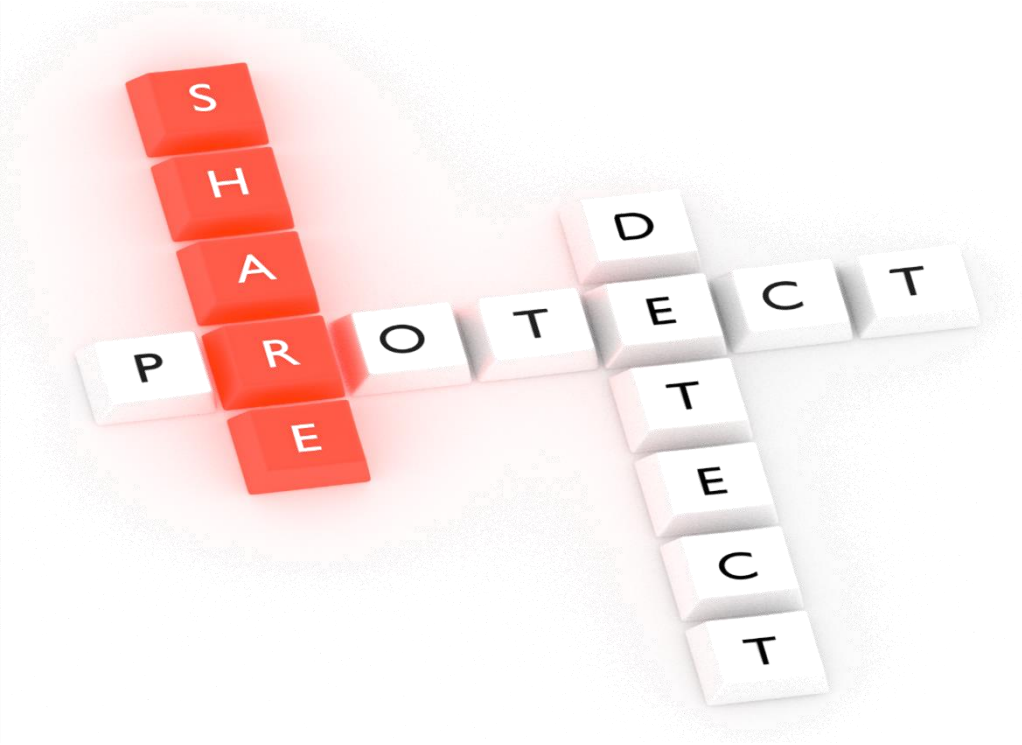
Detect, SHARE, Protect

Solutions for Improving Threat Data Exchange among CERTs



Agenda

- Objectives
- Methodology
- Overview of Communication Practices
- Barriers to Information Sharing
- Requirements for a Common Platform
- Overview of Existing Solutions
- Recommendations

Objectives: What we wanted

- Take stock of existing communication solutions and practices among European CERTs
- Promote best practices for threat intelligence exchange
- Identify the functional and technical gaps to threat intelligence exchange between CERTs in Europe
- Outline recommendations for improved communications interoperable with existing solutions

