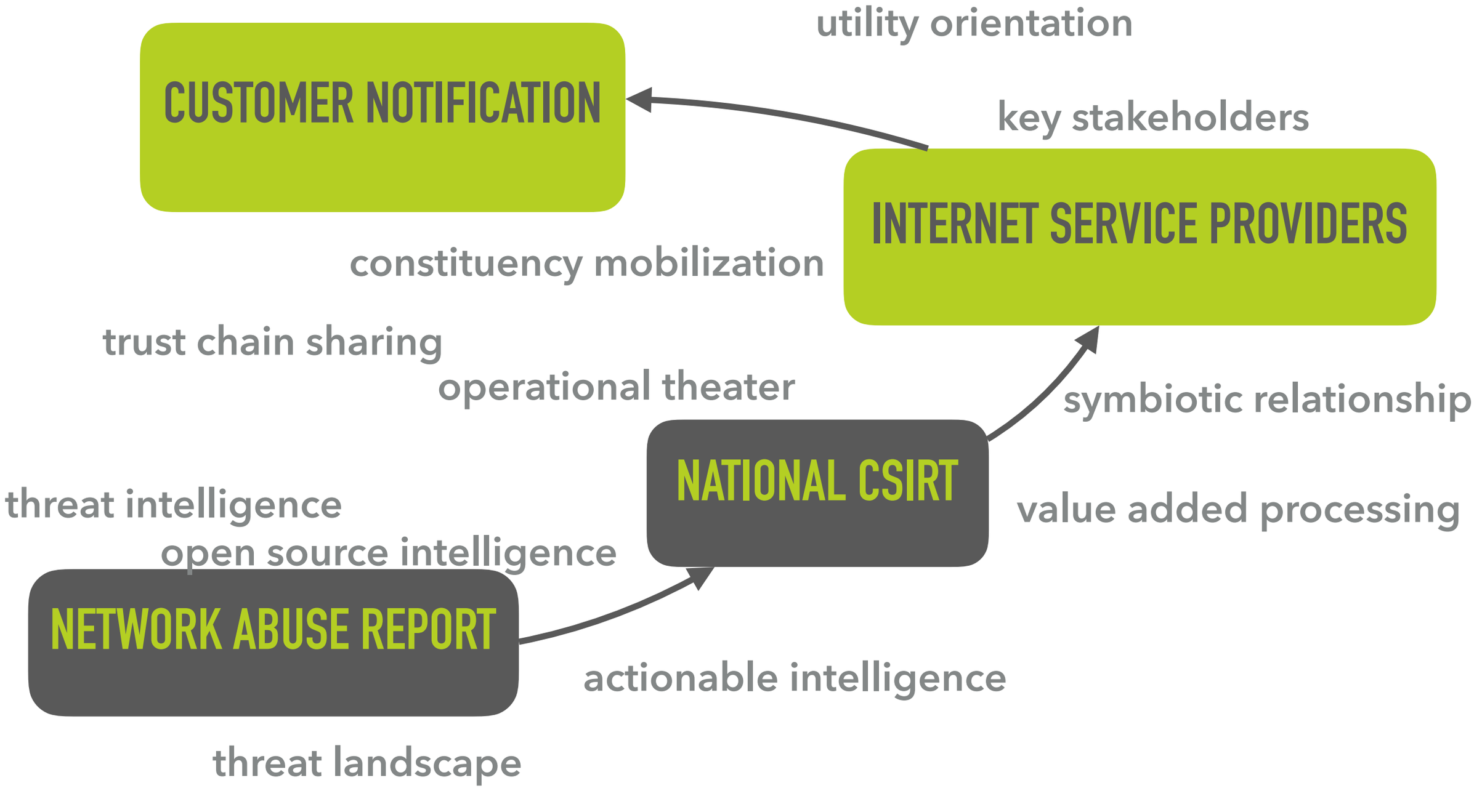
INFORMATION SHARING

OUTREACH

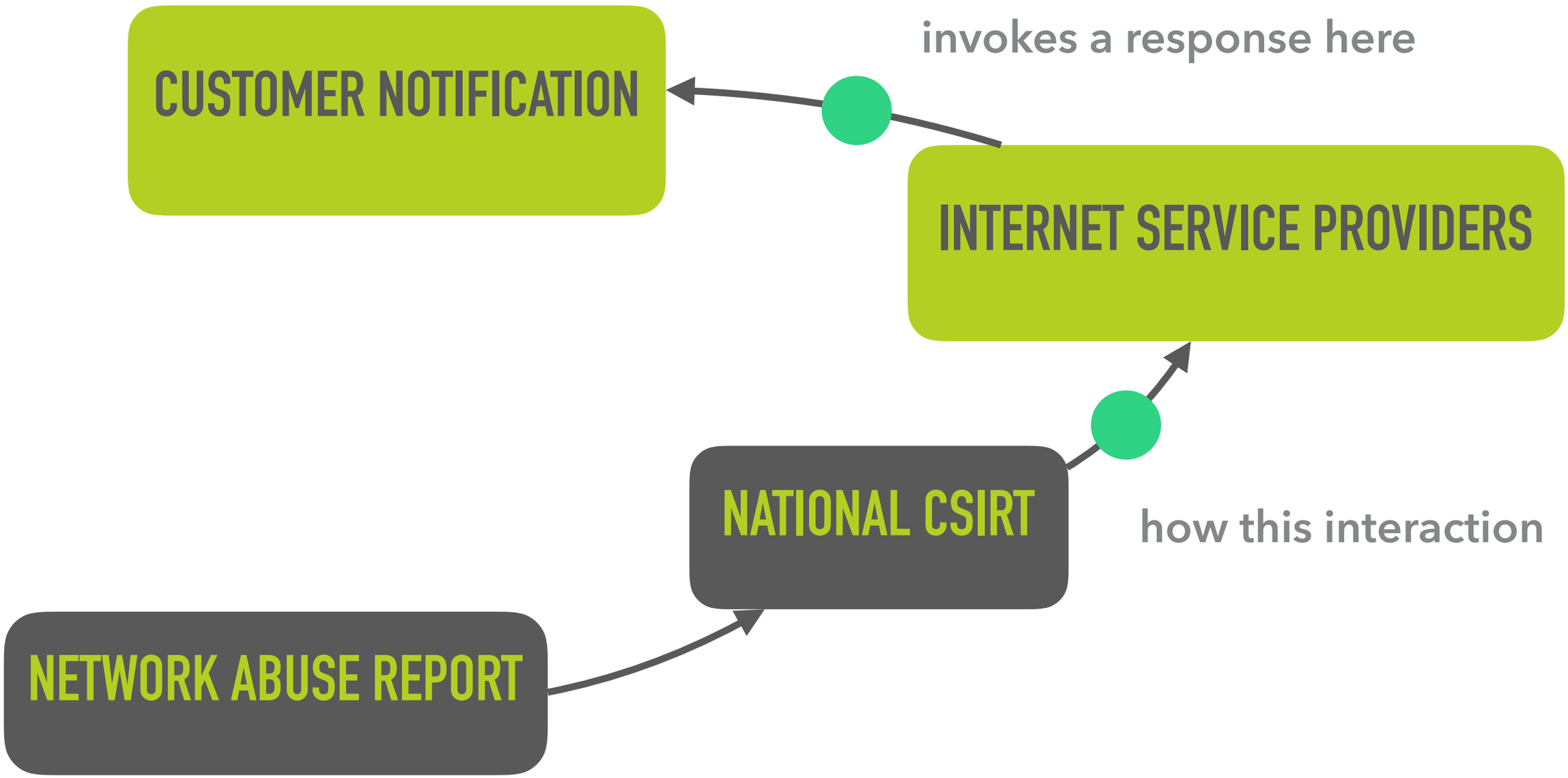
NATIONAL POINT OF CONTACT

INTERNATIONAL LEVEL

IN A WORLD FULL OF TERMS



THE FUNDAMENTAL CHALLENGE



TODAY'S MENU: 3 COURSE ARCTIC SPECIAL

- **APPETIZER**
  - Understanding the risk of ISP codependency
  - How the operational theater is changing
  - The background to our approach
- **ENTREE: THE TOPIC DONE THREE WAYS**
  - The national CSIRT perspective
  - The ISP perspective
  - Success stories
- **DESSERT:**
  - Summary

