CSIRT Information sharing: for good and for better

Prof. Manel Medina

medina@ac.upc.edu / manel@apwg.eu

Unifying the
Global Response
to Cybercrime

Content

- Why do we need to Exchange information
- What to share:
  - data vs information
- How to share:
  - manual vs automatic,
  - actionable vs statistic
  - Current sharing initiatives and recommendations
- Conclusions
  - Efforts to improve: cybersecurity, capability, consciousness,

Why to share in Internet?

CYBER 7
SEVEN MESSAGES TO THE EDGE OF CYBER-SPACE

1 CONTEXT is more relevant than the volume of information

2 SHARING is promising but does not yet work properly

3 cyber threat STATISTICS will need to be elaborated

4 cyber ATTACK METHODS become more pervasive

5 THREAT AGENTS need to be looked at more closely

6 INTERNET OF THINGS is here to stay, so is the cyber threat exposure that it represents

7 lessons from DATA BREACHES in 2015

1

CREATING CONTEXT MEANS MAKING MORE CYBER-SECURITY SENSE

In cyber-security, it is important to create as much as possible long-living contextual information and knowledge on threats from the vast amount of short-living incident data. The acquired KNOWLEDGE and CONTEXT should be of high quality and be transferrable to all relevant players in the cyber space.

2

INTELLIGENT SHARING OF CYBER THREAT INTELLIGENCE

SHARING of cyber-threat intelligence will be more efficient if the context of shared information is known and if there is a balance of knowledge among the participating parties.

There is a lot of work to be done to achieve this.

3

THE ISSUE WITH THE STATISTICS AND METRICS

The STATISTIC and METRICS models used in cyber-threat intelligence require elaboration. Otherwise the quality and comparability of the achieved results will remain questionable. This is an obstacle in the creation of usable, contextual cyber threat intelligence.

5

CYBER THREAT AGENTS:
THE BIG UNKNOWN IN THE CYBER-EQUATION

Efforts to increase attribution rates of CYBER THREAT AGENTS are necessary. This will lead primarily to sentence already performed criminal activities, but it will also achieve precedent and increase the knowledge about who is the enemy.

6

THE NEW FIELD OF CYBER-ABUSE: INTERNET OF THINGS

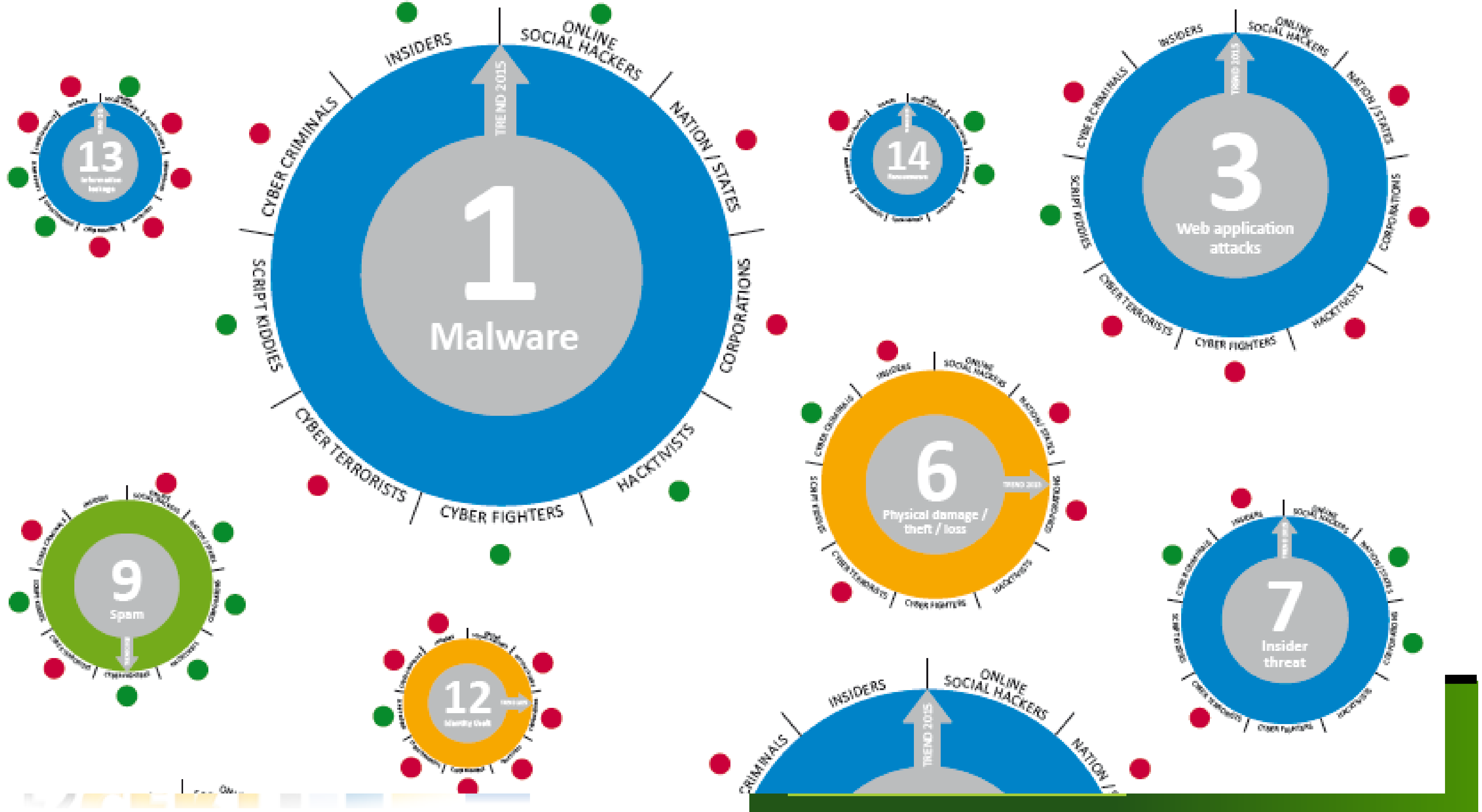
The INTERNET OF THINGS is at the edge of the cyber-space. As such, cyber-security must be embedded and ready-to-use without any technical knowledge. In order to achieve this, a bigger cooperation between producers and operators of technical systems, but also society and service providers will be necessary.

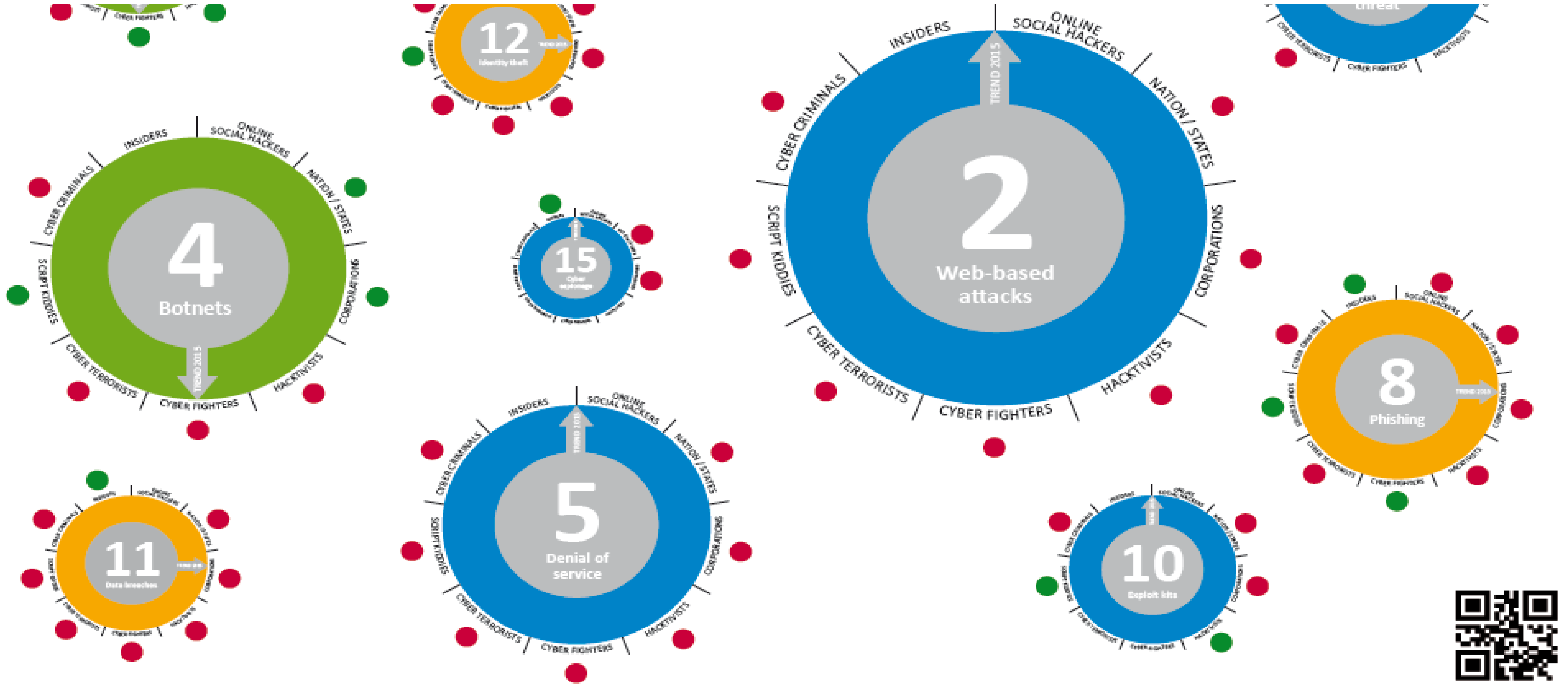
DATA BREACHES: THE DEBRIS OF CYBER-SPACE

Lessons learned from DATA BREACHES are one of the most valuable resources for cyber intelligence. Lessons learned need to be made available for all relevant stakeholders at the highest speed possible. The form of this information need to be such, that it can be immediately translated to corrective actions.

ENISA threat landscape

Top 15 Cyber Threats 2015





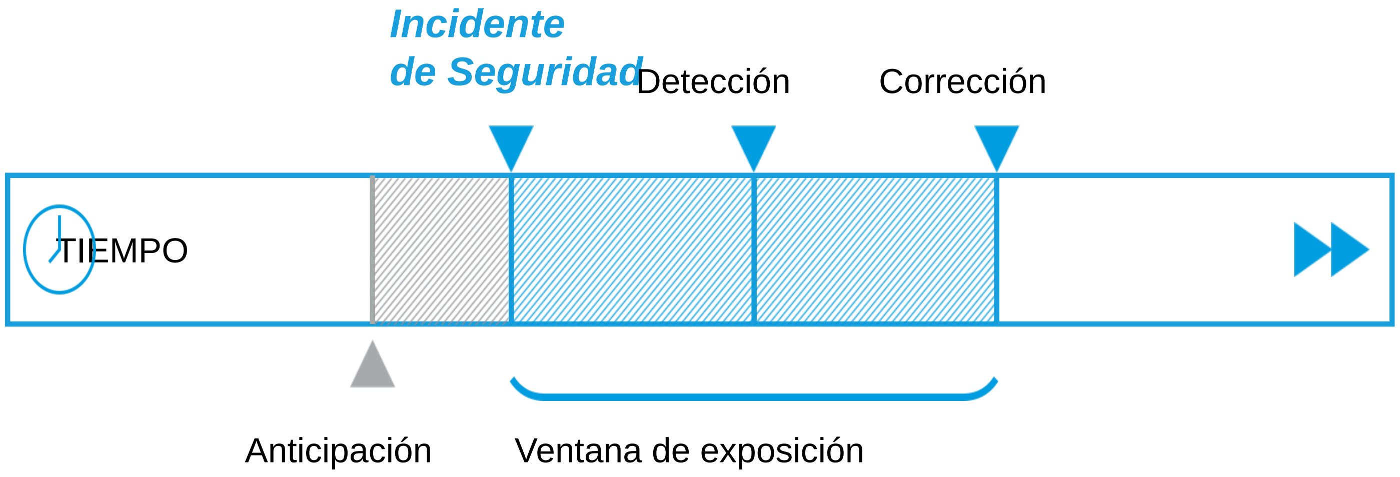
RANKING OF ASSESSED CYBER THREATS

LEGEND ● Primary group for threat ● Secondary group for threat ↑ Increasing trend ↓ Declining trend → Stable trend