Objectives: What we didn't want

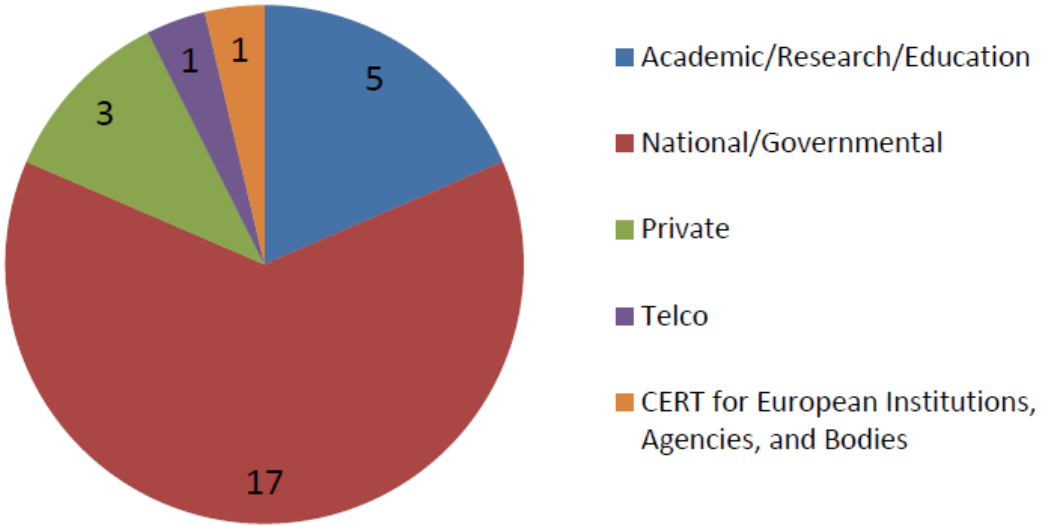
- ~~We do not want yet another report on secure communication (a-z).~~
- ~~We don't want to come up with new, revolutionary and unrealistic solutions.~~
- ~~We don't want to get stuck in unsolvable issues (legal, data protection, trust…)~~

Previous ENISA Work on Data Sharing

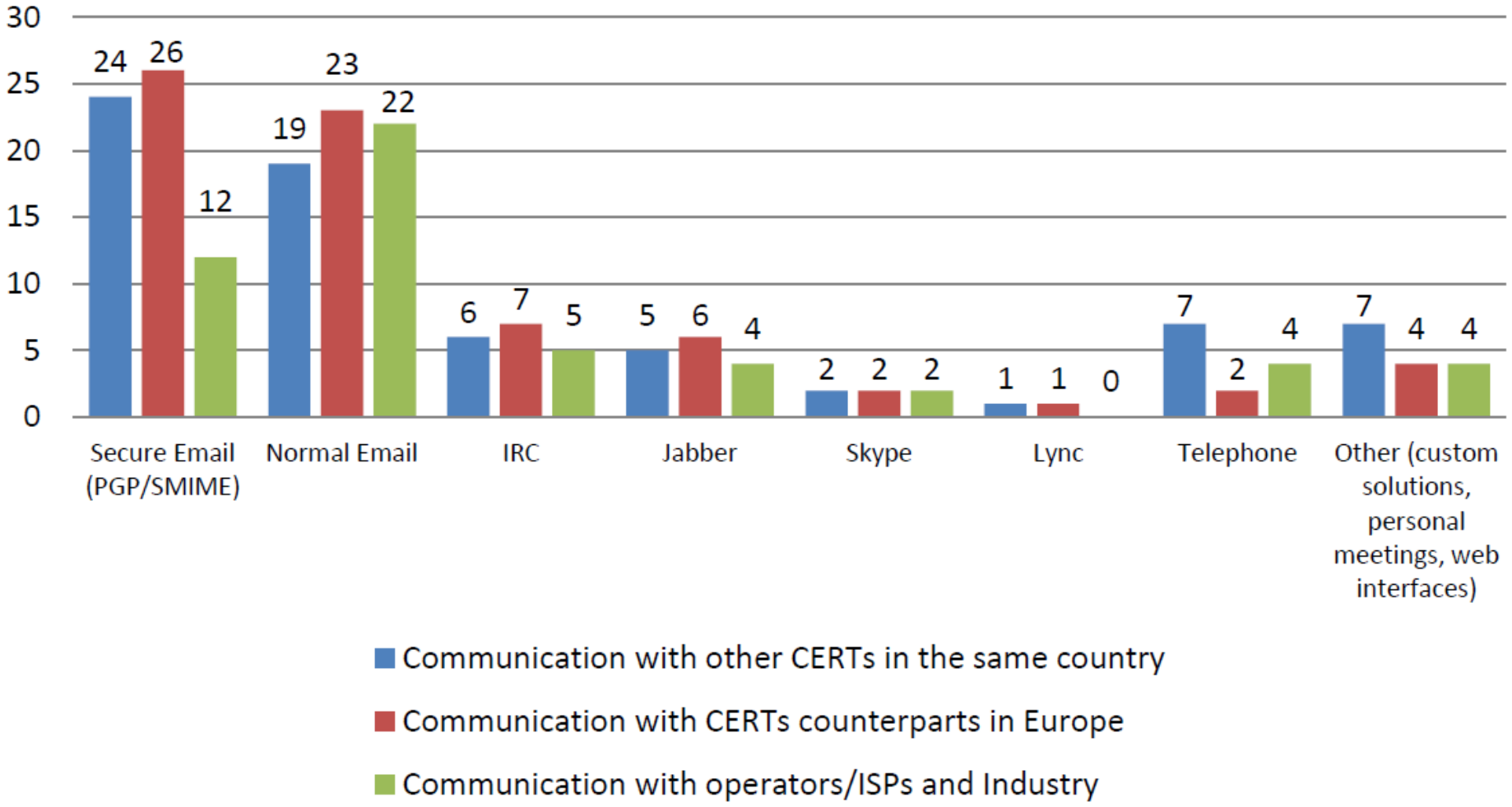
- 2010 – Proactive detection of network security incidents, report – http://www.enisa.europa.eu/activities/cert/support/proactive-detection/proactive-detection-report
- 2011 – A flair for sharing - encouraging information exchange between CERTs – http://www.enisa.europa.eu/activities/cert/support/fight-against-cybercrime/legal-information-sharing
- 2011 – Secure Communication with the CERTs & Other Stakeholders – http://www.enisa.europa.eu/activities/cert/other-work/files/secure-communication
- 2012 – Proactive detection of security incidents II – Honeypots – http://www.enisa.europa.eu/activities/cert/support/proactive-detection/proactive-detection-of-security-incidents-II-honeypots