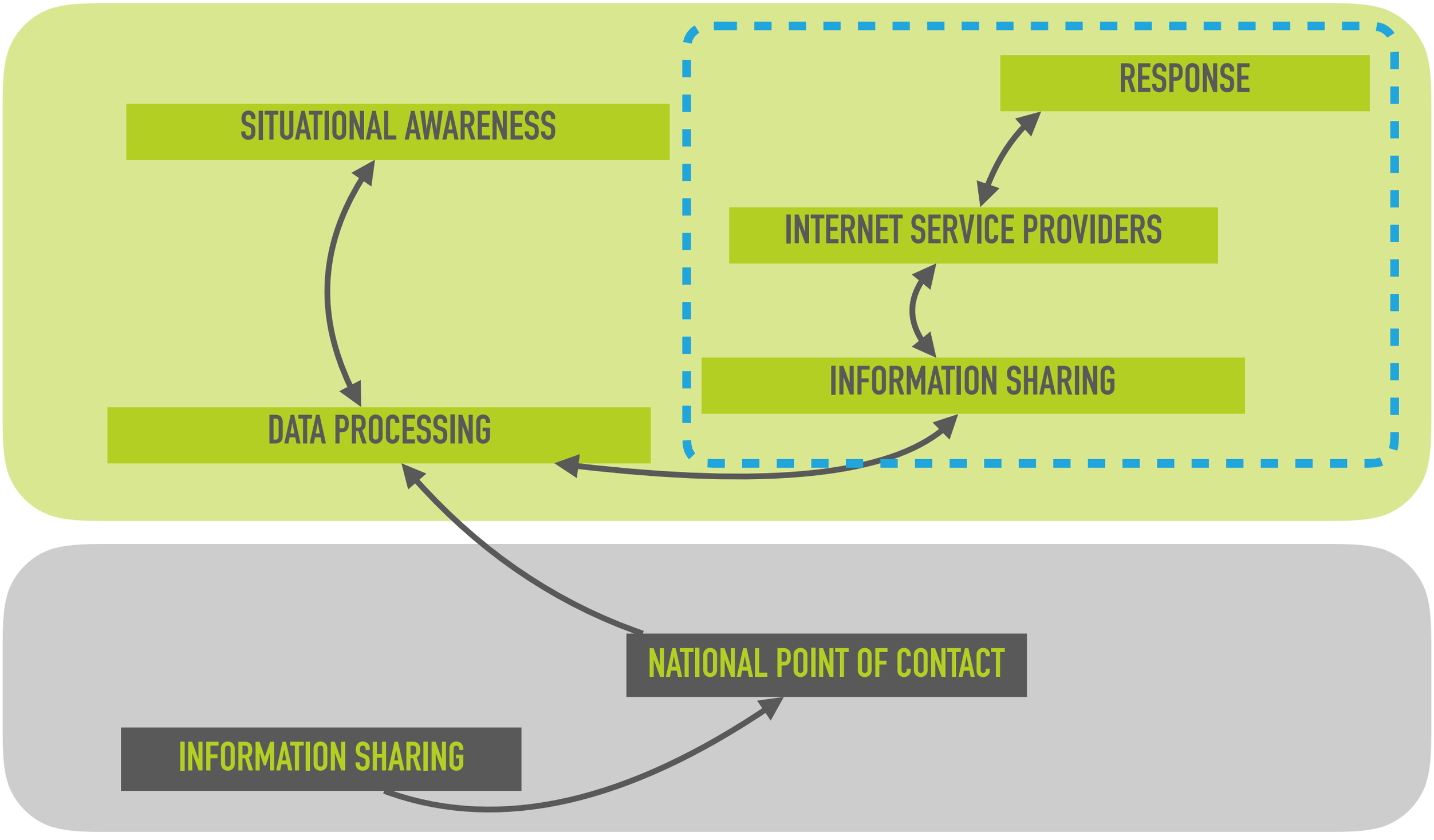
THE CHEFS

- Sindri Bjarnason (sindri@synopsys.com)
- Founding member of CERT-IS from 2011 - 2014
- Problem solving in collaboration with multiple national CSIRTs

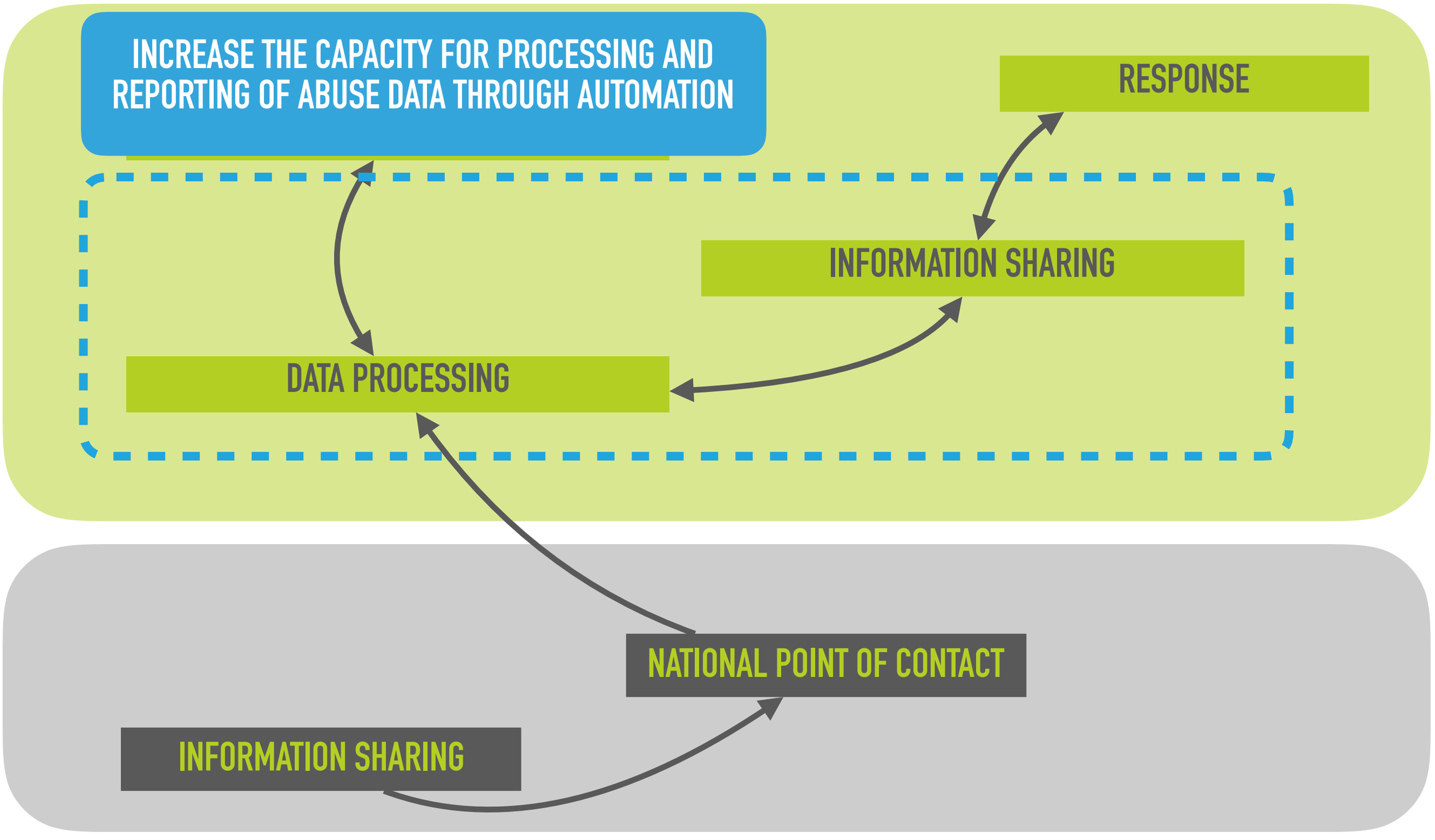
- Juha Haaga (juha.haaga@synopsys.com)
- Developer for Codenomicon since 2012, working with AbuseSA and NCSC-FI projects
- Product manager for AbuseSA at Synopsys

AND NOW BACK TO OUR MAIN STORY . . .