2014	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
TREND	↑	↑	↑	↓	↑	↓	↑	↓	↑	↑	→	↑	↑	↑	↓
TOP 15	Malicious code: Worms / Trojans	Web-based attacks	Web application / Injection attacks	Botnets	Denial of service	Spam	Phishing	Exploit kits	Data breaches	Physical damage / theft / loss	Insider threat	Information leakage	Identity theft / fraud	Cyber espionage	Ransomware / Rogueware / Scareware
2013	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
TREND	↑	↑	↑	↑	→	↑	↑	↑	↑	→	↑	↑	↑	↑	↑
TOP 15	Drive by downloads	Worms / Trojans	Code Injection	Exploit kits	Botnets	Physical damage / theft / loss	Identity theft / fraud	Denial of service	Phishing	Spam	Ransomware / Rogueware / Scareware	Data breaches	Information leakage	Targeted Attacks	Watering Hole

The ultimate goal: ANTICIPATION

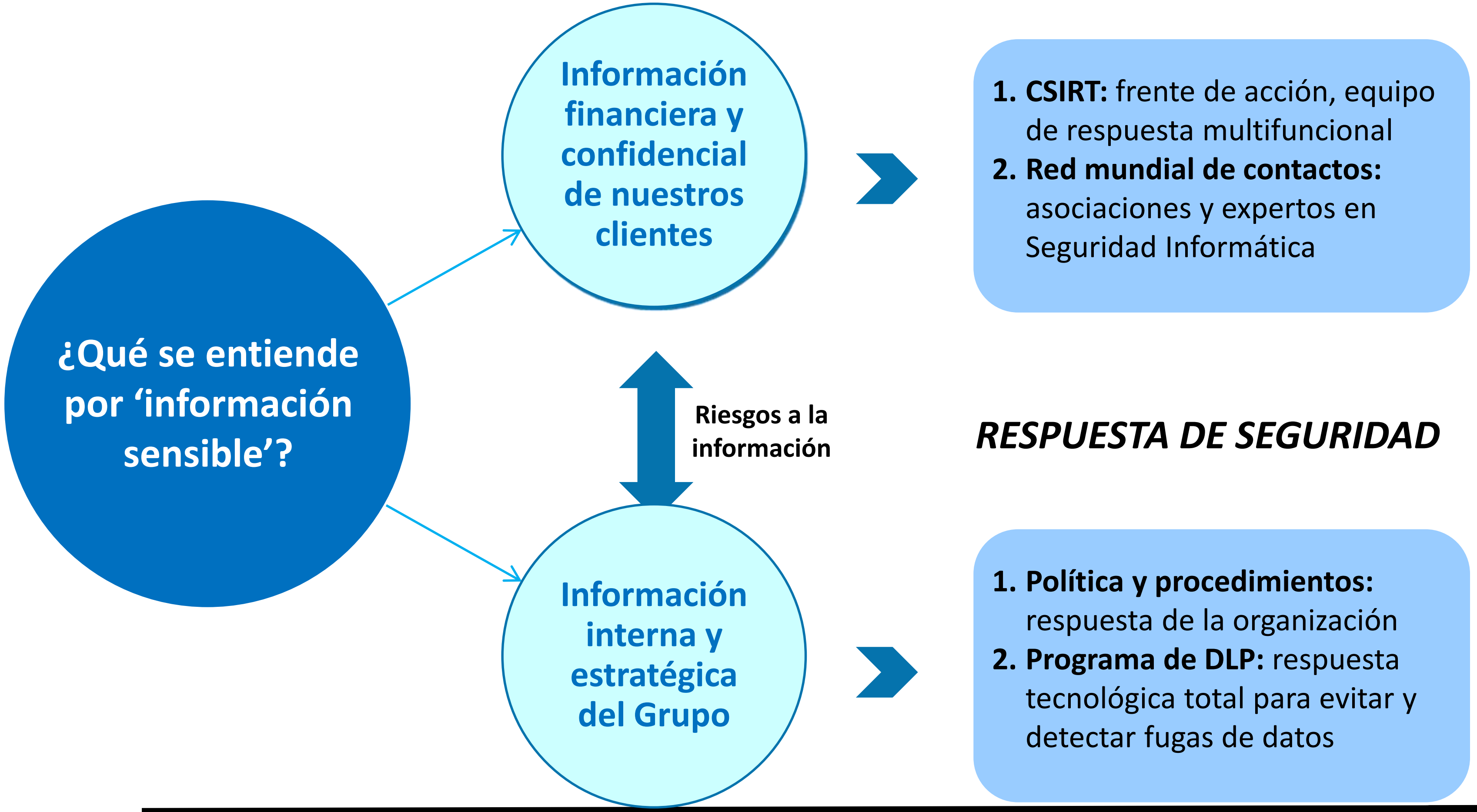
Las técnicas y los algoritmos de iSOC permiten adelantarse a los posibles incidentes de seguridad que sucedan y así, reducir aún más el tiempo que está expuesto un cliente o el banco a un problema de seguridad.



What to share: data vs information

Legal Constraints: Personal data protection

B. DLP: Protección de la información sensible



¿Qué se entiende por ‘información sensible’?

Información financiera y confidencial de nuestros clientes

Información interna y estratégica del Grupo

Riesgos a la información

1. **CSIRT:** frente de acción, equipo de respuesta multifuncional
2. **Red mundial de contactos:** asociaciones y expertos en Seguridad Informática

RESPUESTA DE SEGURIDAD

1. **Política y procedimientos:** respuesta de la organización
2. **Programa de DLP:** respuesta tecnológica total para evitar y detectar fugas de datos

Respuesta a Incidentes

Punto de contacto del operador y CERT

- Notificación incidentes: pic@cert.inteco.es
- Otras cuestiones: ses.occ@interior.es
  info.pic@inteco.es
- SOC 24x7: 647300717

Toda la comunicación estará auspiciada bajo un **Acuerdo de Confidencialidad**

SOC -> CSIRT : Información que el operador debería enviar al notificar un incidente

- Activos afectados
- Descripción del caso
- Evidencias del caso (captura, log, etc.)

Información de seguimiento que proporciona el CERT

- Información en poder del CERT
- Solicitud de más información
- Identificador del incidente

Informe de cierre que proporciona el CERT

- Hallazgos
- Pasos a seguir por parte del operador para la desinfección / recuperación

cert.org: Incident management Publications

- Collecting Evidence/Forensics
  CERT forensics work, basic forensic data collection, and forensic methodology.
- Incident Management and General CSIRT Publications

- Security and Ontology
  need for controlled vocabularies, taxonomies, and ontologies to make progress toward a science of cybersecurity.
- An Incident Management Ontology
  In this paper, the authors describe the shortcomings of the incident management meta-model and how an incident management ontology addresses those shortcomings.
- Competency Development
  Workforce effectiveness relies on two critical characteristics: competence and readiness. Our work in competency development is designed to help organizations improve their training and development programs. Our researchers identify and document cybersecurity competencies within organizations. As these competencies are identified, the organization begins to understand that competence is not readiness.

ENISA information sharing

- https://www.enisa.europa.eu/activities/cert/support/information-sharing
  - **European FI-ISAC, A Public-Private Partnership**
  - **Scalable and Accepted Methods for Trust Building**
  - **Detect, SHARE, Protect - Solutions for Improving Threat Data Exchange among CERTs**

ENISA: Actionable Information for Security Incident Resp.

ENISA publishes a good practice guide

- challenges national CERTs and other security organizations encounter as they try to generate actionable output from large amounts of data.
- overview of the current information-sharing landscape in the context of generating actionable information
- identifies existing tools and standards,
- reports best practices and gaps, and
- provides recommendations for improvement

- Actionable Information for Security Incident Response
- Standards and tools for exchange and processing of actionable information
- Using indicators to enhance defence capabilities-Actionable information

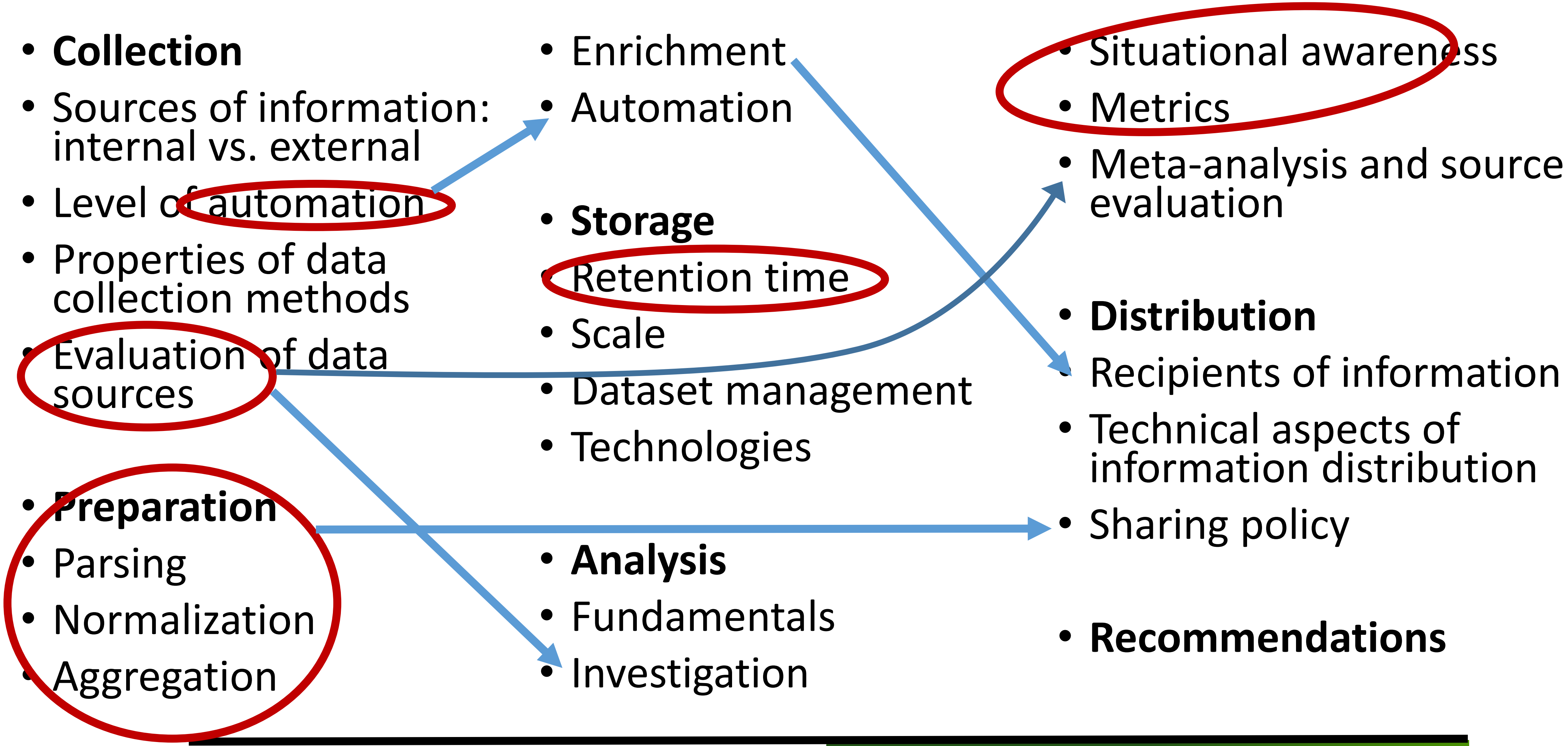
ENISA: Actionable information sharing

- **Properties of actionable information**
- Relevance
- Timeliness
- Accuracy
- Completeness
- Ingestibilty

- **Levels of information**
- Low-level data
- Detection indicators
- Advisories
- Strategic reports

- **Destination**
- SOC
- CERT/CSIRT
- CIO/CISO
- CEO

Processing actionable information



- **Collection**
- Sources of information: internal vs. external
- Level of automation
- Properties of data collection methods
- Evaluation of data sources

- **Preparation**
- Parsing
- Normalization
- Aggregation

- Enrichment
- Automation

- **Storage**
- Retention time
- Scale
- Dataset management
- Technologies

- **Analysis**
- Fundamentals
- Investigation

- Situational awareness
- Metrics
- Meta-analysis and source evaluation

- **Distribution**
- Recipients of information
- Technical aspects of information distribution
- Sharing policy

- **Recommendations**

Analyzing the Data (org. impact)

Snapshot from the training materials

Some questions that we would like to answer…

- **correlation** between number of **incidents** and economy growth
  - How does addressing an incident affect the **economy**?
- How much does an **incident ‘cost**’?
  - In terms of **economy**
  - In terms of **man/hours**
- **correlation** between **growth in internet users** and number of **incidents**
  - Compare with population skills also
- How many **people are actually affected** when something goes wrong?
- What is the **average lifespan of a phishing site** (compromise)?

