X.1500 - Cybersecurity Information Exchange Framework (CYBEX)

(draft-takahashi-cybex-intro-00.txt)

Takeshi Takahashi, Youki Kadobayashi

ITU-T Study Group 17 Question 4

(ITU-T Q.4/17)

Messages of this presentation

- We would like to support your SCAP activities in IETF
- Our works are strongly related though they are not overlapping
- We believe we can collaborate, complement each other, and enjoy synergies

On behalf of ITU-T Q.4/17, we would like to introduce CYBEX in this presentation

Contributors to X.1500 (CYBEX)*

Anthony Rutokowski
Rapporteur

YAANA TECHNOLOGIES
BRIDGING THE FUTURE !

Youki Kadobayashi
Associate Rapporteur

NiCT

S. Adegbite

FIRST Improving Security Together

I. Furey

M. Hird

Homeland Security

BIS

R. Martin

MITRE

A. McKay

Microsoft

D. Rajnovic

FIRST Improving Security Together

G. Reid

CISCO

G. Schudel

CISCO

T. Takahashi

NiCT

M. Terada

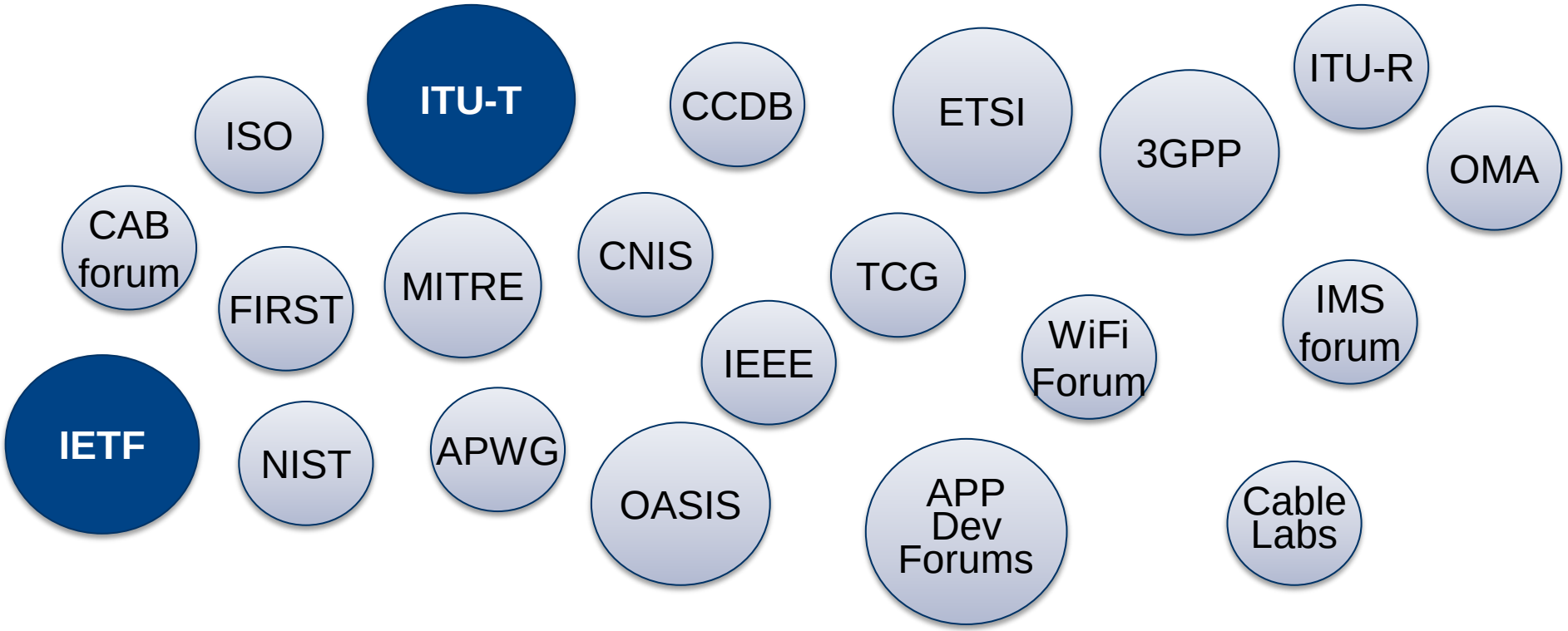
HITACHI
Inspire the Next

* Contributors include editors, but not limited to them

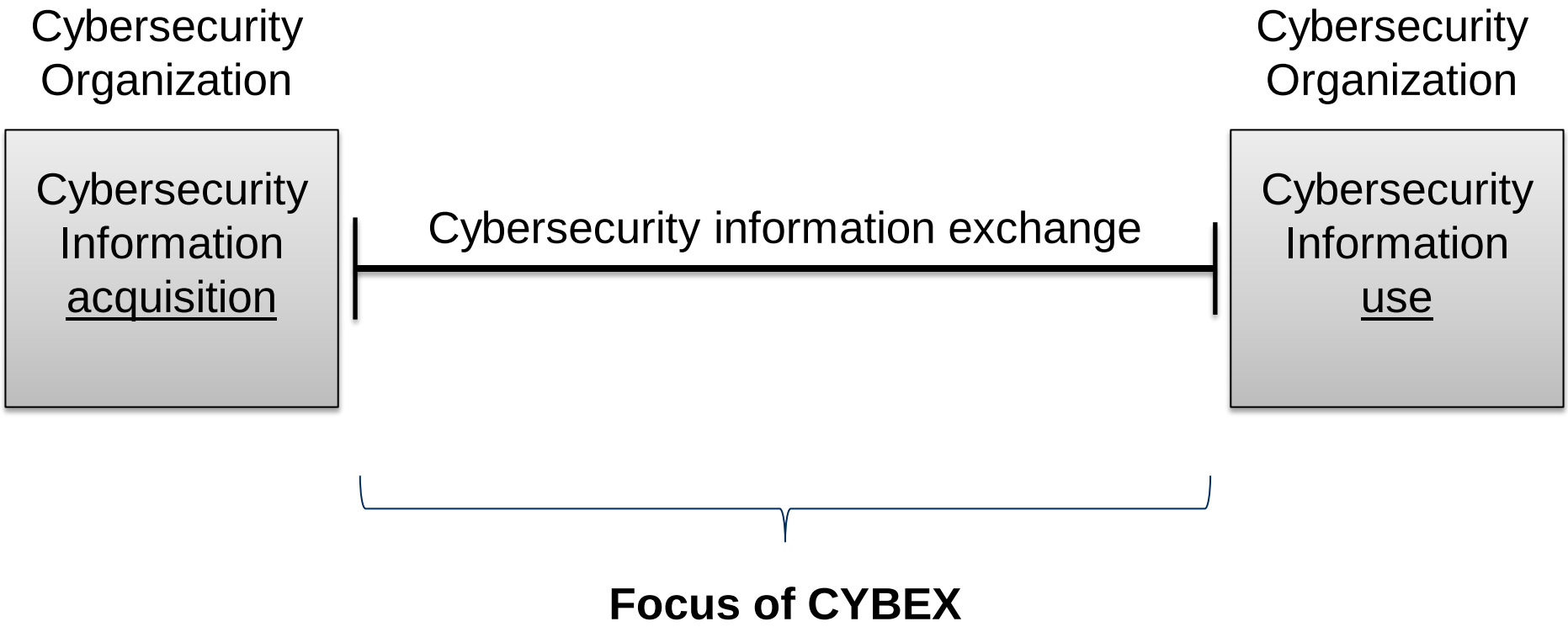
What is CYBEX?

- CYBEX is cybersecurity information exchange framework
- It structures cybersecurity information, and then, enables assured exchange of the information
- For that purpose it gathers all the professional works related to this and orchestrates them

We would like to provide outreach among standards bodies



ITU-T is building X.1500, which provides the cybersecurity information exchange framework, known as CYBEX



CYBEX consists of 5 functional blocks

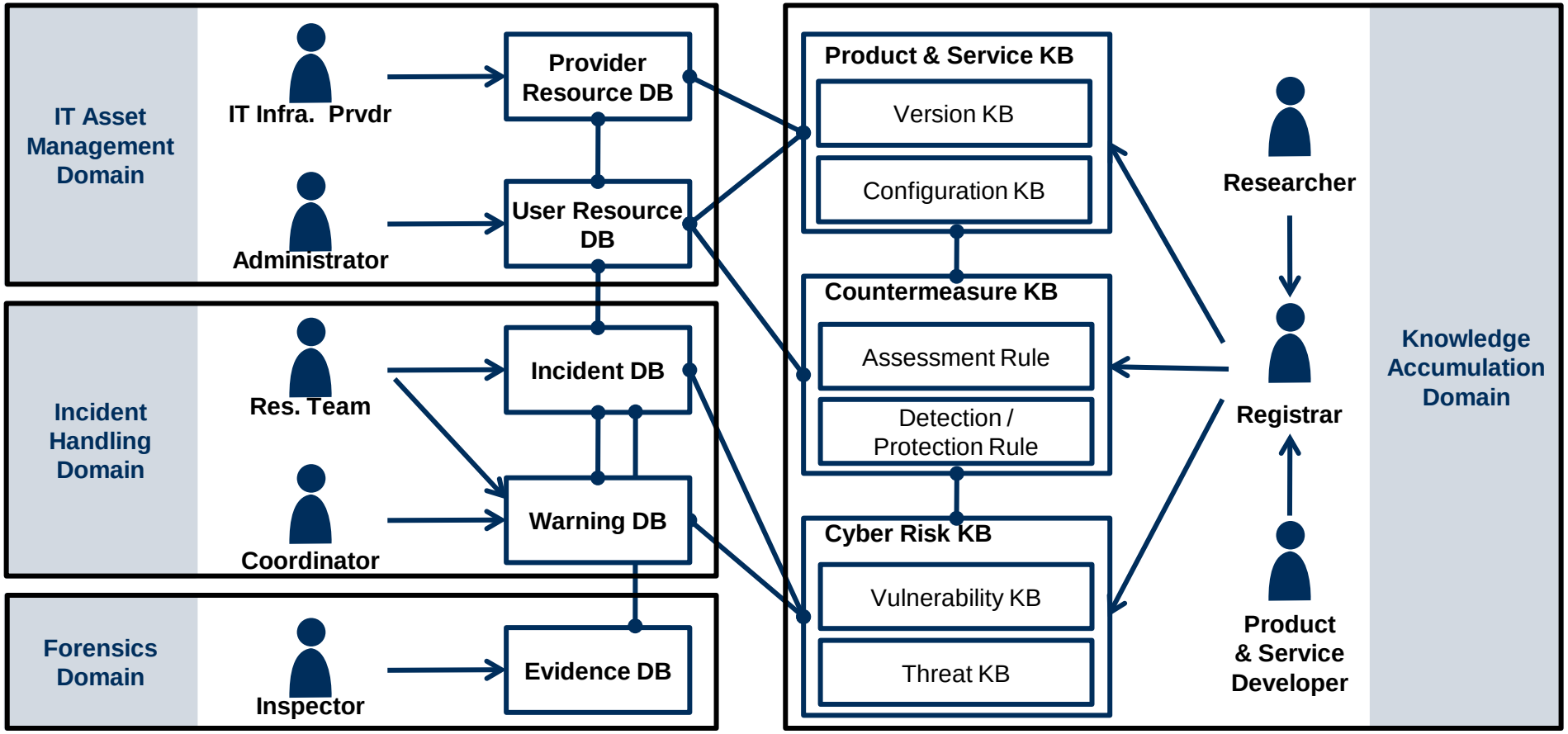
Five functional blocks of CYBEX

Focus of today's presentation

Information Description block	This block structures and describes cybersecurity information
Information Discovery block	This block identifies and discovers cybersecurity information and entities
Information Query block	This block requests and responds with cybersecurity information
Information Validation block	This block ensures the validity of the information
Information Transport block	This block exchanges cybersecurity information over networks

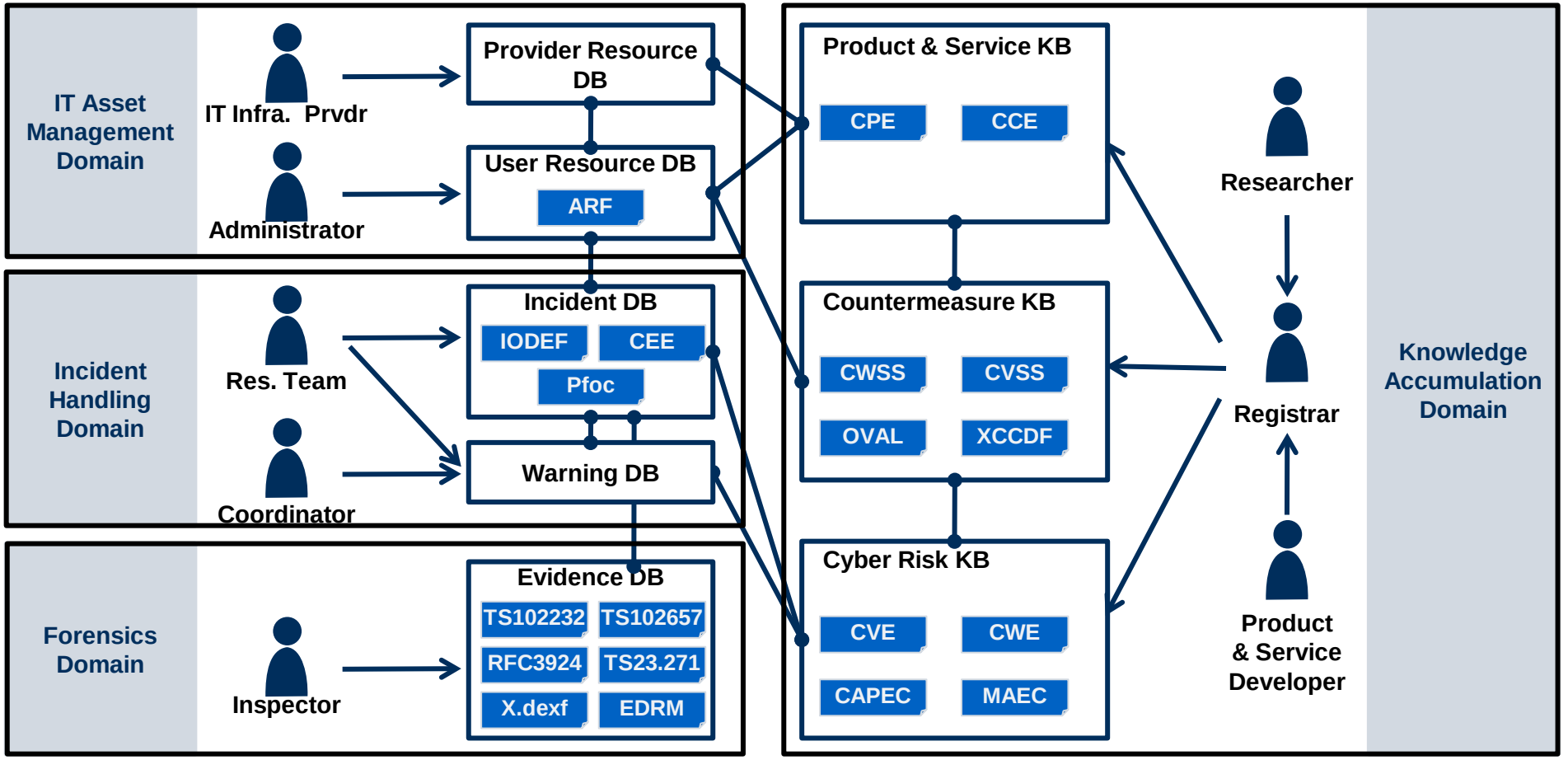
This block uses the cybersecurity ontology to identify what kind of information needs to be exchanged

Cybersecurity Operational Information Ontology

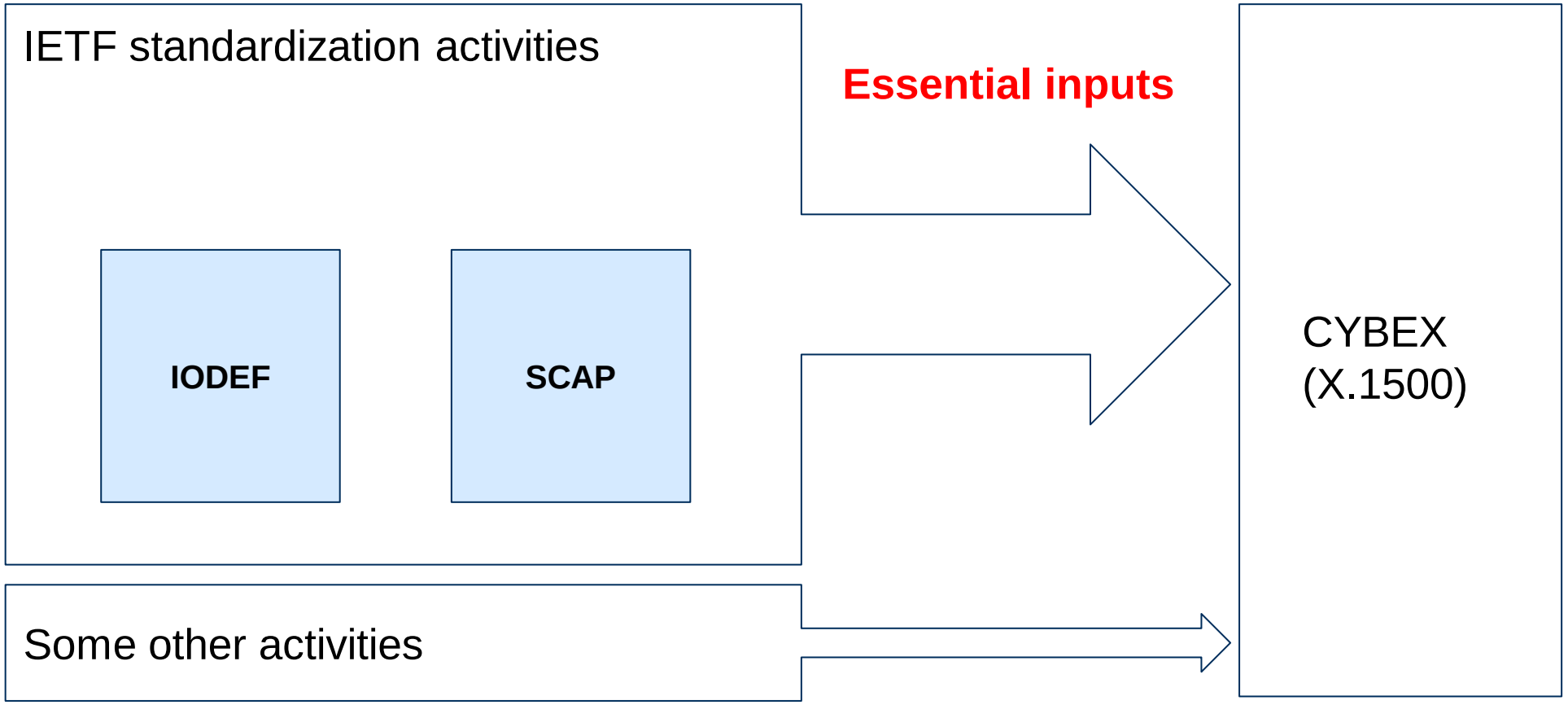


The ontology orchestrates specifications, with which various types of cybersecurity information can be described

Mapping of cybersecurity information standards



Standardization activities in IETF are essential for the purpose of enabling such functional blocks



Following the philosophy of CYBEX, we would like to utilize IETF standards

Summary text from draft Rec. ITU-T X.1500 (CYBEX)

- This Recommendation
  - describes a framework and general principles for coherent, comprehensive, global, timely and assured exchange of cybersecurity information, and
  - enables this exchange by
    - identifying and incorporating existing capability specifications implemented in various environments
    - as necessary, making the existing standards more global and interoperable
    - providing extensible means for adapting to new exchange requirements and capabilities.

We believe we share the same philosophy, and we would like to support your IETF activities

- Historically, IETF and ITU-T SG17 have established close collaborative relationship
- Important specifications such as PKIX (X.509), ASN.1 (X.680) were build based on the close collaboration
- We believe we share the same philosophy - building charge-free, practical and effective standard
- We believe SCAP is a key use case of the needed capabilities for the ICT security toolkit, and it is synergistic and interoperable with other components of the CYBEX ensemble

CYBEX is a substantive ongoing global Cyber/ICT security initiative

- CYBEX structures cybersecurity information, and then enables assured exchange of the information
- The CYBEX initiative aimed at identifying the emerging set of specifications for the global platforms for achieving these trusted exchanges
- Most of the work has been accomplished within existing systems assurance, incident response, and intelligence/surveillance communities
- Pro-active outreach is part of the initiative
  - Constant attempt to survey what is occurring in all other forums and bringing important capabilities into the framework
  - Constant analysis of what is missing or needed
- Unique – no comparable activity exists

Please refer to the following articles and tools for further information, or feel free to contact us

- cg-cybex : correspondence group regarding cybex. It holds telephone conferences bi-weekly. Subscription to the mailing list is warmly welcomed
- “Cybersecurity Information Exchange Framework”, draft-takahashi-cybex-intro-00.txt, IETF, Oct. 2010
- “CYBEX – the Cybersecurity Information Exchange Framework (X.1500),” ACM CCR technical note, http://ccr.sigcomm.org/drupal/?q=node/691, Oct. 2010
- Cybex Information Exchange Tool (cybiet) -- A Cybex Discovery and Cybex BEEP profile implementation, http://cybiet.sourceforge.net/

…etc.

Messages of this presentation

- We would like to support your SCAP activities in IETF
- Our works are strongly related though they are not overlapping
- We believe we can collaborate, complement each other, and enjoy synergies