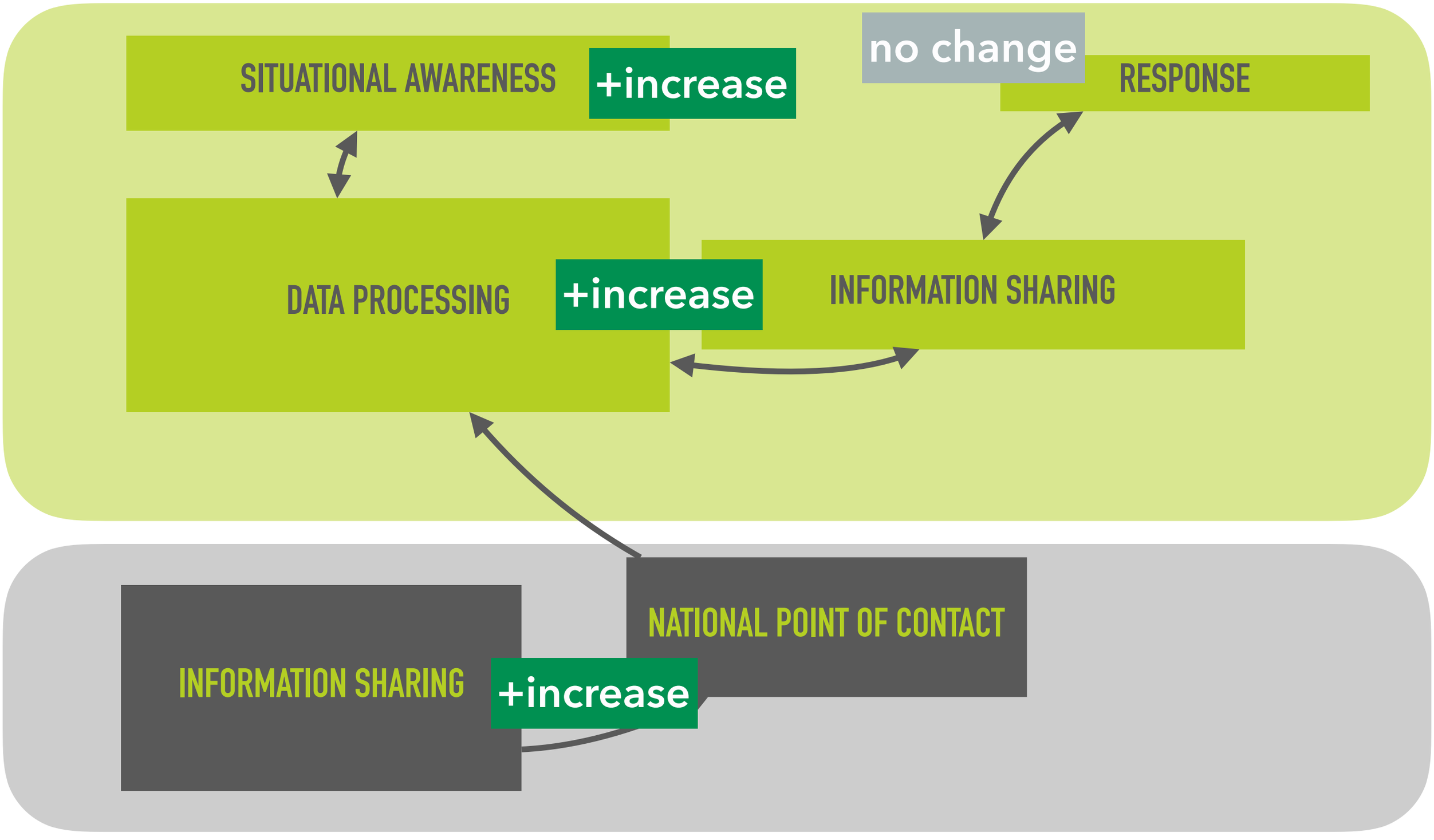
THE AREA OF INTEREST



THE FOCUS IN RECENT YEARS



THE IMPACT


SITUATIONAL AWARENESS
+increase
no change
RESPONSE
DATA PROCESSING
+increase
INFORMATION SHARING
INFORMATION SHARING
+increase
NATIONAL POINT OF CONTACT

WHY NOT ASK THEM NICELY DO RESPOND?

THE FAMILIAR RESPONSE

WE NEED A CONTACT

WE NEED RESPONSE

YOU SHOULD BE AWARE

LOOK AT THE DATA

WE ALREADY RESPOND

NOT OUR PROBLEM!

WHO ARE YOU?

SPEAK WITH THE NOC!

WHERE IS THIS DATA COMING FROM?

LET ME GET OUR LAWYERS

THE TOPIC DONE THREE WAYS

THE CSIRT PERSPECTIVE
CERT-IS, ICELAND

THE ISP PERSPECTIVE
NCSC-FI, FINLAND

SUCCESS STORIES
CERT-EE, ESTONIA

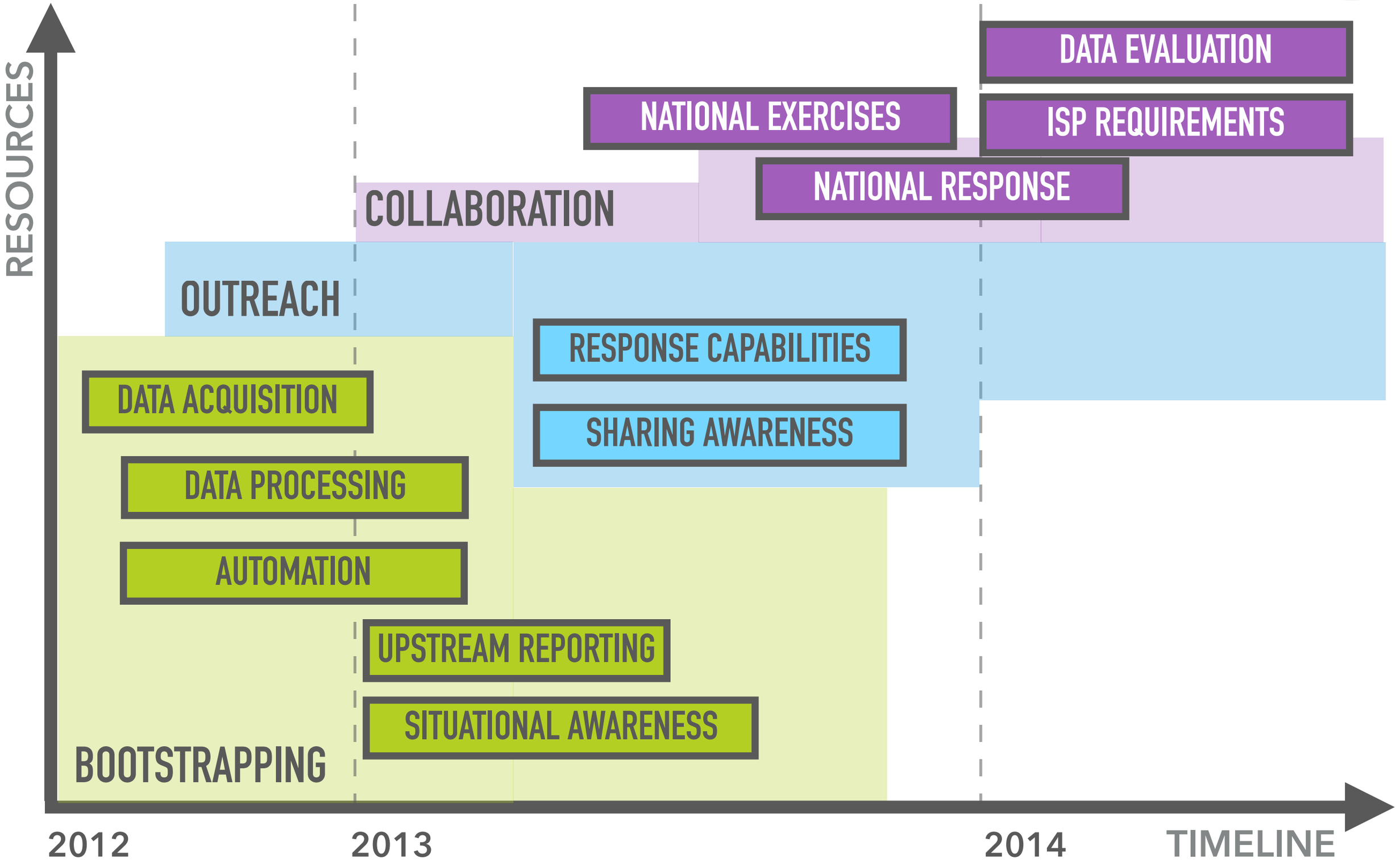
ICELAND: THE NATIONAL CSIRT PERSPECTIVE

THE CSIRT PERSPECTIVE
CERT-IS, ICELAND

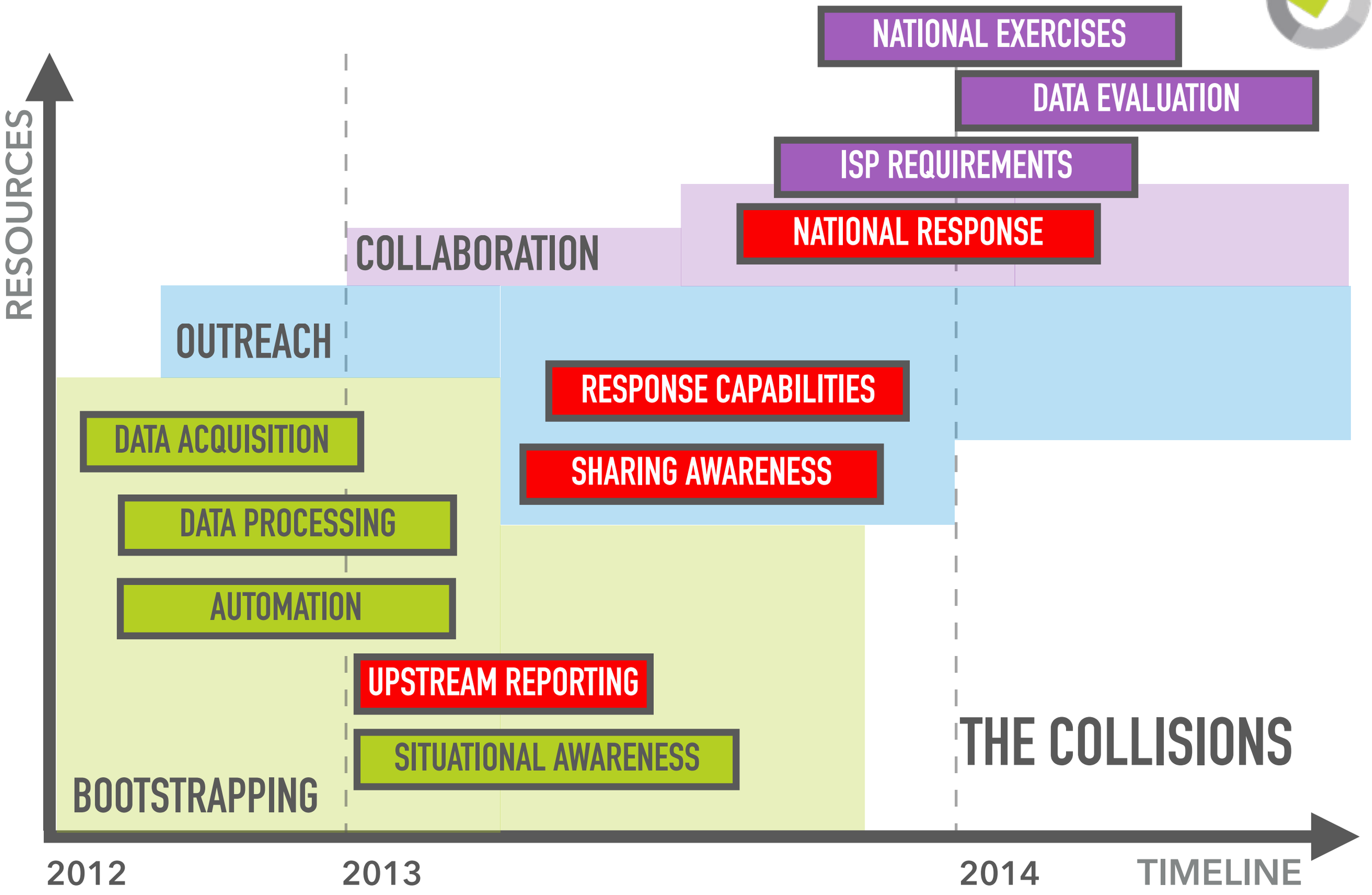
CERT-IS: THE BACKGROUND

- The national CERT in Iceland was established in 2011, legislation "enacted" in spring 2012
- Operates independently within the telecommunication regulatory authority
- Telecommunication organizations formed the initial constituency
- Rapid bootstrap phase provided early operational capabilities

ICELAND: THE NATIONAL CSIRT PERSPECTIVE



ICELAND: THE NATIONAL CSIRT PERSPECTIVE



MAJOR COLLISIONS

UPSTREAM REPORTING	ASSUMED EXISTING UPSTREAM CAPABILITIES
SHARING AWARENESS	ASSUMED EXISTING AWARENESS OF THE DATA
RESPONSE CAPABILITIES	ASSUMED EASY INTEGRATION
NATIONAL RESPONSE	ASSUMED DOMESTIC READINESS

UPSTREAM REPORTING

ASSUMED EXISTING UPSTREAM CAPABILITIES