Methodology

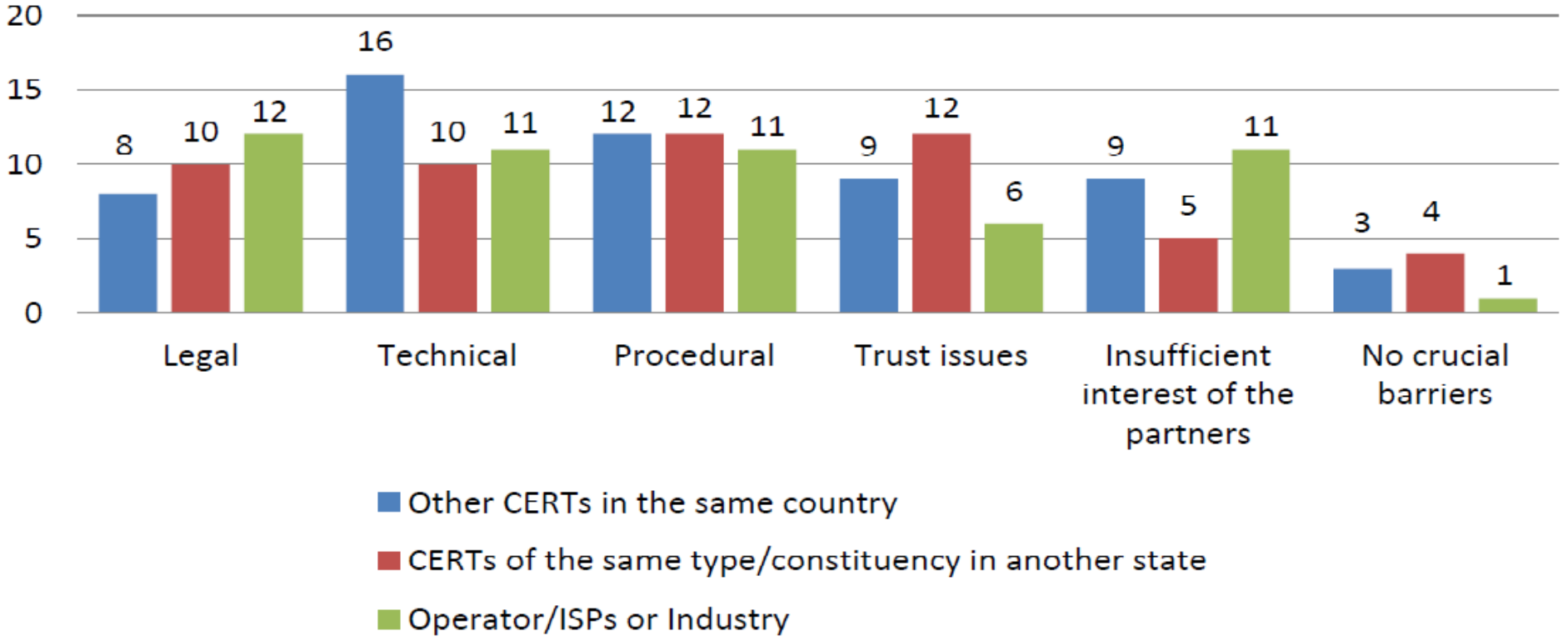
- Survey (27 Teams)
- Interviews (12 Stakeholders)
- Face-to-face Workshop (14 Participants)