Comparing and Trending ASN’s (network impact)

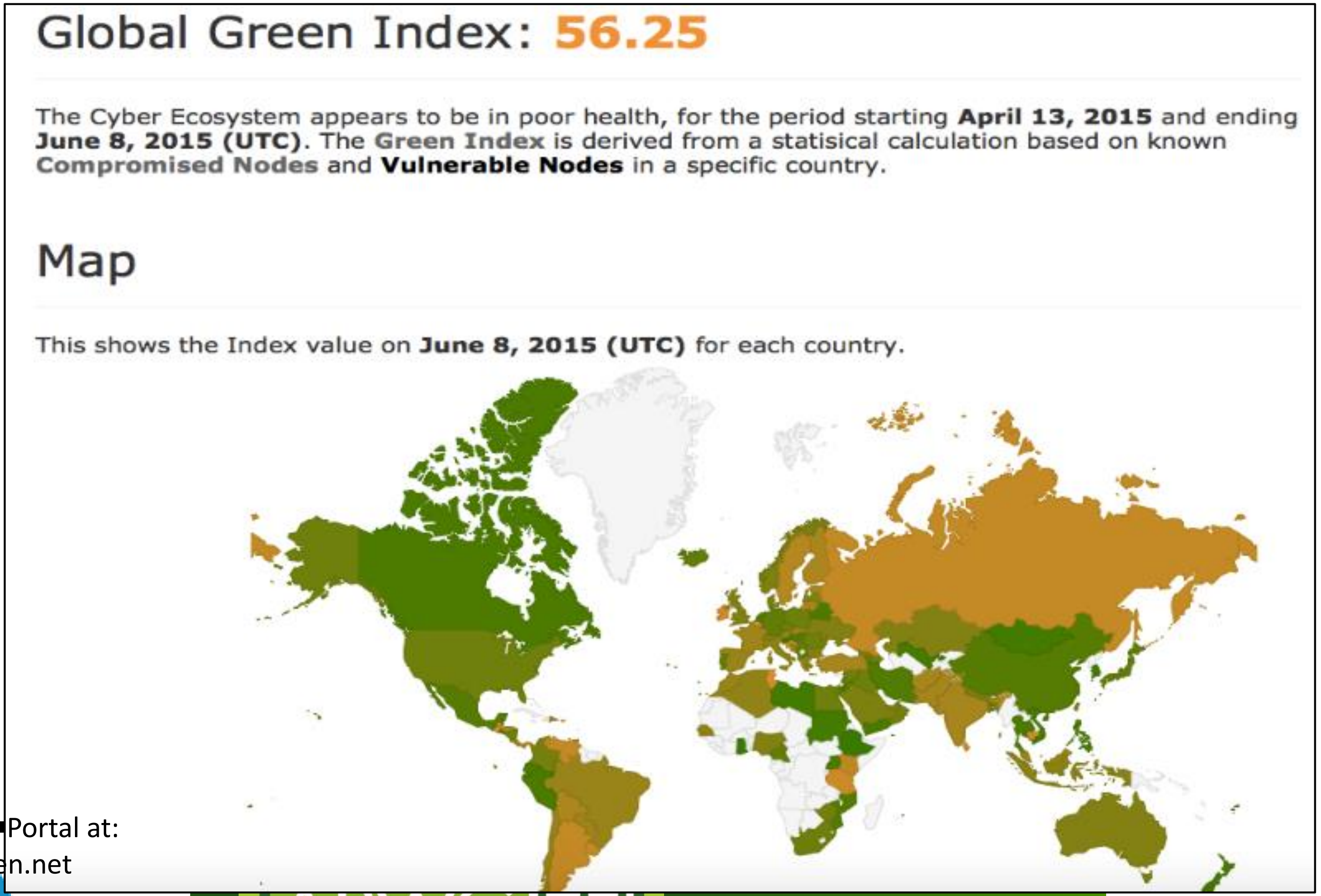
Snapshot from the training materials

- Performance (nodes)
  - Increase / Decrease
- Average time that a node exists as compromised
  - Look at the data and see when an **IP ‘disappears**’
  - IP’s may ‘**re-appear’**
  - Take a look at how often this happens within an ASN
- Is this something that should be explored?

The CyberGreen Initiative

- Mission: The CyberGreen project will improve cyber health by enhancing collaboration between key stakeholders in cyberspace

- How will CyberGreen Accomplish its Mission:
  CyberGreen established a reliable platform for generating cross-comparable statistics & information sharing mechanisms to enable operational cyber remediation efforts and provide insight into systemic risk conditions in the cyber ecosystem.



Global Green Index: **56.25**

The Cyber Ecosystem appears to be in poor health, for the period starting **April 13, 2015** and ending **June 8, 2015 (UTC)**. The **Green Index** is derived from a statisical calculation based on known **Compromised Nodes** and **Vulnerable Nodes** in a specific country.

Map

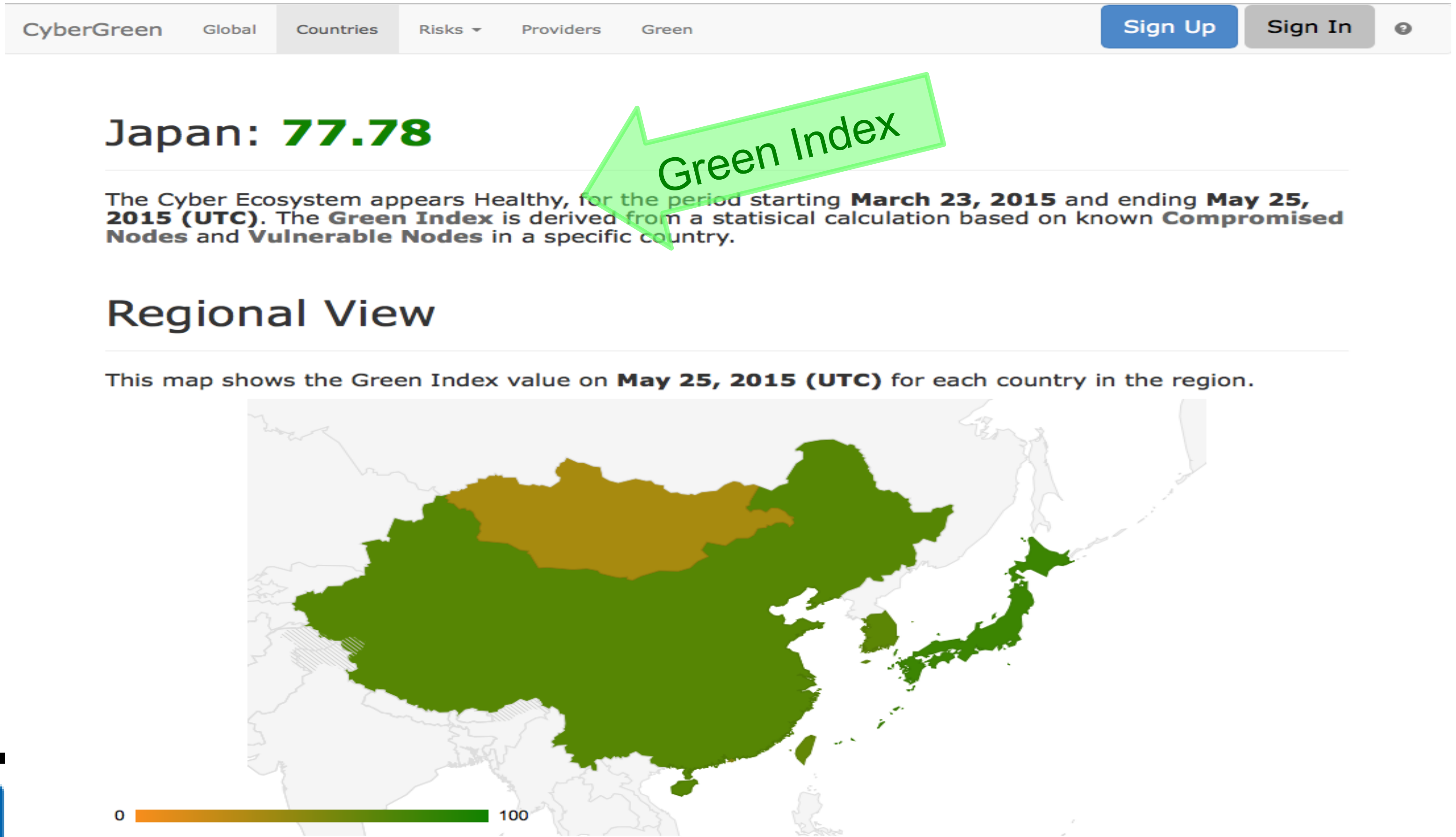
This shows the Index value on **June 8, 2015 (UTC)** for each country.

CyberGreen Statistics Portal at: http://stats.cybergreen.net

What is the Green Index – Overview

Snapshot from the training materials

- Represents if a region is becoming “more healthy” or “less healthy”
  - A number between **0 (getting worse) and 100 (getting better).**
- Calculated using 2 categories of data
  - # of **Compromised** Nodes, such as zombie-PCs
  - # of **Vulnerable** Nodes, such as open resolvers
- Gathered data are categorized into the each of the 2 buckets above for calculation



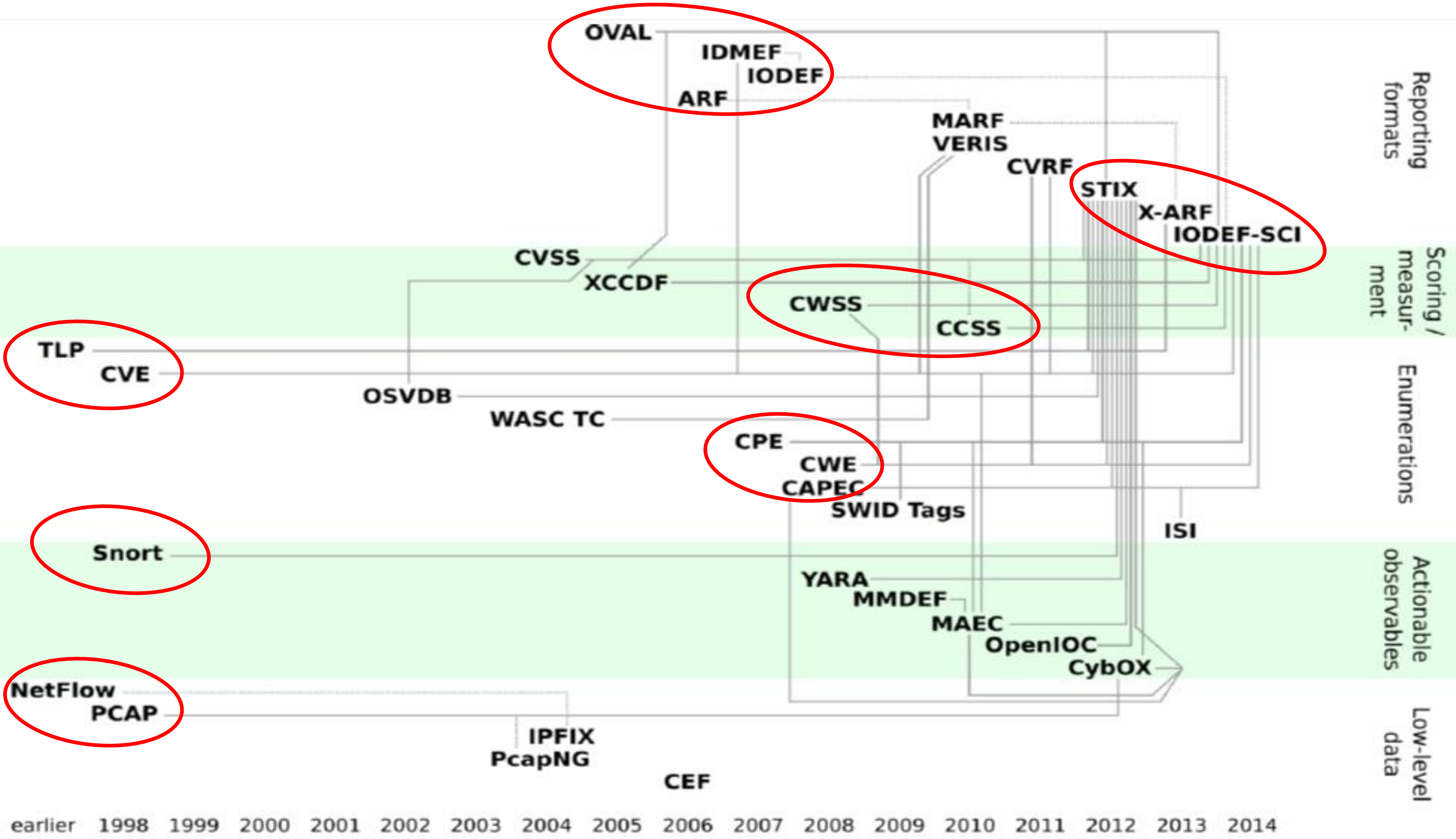
Japan: **77.78**

The Cyber Ecosystem appears Healthy, for the period starting **March 23, 2015** and ending **May 25, 2015 (UTC)**. The **Green Index** is derived from a statisical calculation based on known **Compromised Nodes** and **Vulnerable Nodes** in a specific country.

Regional View

This map shows the Green Index value on **May 25, 2015 (UTC)** for each country in the region.

How to share: manual vs automatic, actionable vs statistic



OVAL
IDMEF
IODEF
ARF
MARF
VERIS
CVRF
STIX
X-ARF
IODEF-SCI
CVSS
XCCDF
CWSS
CCSS
TLP
CVE
OSVDB
WASC TC
CPE
CWE
CAPEC
SWID Tags
ISI
Snort
YARA
MMDEF
MAEC
OpenIOC
CybOX
NetFlow
PCAP
IPFIX
PcapNG
CEF

Reporting formats
Scoring / measur-ment
Enumerations
Actionable observables
Low-level data

earlier 1998 1999 2000 2001 2002 2003 2004 2005 2006 2007 2008 2009 2010 2011 2012 2013 2014

IODEF: Incident Object Description and Exchange Format

- **VEDEF - Vulnerability and Exploit Description and Exchange Format**
- **SecDEF - Security Description and Exchange Format**
- **ENISA baseline capabilities of national/governmental CERTs**

The report cover recommendations and proposals for capabilities of so called national / governmental CERTs, thus teams who serve the government of a country to protect critical information infrastructure. http://www.enisa.europa.eu/activities/cert/support/baseline-capabilities

TERENA's Incident Object Description and Exchange Format

IODEF notification

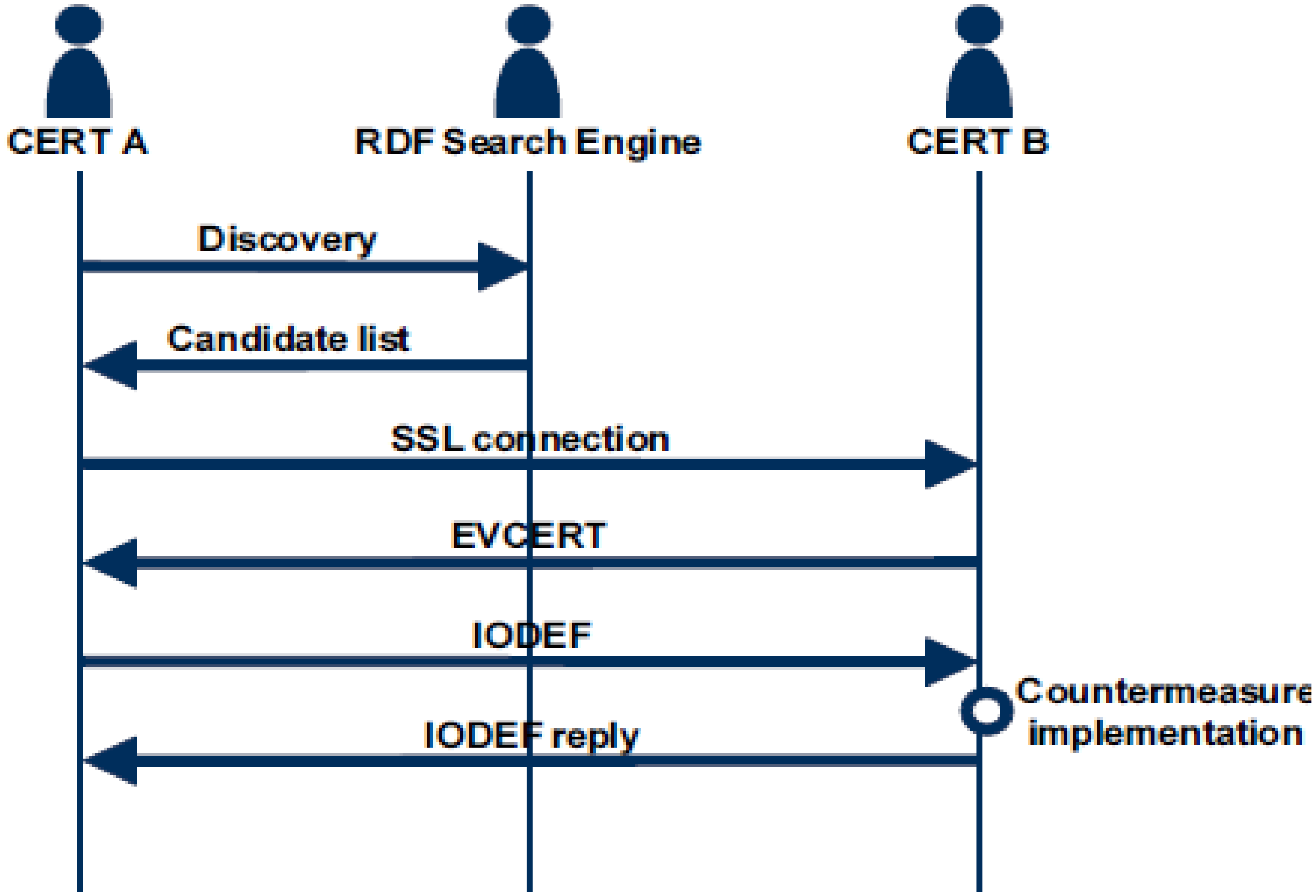


Figure 8: IODEF information notification

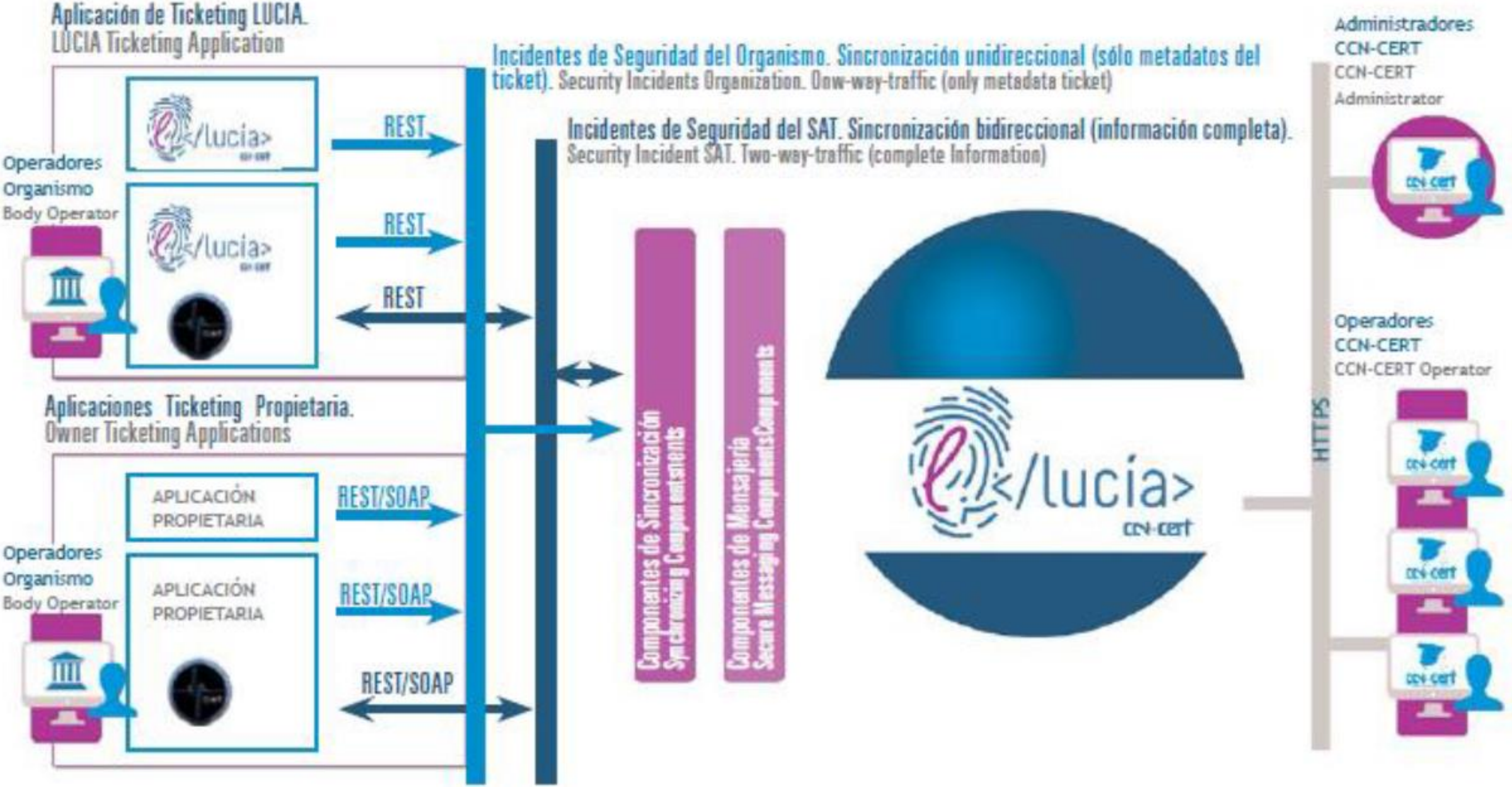
RTIR

- Evolution of RT, intended for: Bug tracking, helpdesk, customer service, abuse, network operations, sales lead tracking, to do lists….
- RTIR adds:
  - IRT specific workflows
  - ‘clicky’ data extraction and tracking
  - whois integration
  - separate “threads” for each conversation
  - convenient searching
  - simple scriptable actions
  - new reporting functionality tied into our new SLA requirement

LUCIA: CCN-CERT

- LUCIA (Listado Unificado de Coordinación de Incidentes y Amenazas) es una herramienta desarrollada por el CCN-CERT para la Gestión de Ciberincidentes en las entidades del ámbito de aplicación del Esquema Nacional de Seguridad. Con ella se pretende mejorar la coordinación entre el CERT Gubernamental Nacional y los distintos organismos y organizaciones con las que colabora.
- LUCIA ofrece un lenguaje común de peligrosidad y clasificación del incidente y mantiene la trazabilidad y el seguimiento del mismo. El sistema permite, además, automatizar las tareas e integrarse con otros sistemas ya implantados.
- Con la herramienta LUCIA, el organismo podrá gestionar tres tipos de ciberincidentes:
- Los incidentes propios del Organismo
- Los provenientes del Sistema de Alerta Temprana de Red SARA (SAT-SARA).
- Los provenientes del Sistema de Alerta Temprana de Internet (SAT-INET).

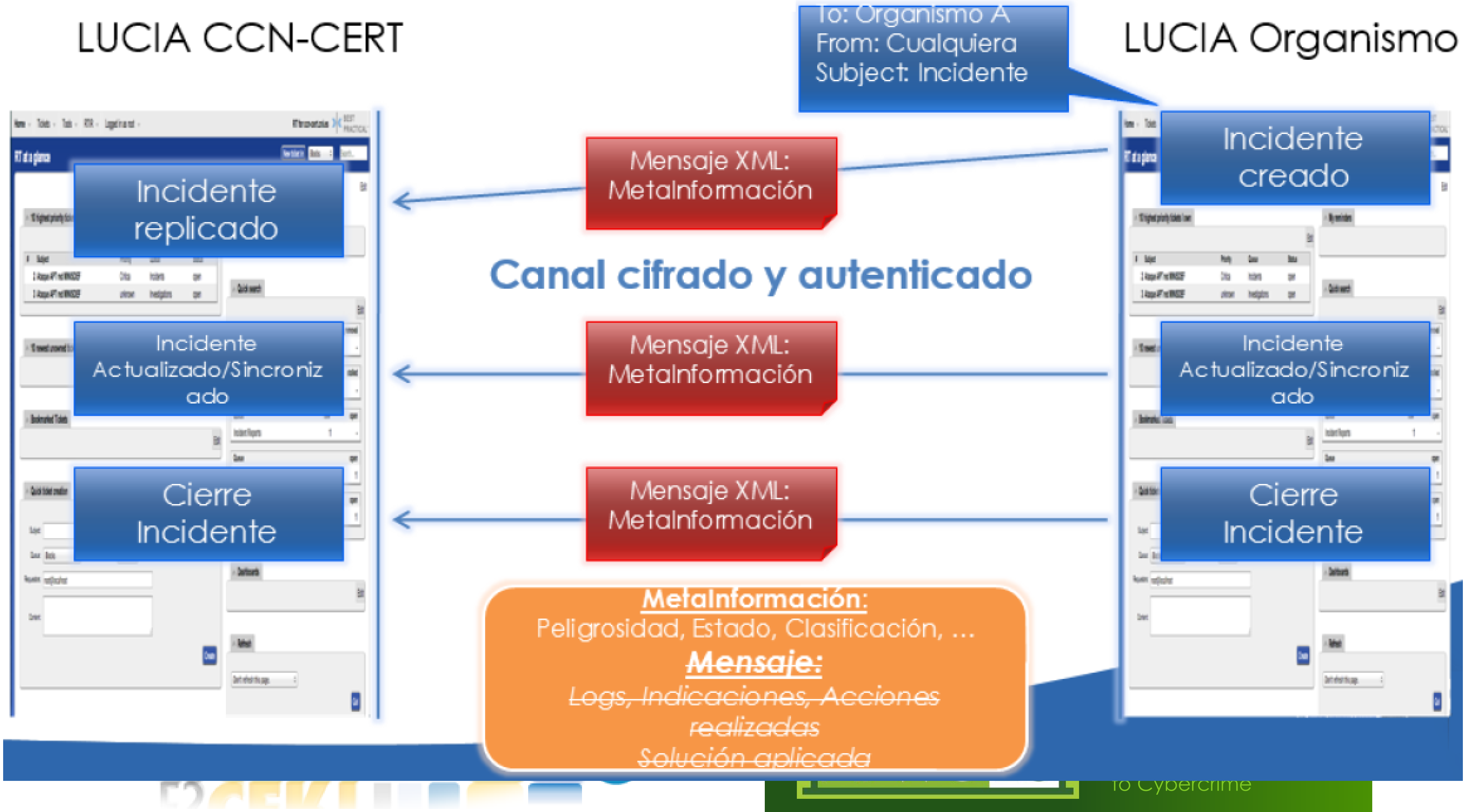
esquema de federación de sistemas LUCIA



Incidentes de Seguridad del Organismo. Sincronización unidireccional (sólo metadatos del ticket). Security Incidents Organization. Oow-way-traffic (only metadata ticket)

Incidentes de Seguridad del SAT. Sincronización bidireccional (información completa). Security Incident SAT. Two-way-traffic (complete Information)

LUCIA: intercambio unidireccional no-integrado



LUCIA CCN-CERT

LUCIA Organismo

To: Organismo A
From: Cualquiera
Subject: Incidente

Incidente creado

Incidente replicado

Mensaje XML: MetaInformación

Canal cifrado y autenticado

Incidente Actualizado/Sincronizado

Mensaje XML: MetaInformación

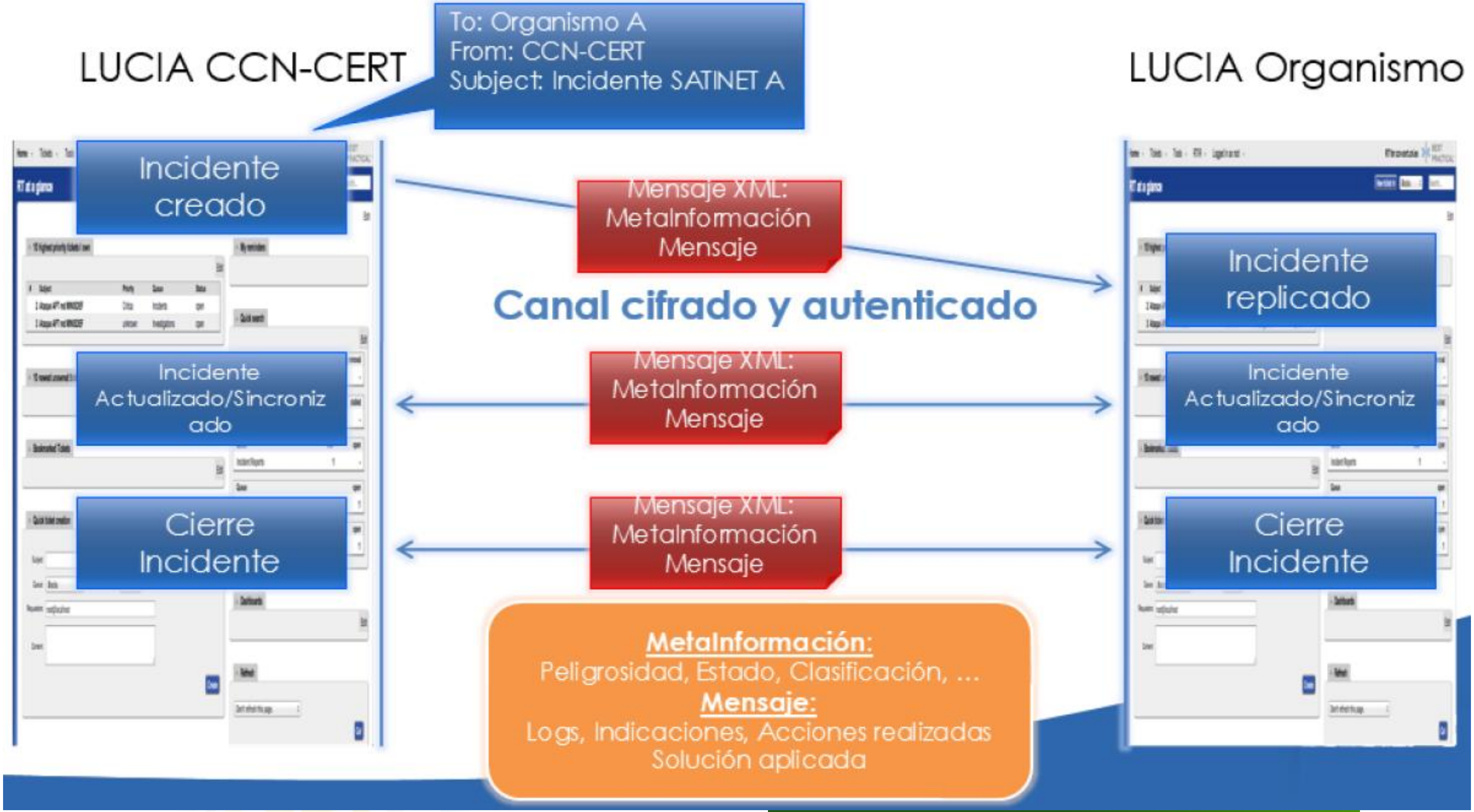
Cierre Incidente

Mensaje XML: MetaInformación

MetaInformación:
Peligrosidad, Estado, Clasificación, …

Mensaje:
~~Logs, Indicaciones, Acciones realizadas~~
~~Solución aplicada~~

LUCIA: intercambio unidireccional org. integrado



LUCIA CCN-CERT

To: Organismo A
From: CCN-CERT
Subject: Incidente SATINET A

LUCIA Organismo

Incidente creado

Mensaje XML:
MetaInformación
Mensaje

Incidente replicado

Canal cifrado y autenticado

Incidente Actualizado/Sincronizado

Mensaje XML:
MetaInformación
Mensaje

Incidente Actualizado/Sincronizado

Cierre Incidente

Mensaje XML:
MetaInformación
Mensaje

Cierre Incidente

MetaInformación:
Peligrosidad, Estado, Clasificación, …
Mensaje:
Logs, Indicaciones, Acciones realizadas
Solución aplicada

Current sharing initiatives and recommendations

Recom. ITU-T X.1500 (Cybersecurity) CYBEX SG17, Q4/17

Objectives:

(a) determining in real time the security integrity of systems and services, and

(b) collecting and maintaining relevant security incident data in a form suitable for sharing among Information Assurance, and incident response communities as appropriate.

Means:

1. “locking down” on-line systems to minimize vulnerabilities,
2. capturing incident information for subsequent analysis when harmful incidents occur,
3. exchanging threat information, including attacks and malware specifics, in a structured manner,
4. discovering and exchanging related information with appropriate degree of assurance.

Goals:

Approved in April 2015 SG17 meeting, five years of work resulted in 20 standards.

Incorporates 1st **structured ontology for Cybersecurity information exchange**, produced by Japan’s NICT research centre.

The Appendix I includes latest developments in CYBEX techniques, including:

- threat sharing expression, attack pattern enumeration and malware description format, e.g. ITU-T X.1544 and X.1546.
- weaknesses within software ITU-T X.1524,
- weakness scoring of software ITU-T X.1525.

The ITU-T mission includes facilitating collaboration among Computer Incident Response Teams (CIRTs) worldwide. Q.4/17 has built a close collaborative relationship with the Forum of Incident Response and Security Teams (FIRST) organization.

Q.4/17 also maintains a compilation of discovered CIRTs and related agencies and bodies to the SG 17 website at: http://www.itu.int/en/ITU-T/studygroups/2013-2016/17/Pages/nfvo.aspx

CYBEX X.1500 – Framework family

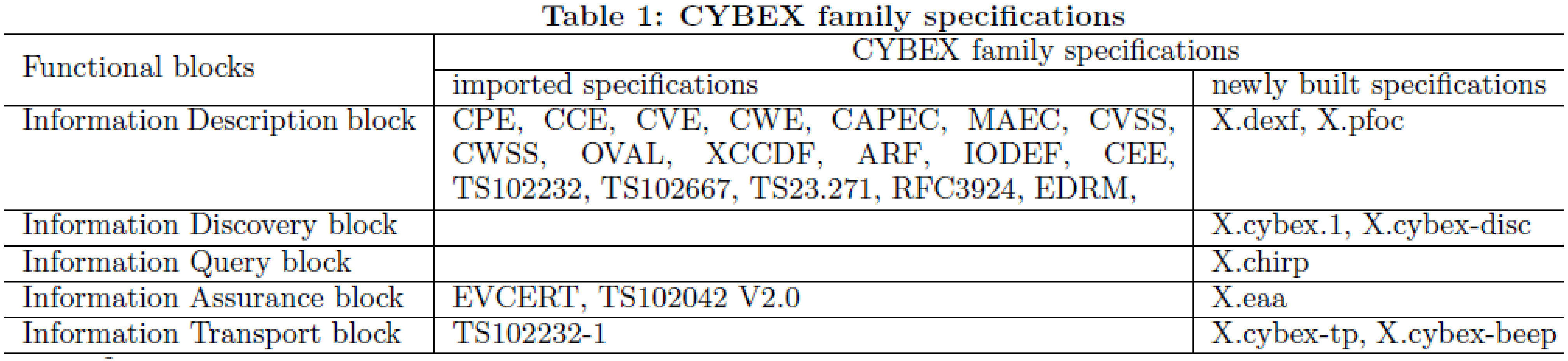
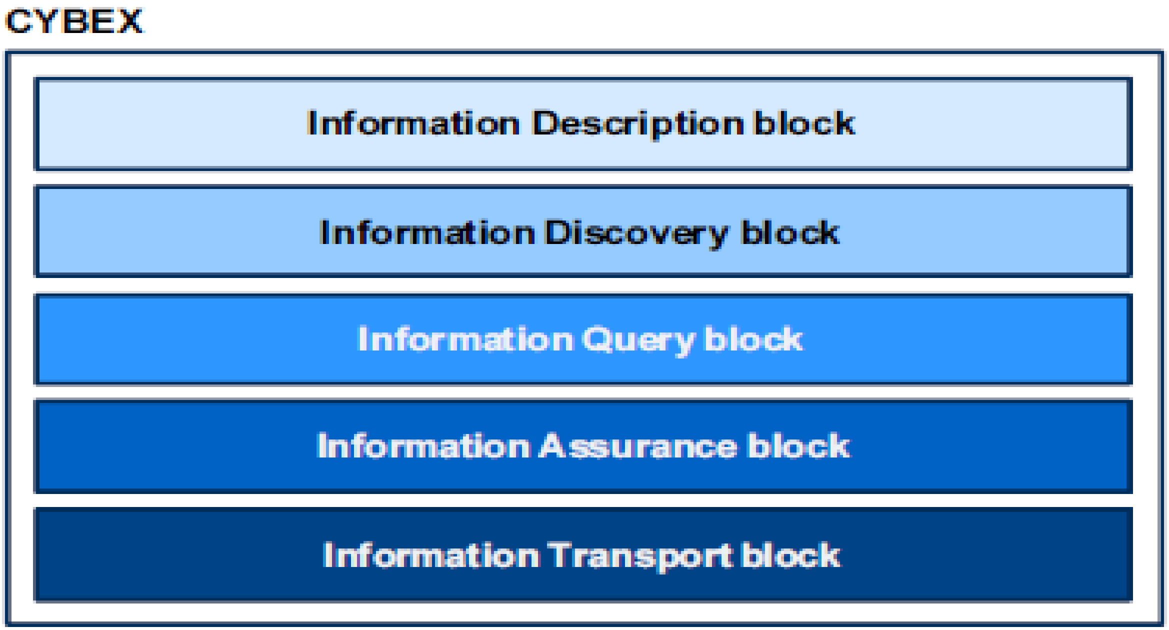


Table 1: CYBEX family specifications

Functional blocks	CYBEX family specifications	
	imported specifications	newly built specifications
Information Description block	CPE, CCE, CVE, CWE, CAPEC, MAEC, CVSS, CWSS, OVAL, XCCDF, ARF, IODEF, CEE, TS102232, TS102667, TS23.271, RFC3924, EDRM,	X.dexf, X.pfoc
Information Discovery block		X.cybex.1, X.cybex-disc
Information Query block		X.chirp
Information Assurance block	EVCERT, TS102042 V2.0	X.eaa
Information Transport block	TS102232-1	X.cybex-tp, X.cybex-beep



CYBEX

Information Description block

Information Discovery block

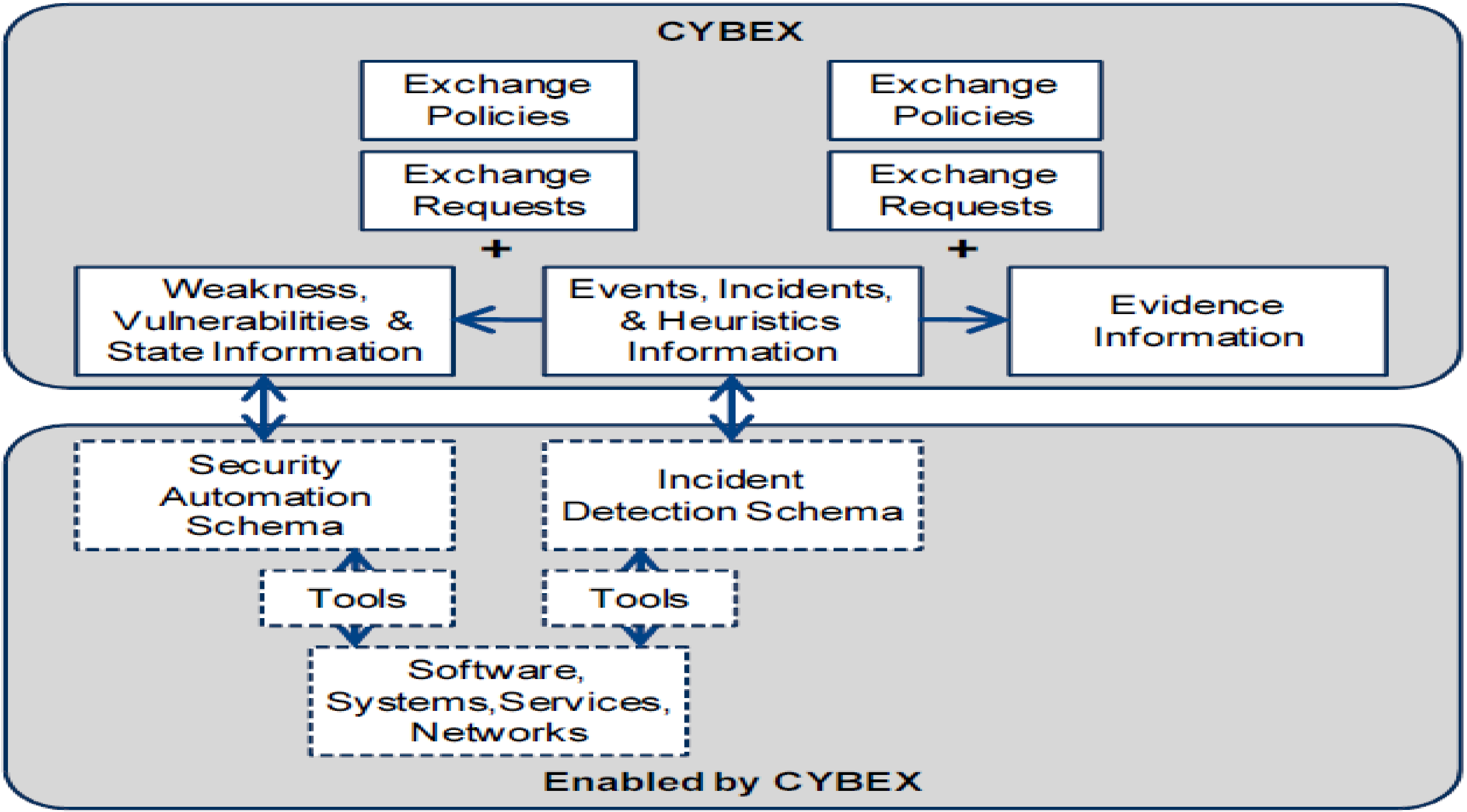
Information Query block

Information Assurance block

Information Transport block

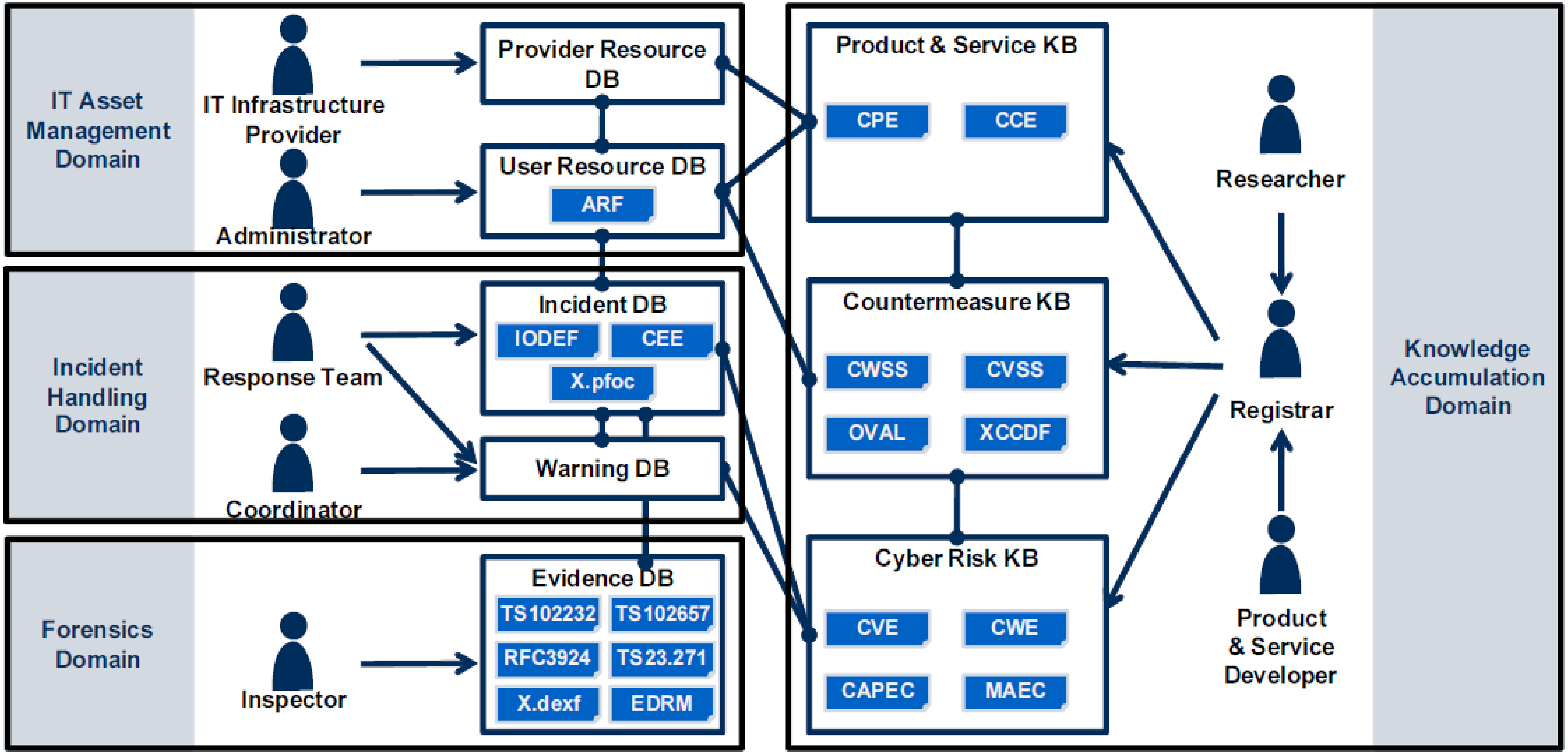
Unifying the
Global Response
to Cybercrime

Cybersecurity ecosystem enabled by CYBEX


CYBEX
Exchange Policies
Exchange Requests
+
Exchange Policies
Exchange Requests
+
Weakness, Vulnerabilities & State Information
Events, Incidents, & Heuristics Information
Evidence Information
Security Automation Schema
Incident Detection Schema
Tools
Tools
Software, Systems, Services, Networks
Enabled by CYBEX

Global Response to Cybercrime

CYBEX Blocks: Information Description Block



DB: Database KB: Knowledge Base

CYBEX Blocks: Information Description Block

- *Knowledge Accumulation Domain: e.g. National Vulnerability DB*
  - Cyber Risk
    - *Common Vulnerabilities and Exposures(CVE)*
    - *Common Weakness Enumeration (CWE) in software code, design, architecture, or implementation*
    - *Common Attack Pattern Enumeration and Classification (CAPEC): steps, impact, and mitigations*
    - *Malware Attribute Enumeration and Characterization (MAEC): behaviors and actions of malware with two core components consisting of enumerated elements (vocabulary) and schema (grammar)*
  - Countermeasure
    - *Common Vulnerability Scoring System (CVSS)* characteristics and impacts
    - *Common Weakness Scoring System (CWSS): SW* characteristics and impacts
    - *Open Vulnerability and Assessment Language (OVAL)*
    - *eXtensible Configuration Checklist Description Format (XCCDF)*
  - Product & Service,
    - *Platform Enumeration (CPE) [9, 13] and*
    - *Common Configuration Enumeration (CCE)*

CYBEX Blocks: Information Description Block

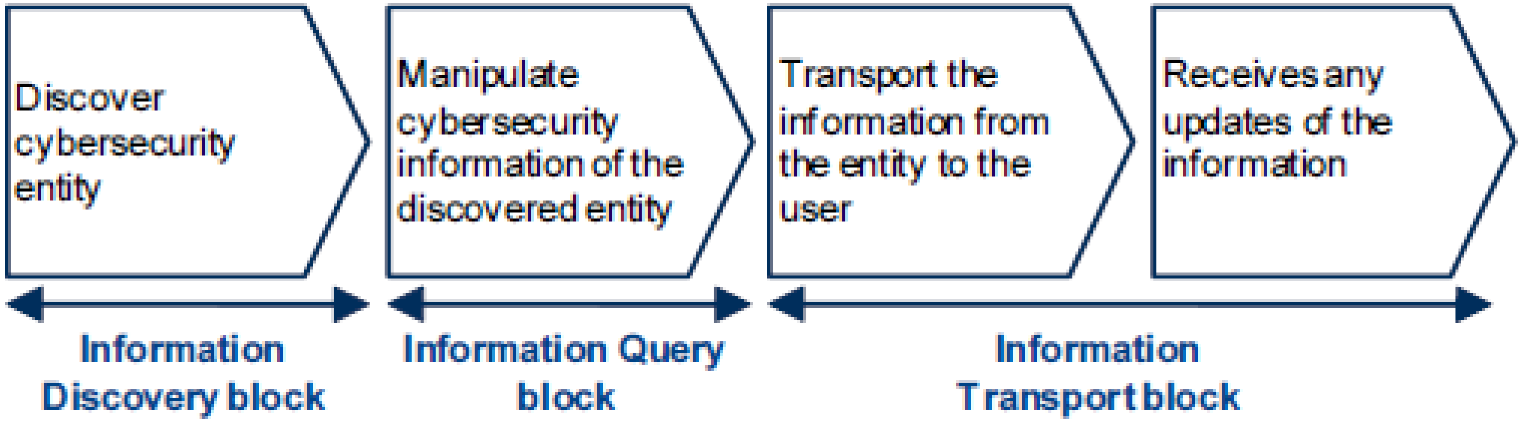
- *IT Asset Management Domain*
  - User Resource Database and Provider Resource Database. To describe information in the User Resource Database, CYBEX introduces the Assessment Result Format (ARF)
- *Incident Handling Domain*
  - Incident Object Description Exchange Format (IODEF)
  - X.pfoc, (Phishing, Fraud, and Other Crimeware Exchange Format) extends IODEF (includes widespread spam incidents)
  - Common Event Expression (CEE) language and syntax for expressing how events are described, logged, and exchanged

CYBEX blocks: Forensic domain

- **ETSI TS102232** defines a data representation that provides a framework for **exchange of information between a network mediation point and a law enforcement facility** to provide an array of different **real-time network forensics** associated with a designated incident or event.
- **ETSI TS102657** defines the same but with **stored network forensics**.
- **ETSI TS23.271** defines a data representation that provides a framework for exchange of information between a **network mediation point and an external facility** to provide an **real-time or stored** location forensics associated with a network device.
- **RFC 3924** defines a data representation that provides a framework for exchange of information between a **network access point and a provider mediation facility** to provide an array of different **real-time network forensics** associated with a designated incident or event.
- **EDRM** (Discovery Reference Model) defines a data representation that provides a framework for exchange of information between a **network mediation point and a juridical designated party** to request and provide an array of different stored network forensics associated with a designated incident or event.
- **X.dexf** (Digital Evidence Exchange Format) **defines structures and data elements** for structured digital evidence exchange.

CYBEX: Information Transport Block

- X.cybex-tp. transport protocols for cybersecurity information exchange. Protocol specific features are described in the
- X.cybex-beep. transport protocol based on BEEP
- Other candidate protocols, such as SOAP, exist but no draft recommendation for such protocols have been presented yet.
- ETSI TS102232-1 is also introduced here. This provides assurance of forensics information delivery to law enforcement and security authorities.



Discover cybersecurity entity

Manipulate cybersecurity information of the discovered entity

Transport the information from the entity to the user

Receives any updates of the information

Information Discovery block

Information Query block

Information Transport block

Figure 7: Cybersecurity information acquisition

FIRST:

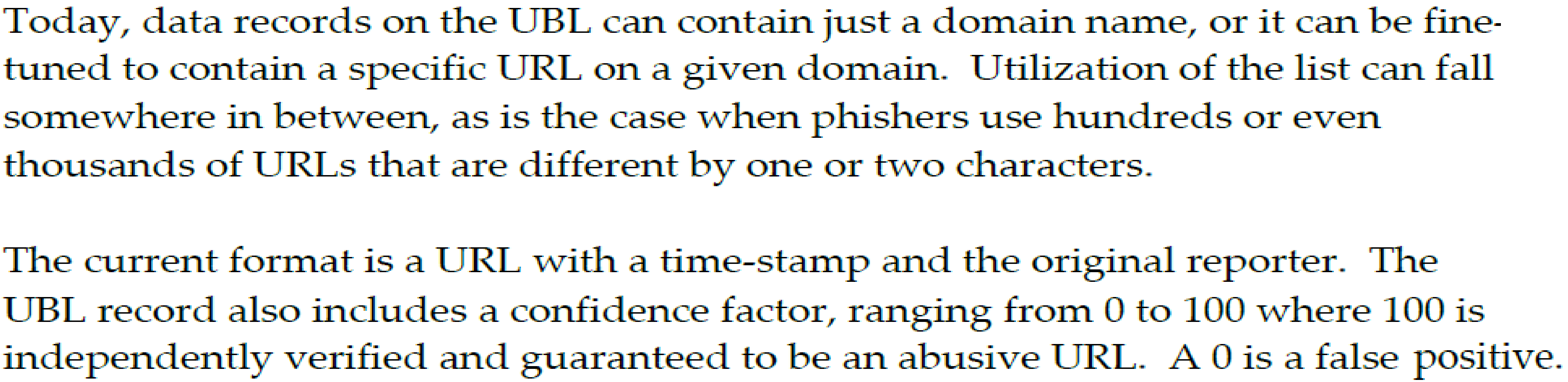
Structured information capabilities are organized into several exchange “clusters” for distinct cybersecurity user groups and requirements. Identified needs include:

- Vulnerability/Mitigation Exchange Cluster: SOC
- Event/Incident/Heuristics Exchange Cluster: CSIRT
- LEA/Evidence Exchange Cluster: CERT
- Cybersecurity organization identity and trust: CERT
- Cybersecurity Heuristics and Information Request Cluster: CSIRT+CERT

APWG & APWG.EU

- Founded in 2003 to focus on Phishing
- APWG.eu established 2014
- Began collecting data and create process for tracking Phishing
- Currently 1800+ companies, NGOs, government, law enforcement agencies, and treaty organizations worldwide
- Membership restricted to cybercrime-mangement stakeholders:
- Three Key Missions:
  - Data Exchange: UBL move up to 100 million records per day
  - Research: eCrime Symposium only peer-reviewed conference focusing exclusively on cybercrime
  - Global awareness: STOP. THINK. CONNECT.
- Common goal: suppression of cybercrime before it is inflicts damage

APWG eXchange

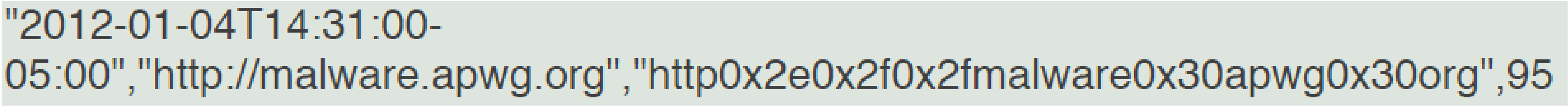


Today, data records on the UBL can contain just a domain name, or it can be fine-tuned to contain a specific URL on a given domain. Utilization of the list can fall somewhere in between, as is the case when phishers use hundreds or even thousands of URLs that are different by one or two characters.

The current format is a URL with a time-stamp and the original reporter. The UBL record also includes a confidence factor, ranging from 0 to 100 where 100 is independently verified and guaranteed to be an abusive URL. A 0 is a false positive.

Most **companies** choose a confidence factor of at least **80 or above** to utilize in their own block lists to minimize the absolute number of false positives that users may experience. A **responder organization**, however, may **examine every single UBL report** related to a brand that belongs to a client company, or a constituent, no matter what the confidence factor.

Accredited Reporters forward report records to APWG in a format that presents 1) the time of detection, 2) the phishing URL and 3) the confidence factor of the accuracy of the report



```
"2012-01-04T14:31:00-
05:00","http://malware.apwg.org","http0x2e0x2f0x2fmalware0x30apwg0x30org",95
```

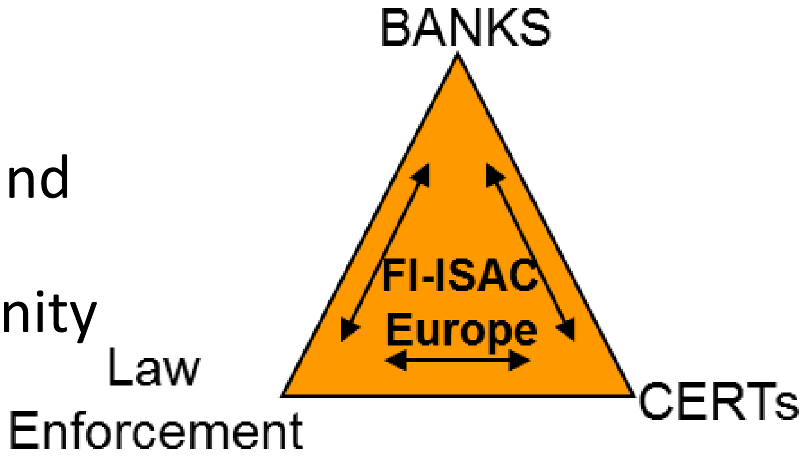
FI-ISAC

The European FI-ISAC, the European Financial Institutes – Information Sharing and Analysis Centre, is an independent organisation, that was founded in 2008.

Membership consists of country representatives coming from the financial sector, national CERT's (GovCerts) and Law Enforcement Agencies (LEA’s). Other organisations represented are: ENISA, Europol, the European Central Bank (ECB), the European Payments Council (EPC) and the European Commission. The European FI-ISAC is actively supported by ENISA.

Mission statement
The mission of the European FI-ISAC is information exchange on e- and m-channel, cards, central systems and all ICT related topics including:

- **Cyber-criminal activity** affecting the financial community
- **Vulnerabilities**, technology trends and threats
- **Incidents** and case-studies



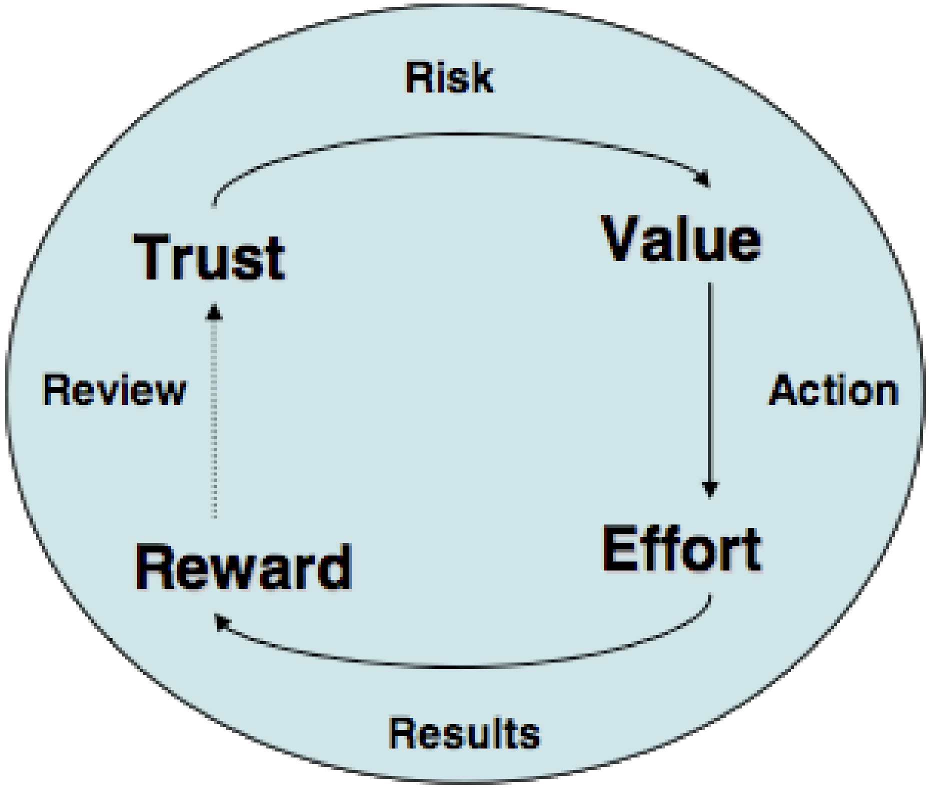
This **information exchange** helps each member and the banks in its member state, to **raise awareness on potentials risks**, and provides an **early warning** on new threats and MO's.

FI-ISAC: **Co-operation model**

The members share information by:

- Meeting twice per year
- Forwarding continuously relevant information via the EU FI-ISAC **list server**
- **Direct individual communication**

Trusted relationships are the key to successful co-operation and exchange between members. Members should actively information exchange.



Members cannot send PROXY to meetings.

Members of the European FI-ISAC must sign the Traffic Light Protocol (TLP).

The European FI-ISAC has signed a Memorandum of Understanding with Europol EC3. The MoU shows the mutual interest for co-operation between the European FI-ISAC and EC3, improving co-operation between the EU banking community and European LEA.

Good Practice PPP: Info sharing: ‘need to know’ vs ‘obligation to share’

Beliefs necessary for sharing cyber security information:

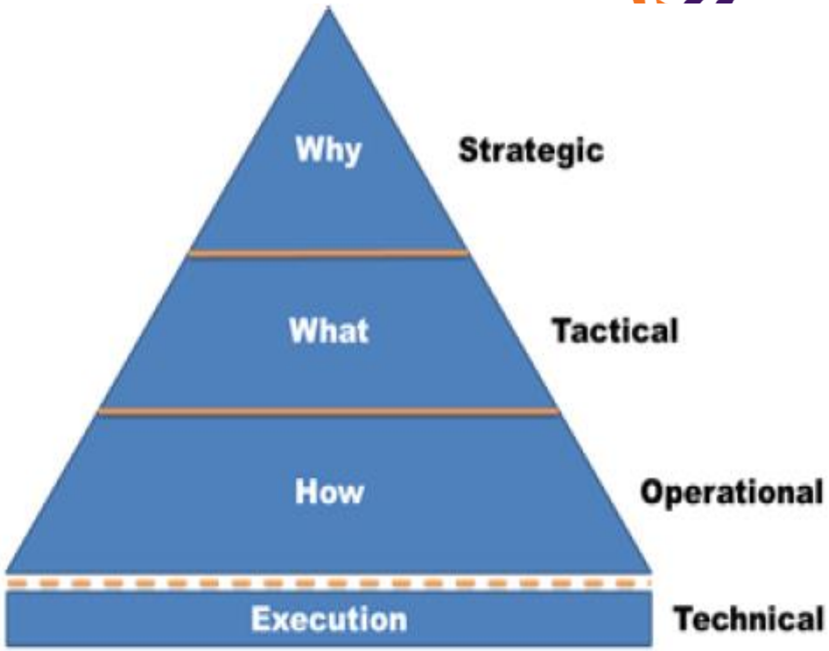
- *1. I know that my information is **important and urgent***
- *2. I know that what I **share will help others***
- *3. I know I am **trusted** by my organisation*
- *4. I know how to **get the information to the right people***
- *5. I know I can **control what happens with what I share***
- *6. I know **they will all act with my interests** at heart*
- *7. I know others will **reciprocate***

Good Practice PPP: Trust

- **Embed at the Top**: the CEO expects to be informed in a timely
- **Building Trust Takes Time**: introduction by a trusted third party, networks of trust and reputation-based trust anonymously established by voting: Information Sharing and Analysis Centre (ISAC) 2 or Information Sharing and Analysis Organisation (ISAO)
- **Mandated Sharing**: obligatory data breach notification reporting regarding large disturbances (EU telecommunications package Article 13a of and the European Directive on privacy and electronic communications Article 4)
- keep **investing in the creation of value for others** by sharing good information. find the right information in your organisation to assess what is valuable for both your own organisation and for others.
- To **start the spiral**: Putting some information of value on the sharing table will increase the other recipients' level of trust in your organisation
- make **use of existing initiatives**, and energy which is already moving in the right direction

Good Practice PPP: Sharing tips

- Sharing Levels, depends a lot on
  the relative job position & responsibilities:
  - the **strategic long-term policy-making** level,
  - the **tactical steering** level, bridging other both
  - the **operational** - **technical** level
- Focus in the Incident Management Cycle:
  - **Org**: pro-action3, via prevention, preparation,
  - **CERT**: incident response, recovery, and
  - **LEA**: intelligence to prevent, evidences & situational info.
  - **All**: aftercare/ (legal) follow-up activities

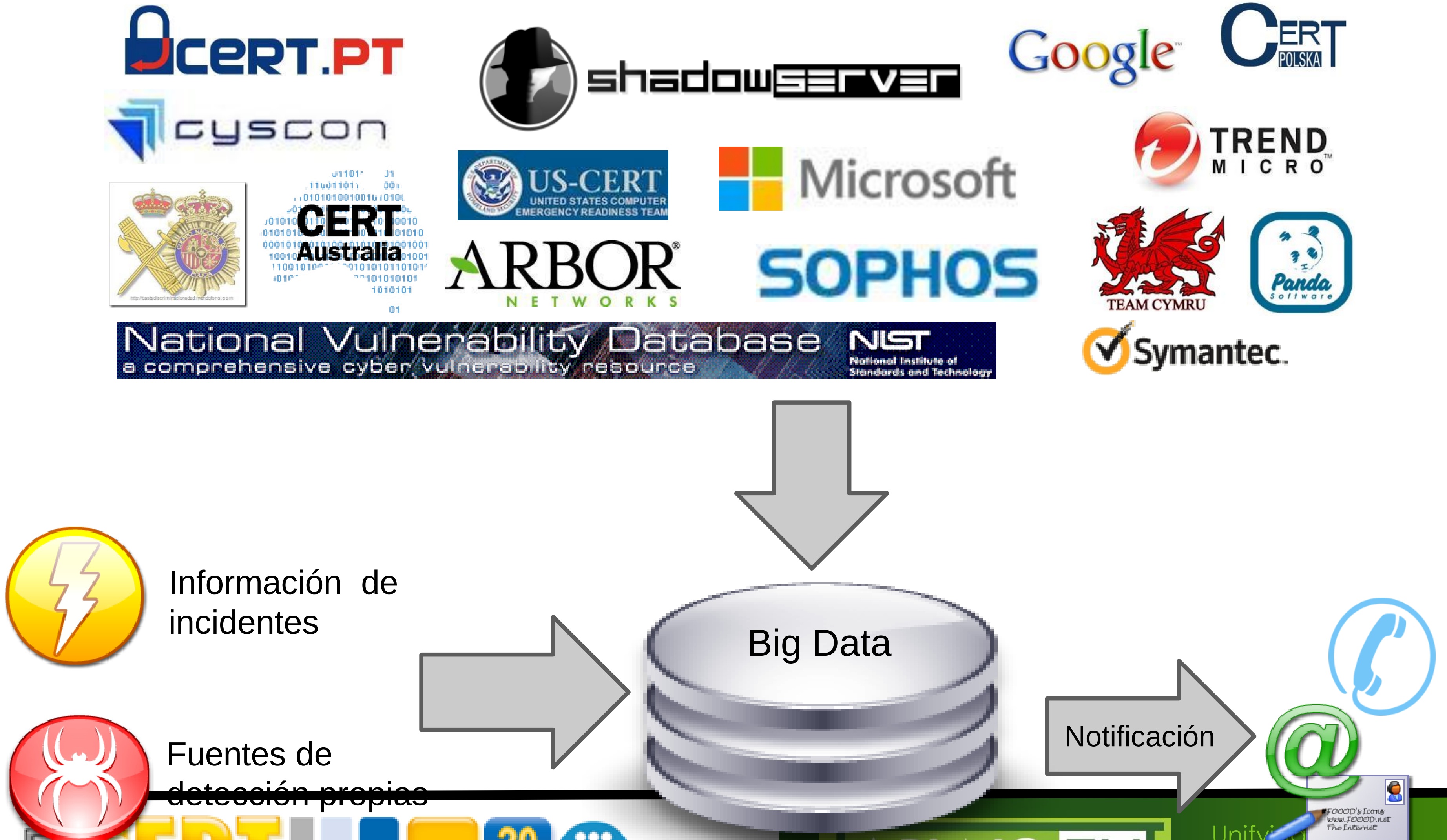


- Actionable Information for the Right Level and Responsibility
  - Adds value? Has relevance? Is timely, accurate, complete, digestible?
  - **subtypes of information** on: actor **intelligence** and **law enforcement**, background and **reference**, **compliance** status, **detection** and **mitigation**, (**analysed**) incident, (**situational) metrics**, good **practices**, **threat**, and **vulnerability**

Efforts to improve: cybersecurity, capability, consciousness

Alerta Temprana / Detección Proactiva

INTERCAMBIO DE INFORMACIÓN CON TERCERAS PARTES

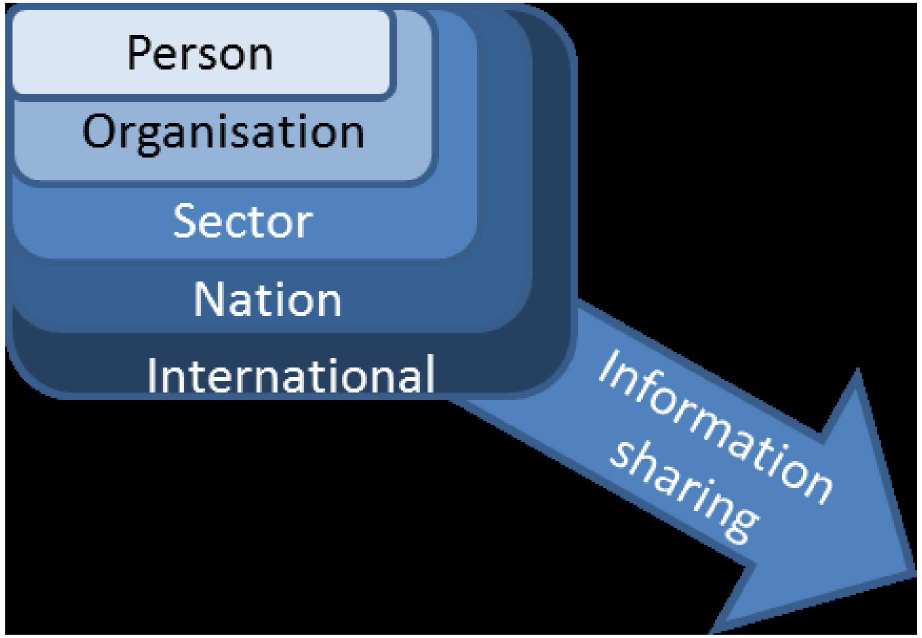

CERT.PT
shadowserver
Google
CERT POLSKA
cyscon
TREND MICRO
US-CERT UNITED STATES COMPUTER EMERGENCY READINESS TEAM
Microsoft
CERT Australia
ARBOR NETWORKS
SOPHOS
TEAM CYMRU
Panda Software
National Vulnerability Database a comprehensive cyber vulnerability resource
NIST National Institute of Standards and Technology
Symantec.
Información de incidentes
Fuentes de detección propias
Big Data
Notificación

STOP | THINK | CONNECT™

A global campaign to raise awareness and educate all people about how to stay safe and secure online.

www.stopthinkconnect.org

Future of sharing



- **Personal perspective: Motivation**
- **Organisational perspective:** ready and willing to trust interacting with your peers. relevant information in the right context is needed and the (Chief) Information Security Officers ((C)ISO)
- **Sector perspective:** be able to create a trusted common picture
- **National perspective**: providing the right conditions and incentives
- **International perspective**: Many private organisations and also some public agencies operate internationally