- CERT-IS automated (with AbuseSA / Abusehelper) most of the data processing needed on a daily basis
- This increased capacity allowed us to rapidly increase the volume and throughput of abuse data
- We assumed that our processing capacity would be met upstream, allowing the gap to grow further
- The negative impact was significant

NEGATIVE IMPACT

- The initial dialog with the upstream responders was focused on dealing with the ever increasing stream of abuse data
- The focus should have been “where could we start” instead of “we need to solve this”
- The underdeveloped knowledge of the actual abuse data added to the confusion
- Significantly delayed any collaboration

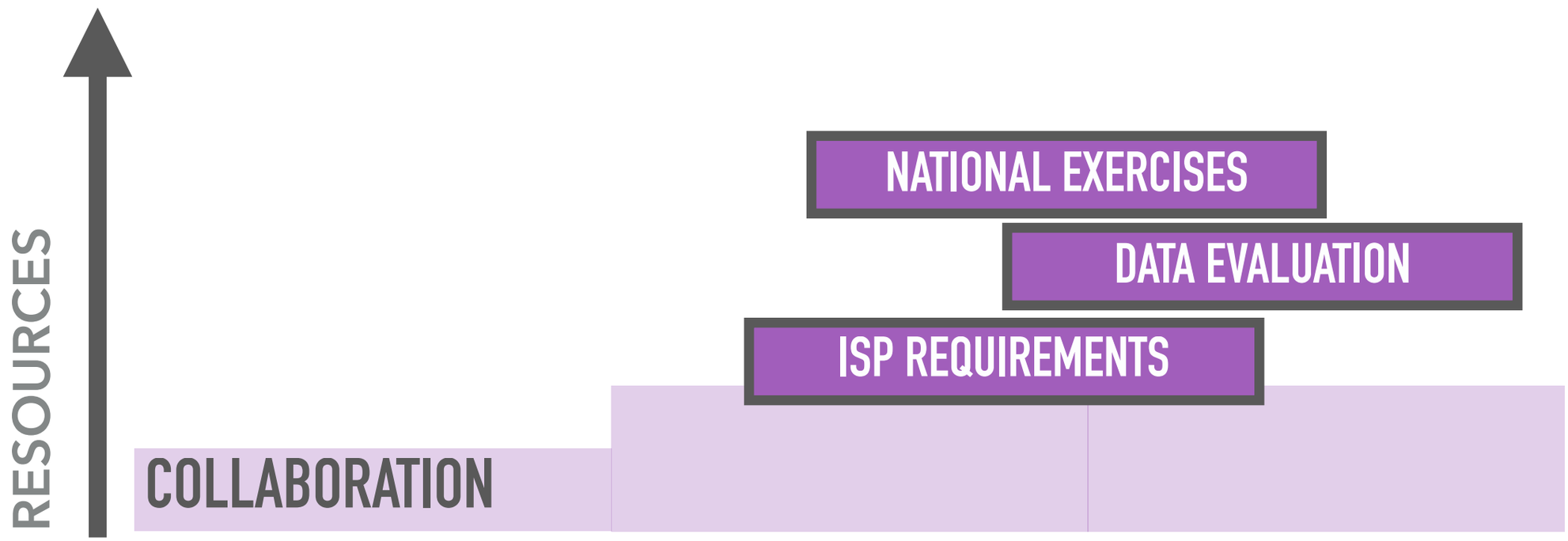
SHARING AWARENESS

ASSUMED EXISTING AWARENESS OF THE DATA

- As more abuse data becomes available to national CSIRTs, the gap between the situational awareness available to the team and domestic actors grows
- If the teams priorities and actions are shaped by its own situational awareness that does not extend to its constituency, the team risks isolation

AREAS OF SUCCESS

WHERE LIMITED RESOURCES YIELD HIGH UTILITY



EASY INTEGRATION

NATIONAL EXERCISES

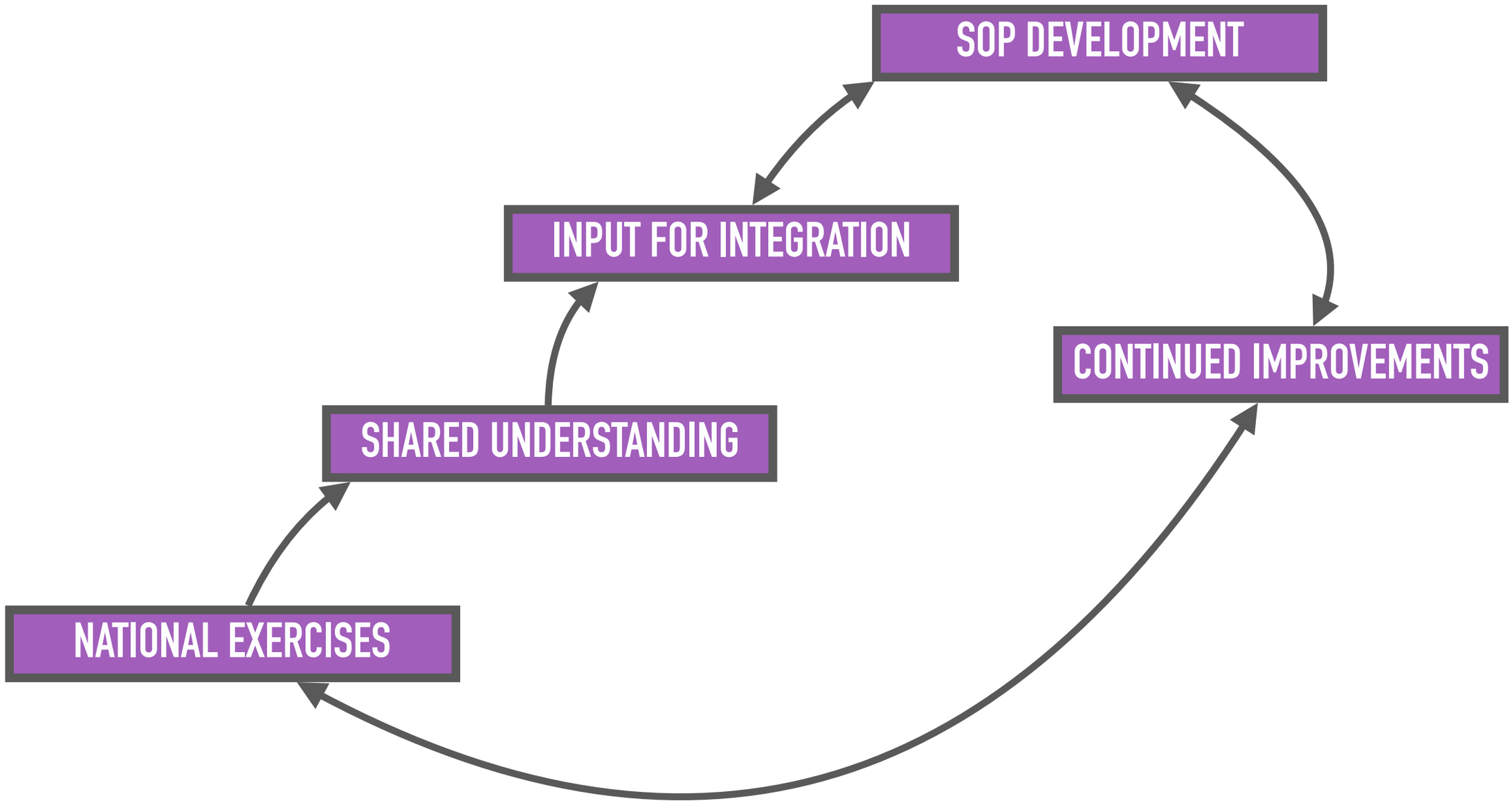
DATA EVALUATION

ISP REQUIREMENTS

DELIVERING UTILITY

- The first step is to identify the roles and requirements within the constituency and estimate the needed commitment of resources
- Translates to asking “what is needed and where”
- Integrating with and enhancing existing response procedures offers higher sustainability

NATIONAL RESPONSE CAPACITY



SUCCESS STORIES
CERT-EE, ESTONIA

CERT-EE: THE BACKGROUND

- The national CERT in Estonia was established in 2006
- Extensive constituency that included majority of public organizations
- Assumed national responsibility roles from the start

THE FUNDAMENTALS

DEVELOPING TRUST

- CERT-EE as an organization
- The capabilities of the team
- Between individual members

BUILDING RELATIONS

- Multiple levels
  - Technical operators
  - management
- Information exchange

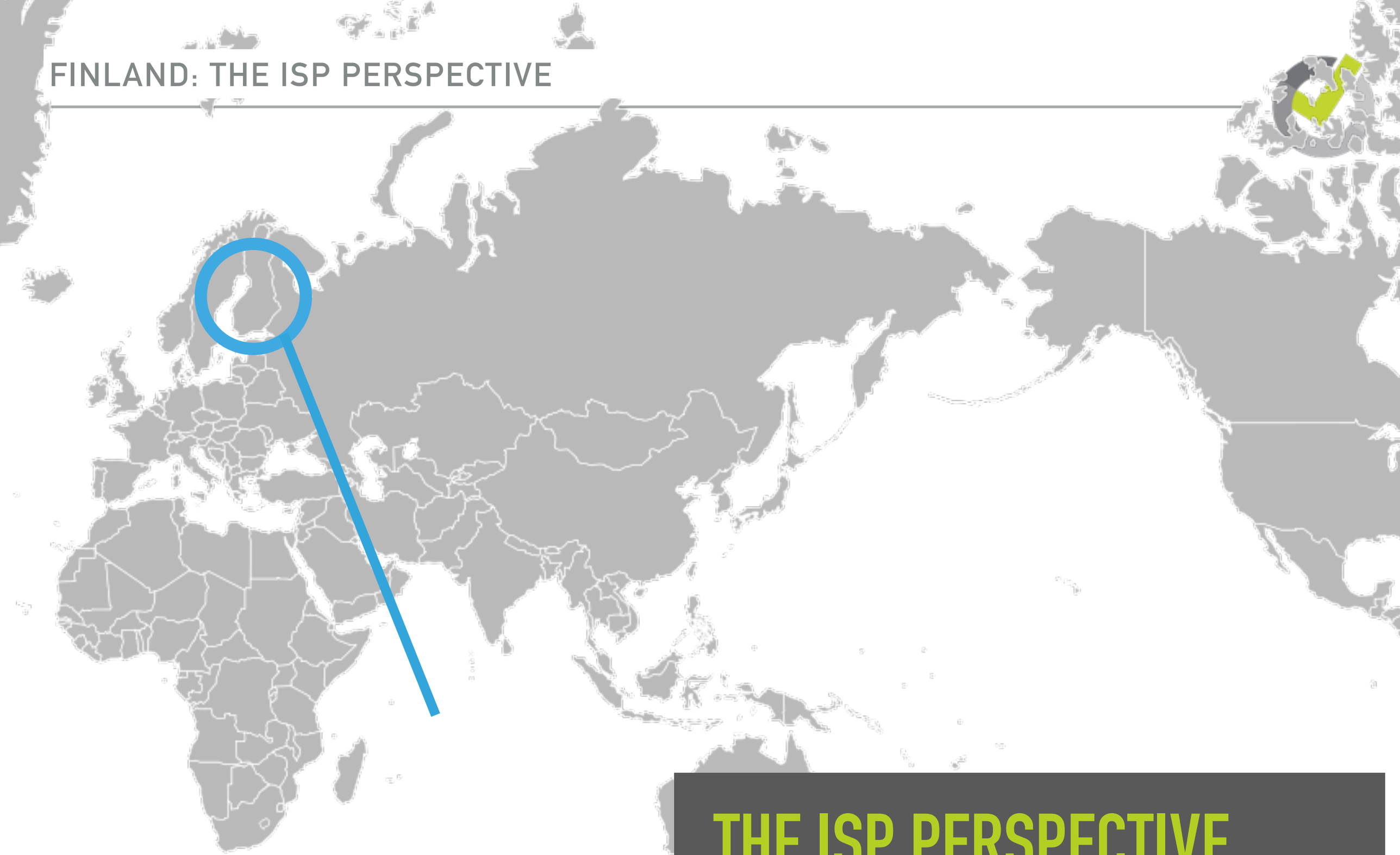
WALLED GARDEN PROJECT

FEATURES

- Automated response to network abuse reports
- Customers temporarily confined to an information portal

THE MAIN POINTS

- Ensuring the quality of the data being processed
- Single ISP implementation at the beginning
- The ISP was the authority



THE ISP PERSPECTIVE
NCSC-FI, FINLAND

FINLAND: THE BACKGROUND

- The National Cyber Security Centre in Finland has a long history
- The largest ISP began incrementally investing resources into abuse reporting already 15 years ago.
- Collaboration is very mature, and the ISP has independent abuse management capability that exceeds CERT expectations

THE SUCCESS FACTORS

TRUST	FRIENDLY CSIRT – ISP RELATIONSHIP
FRIENDLY COMPETITION	ANONYMOUS ISP PERFORMANCE REPORTS
MATURITY OVER TIME	INCREMENTAL BUILD UP OF ABUSE HANDLING CAPABILITY
AUTOMATION	REDUCES ISP RESOURCE IMPACT FOR RESPONSE

TRUST

FRIENDLY CSIRT – ISP RELATIONSHIP

- NCSC-FI is within telecommunications regulatory authority, but they have not needed to apply regulatory pressure to get results
- Lawyers do not run the show – NCSC-FI can discuss directly with subject matter experts
- Open discussion on how to best tackle specific issues, and ISPs contribute by sharing what is easiest for them

FRIENDLY COMPETITION

ANONYMOUS ISP PERFORMANCE REPORTS

- NCSC-FI acts as a neutral party and publishes anonymised annual report on how well ISPs perform on abuse handling
- Each ISP is shown how well they did, and how they are positioned in the rankings
- Top performers are keen to use their status for marketing purposes, and publish who they are in the anonymised report

MATURITY OVER TIME

SMALL INCREMENTS LEADING TO BIG RESULTS

- Finland has the advantage that this process has been ongoing for 15 years
- ISPs who were able to pay attention, developed response capability as new threat types appeared
- Time spent on perfecting the customer communications

AUTOMATION

REDUCES ISP RESOURCE IMPACT FOR RESPONSE

- Automated abuse report processing makes this possible for ISP
  - In-house developed systems in Finland
- Automated notification systems that relay abuse information over various channels – SMS, email, walled garden (captive portal)
- ISPs who were paying attention, developed response capability as new threat types appeared

"SOCIETY'S GROWING INFORMATION INTENSITY, THE INCREASE OF FOREIGN OWNERSHIP AND OUTSOURCING, INTEGRATION BETWEEN INFORMATION AND COMMUNICATIONS TECHNOLOGIES, THE USE OF OPEN NETWORKS AS WELL AS THE GROWING RELIANCE ON ELECTRICITY HAVE SET TOTALLY NEW REQUIREMENTS FOR SECURING SOCIETY'S VITAL FUNCTIONS IN NORMAL CONDITIONS, DURING SERIOUS DISTURBANCES IN NORMAL CONDITIONS AND IN EMERGENCY CONDITIONS."

Finland's Cyber Security Strategy

SUMMARY

- The challenge is almost entirely social – the technical problems are relatively easy to solve

THANK YOU!

Q&A