Overview of Communication Practices



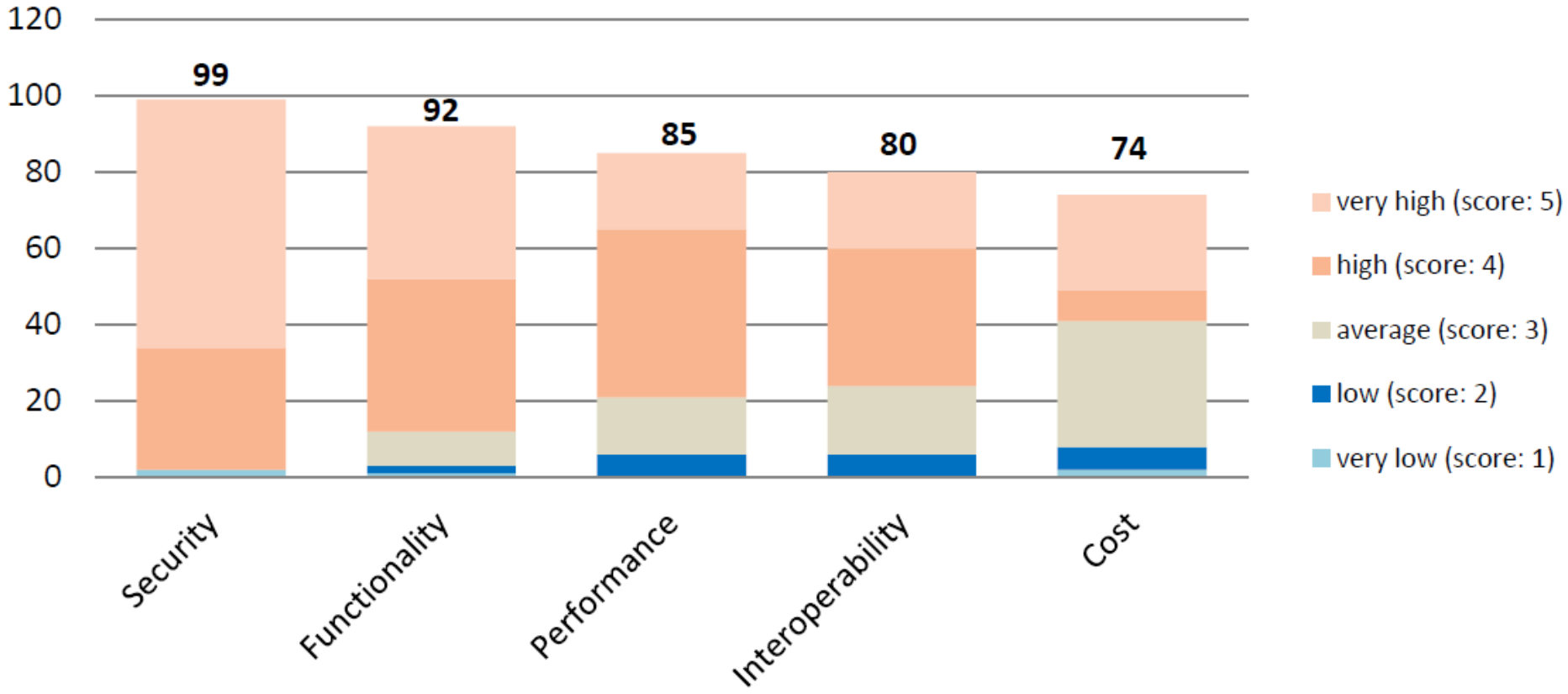
Barriers to Information Sharing



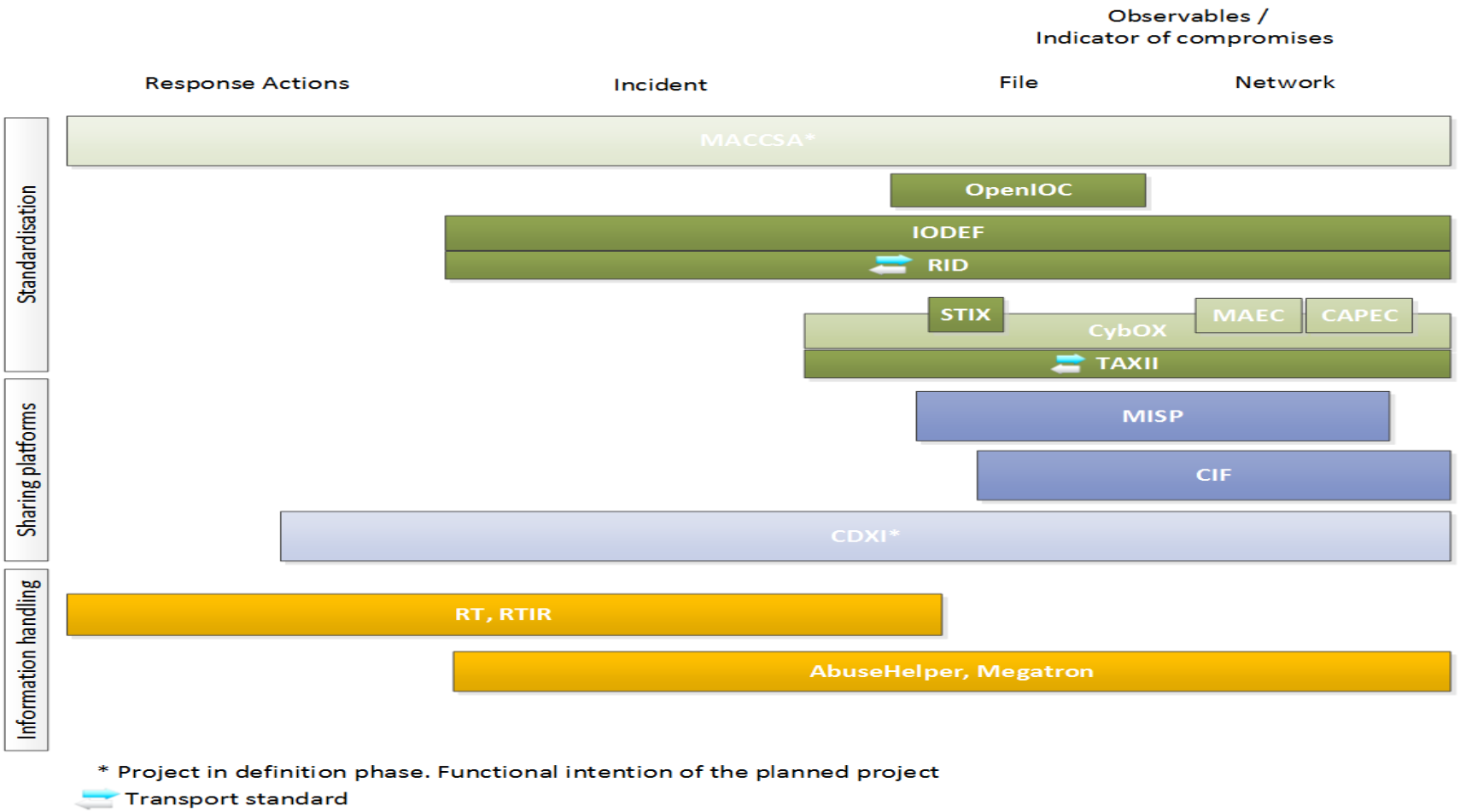
Focus: The Many Technical Issues

- Format changes without prior notice when dealing with automatic reporting
- Too many formats/format standards
- Mapping of IP addresses to ASN or country (and history of changes!)
- Find contact information for IP addresses

Requirements for a Communication Platform
If there is a need



How to overcome barriers: Mapping of standardisation and solutions for response, incident and IoC information sharing



We recommend

1

ENISA should facilitate the adoption of essential tools for the CERT community.

- CERTs interested in working together on RT/RTIR/AH upgrades and improvements should synchronise their efforts.
- CERTs can seek funding from the EU's research and technology programs for updates and upgrades.
- ENISA can provide training sessions at ENISA CERT workshops or via other arrangements.

We recommend

2

Security feeds providers should improve the stability of existing incident information feeds, while now the feed formats are often changed by their publishers without prior notice.

- Wider adoption of some of the best standards of data format for the automated sharing of indicators of compromise (IODEF, STIX, OpenIOC, etc.)
- Wider adoption of 'good community citizen' behaviour, like establishing a minimal notification period for sharing feed format updates

ENISA will further investigate these areas and provide adequate and appropriate support for CERTs and their projects.

We recommend

3

CERTs should enhance functionalities of existing tools for more effective data sharing within their community.

- First and foremost, interoperability for cross-hub and cross-platform sharing
- Correlation engines for incident analysis
- Advanced analytics and visualisation for massive numbers of incidents
- Automatic prioritisation features

This is the subject of an ENISA project this year

We recommend

4

A central body at the cross-border level (enjoying trust in the CERT community) should develop a common incident information repository with the integration of current data exchange efforts.

- Such a repository would include CERTs' contact information to facilitate incident detection and information correlation (DNS, ASN, and IP ranking)
- It would also include a repository for past incident information, with options for sorting and filtering the database of archived information.
- Role for TI?

In 2014, ENISA will carry out a project aiming at providing better support to CERTs in the area of exchanging and processing of actionable information.

We recommend

5

Bridge Sharing CERT Communities in Europe

The 'perfect' scenario for enhancing sharing practices in the CERTs community would include building a bridging platform that would extend existing communities. Such a cross-hub exchange would require:

- Local adoption of interoperable standards of data formats (e.g. IODEF, STIX, etc.)
- The definition of diffusion policy standards (e.g., CDXI Information diffusion policy), thus enabling more complex schemes than Traffic Light Protocol (TLP)
- Coordination at international level

At the EU level, this inter-exchange effort could be entrusted to the CERT community and supported by ENISA.

Thank you for your support to this report! In case of additional comments or suggestions relating to information sharing among CERTs, do not hesitate to contact us!

cert-relations@enisa.europa.eu

Follow ENISA: