

글로벌 ICT 표준 컨퍼런스 2023

Global ICT Standards Conference 2023

(세션5) 사이버보안: 신뢰성 있는 디지털 환경 구축

사이버보안 국제표준화 동향 및 주요이슈 (ITU-T Q4/17 중심)

김종현 책임, ETRI

주최



과학기술정보통신부
Ministry of Science and ICT



특허청
Korean Intellectual
Property Office

주관



국립전파연구원
National Radio Research Agency



ITP

KEA

kista

ETRI

Index

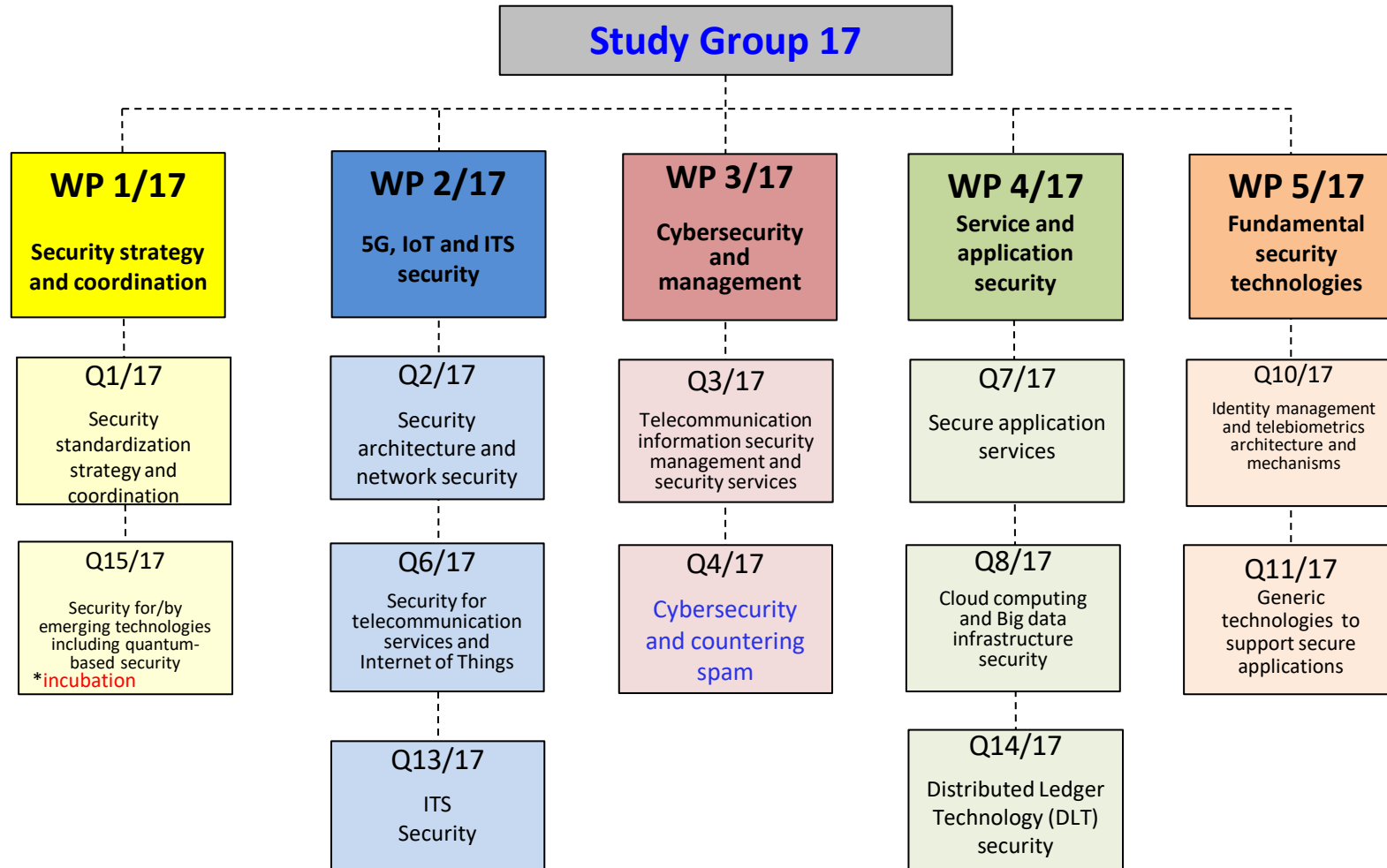
- 01 ITU-T SG17 소개 (역할 및 구조)
- 02 ITU-T SG17 표준화 동향 (Hot Topics)
- 03 Q4/17 소개 (연구주제 및 Work Items)
- 04 Q4/17 주요이슈 (Cybex, STIX/TAXII)

01. ITU-T SG17 소개 - Mission

SG17 – Mission

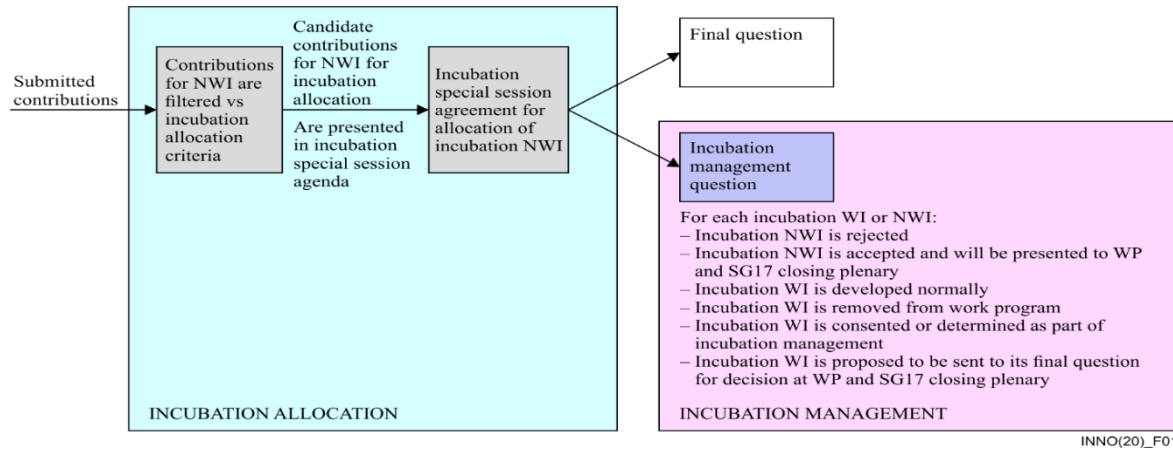
- **Building confidence and security in the use of information and communication technologies (ICTs) is one of the top priorities of the ITU (PP-Res. 130, WSIS Action Line C5).**
- New emerging technologies such as security for IMT-2020/5G and beyond, IoT, smart cities, DLT, big data analytics, ITS, security aspects related to artificial intelligence (AI) and quantum-related technologies, need technical, organizational, and physical measures to protect assets for the network, applications, and services.
- New security approaches to adequately address emerging security threats should be addressed.

01. ITU-T SG17 소개 - 구조



01. ITU-T SG17 소개 - 특별세션

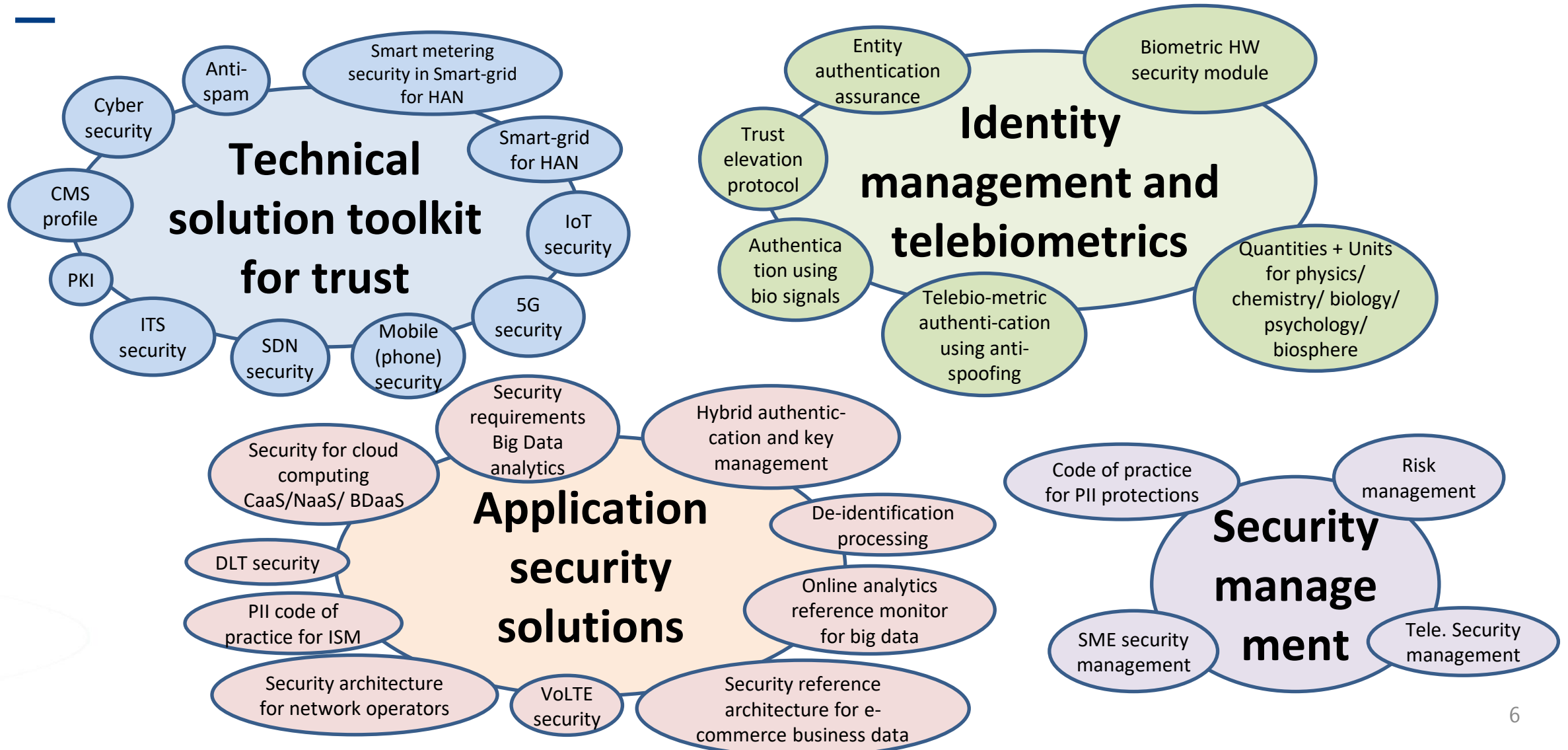
Incubation Mechanism



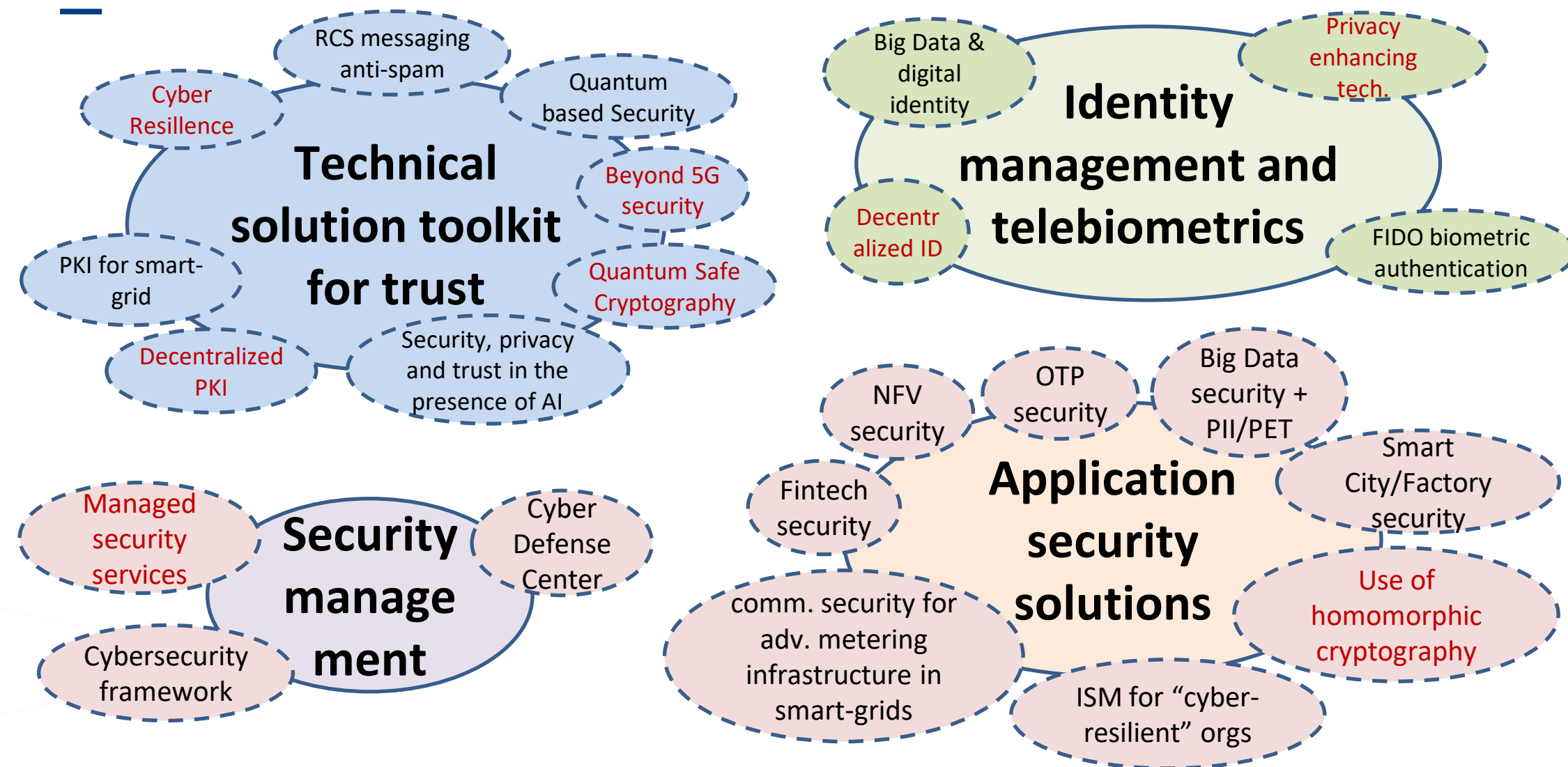
< General flow of the incubation mechanism in two parts: allocation and management >

#	CRITERIA	DESCRIPTION
C1	Innovation	The NWI is an innovation not covered by any Question
C2	Too many target Qs	The NWI lists multiple Questions
C3	Semantic mismatch	The meaning of the NWI doesn't match its target Question mandate
C4	SDO Dependency	A dependency (editorial, bidding) with the work of ITU-T SG17
C5	Semantic misalignment	A full semantic review makes the NWI eligible in multiple or no Question (because it is a Next Big Thing/Innovation)
C6	ITU mandate restriction	The NWI is an innovation that falls in a grey area vs ITU mandates

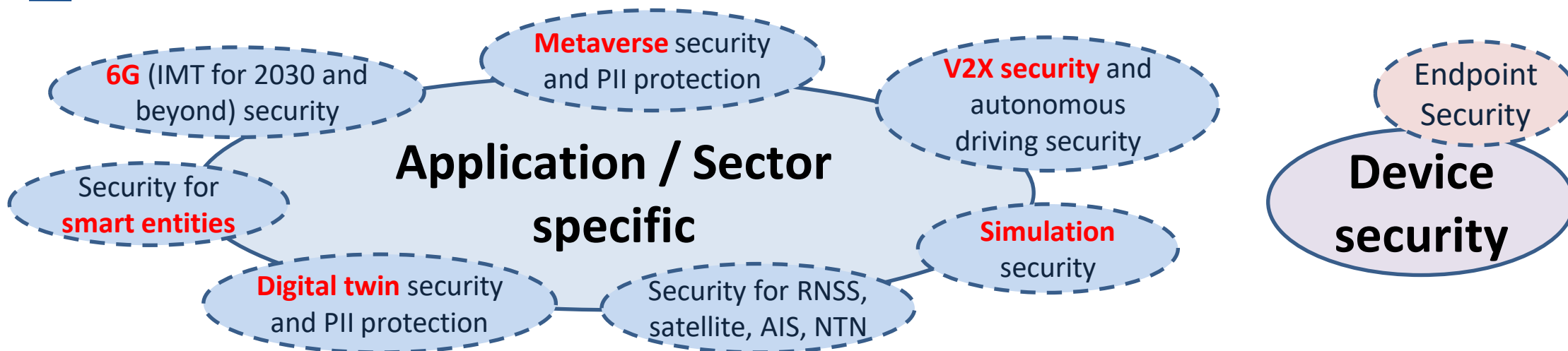
02. ITU-T SG17 표준화 동향 - Current Hot Topics



02. ITU-T SG17 표준화 동향 - Hot Topics under consideration

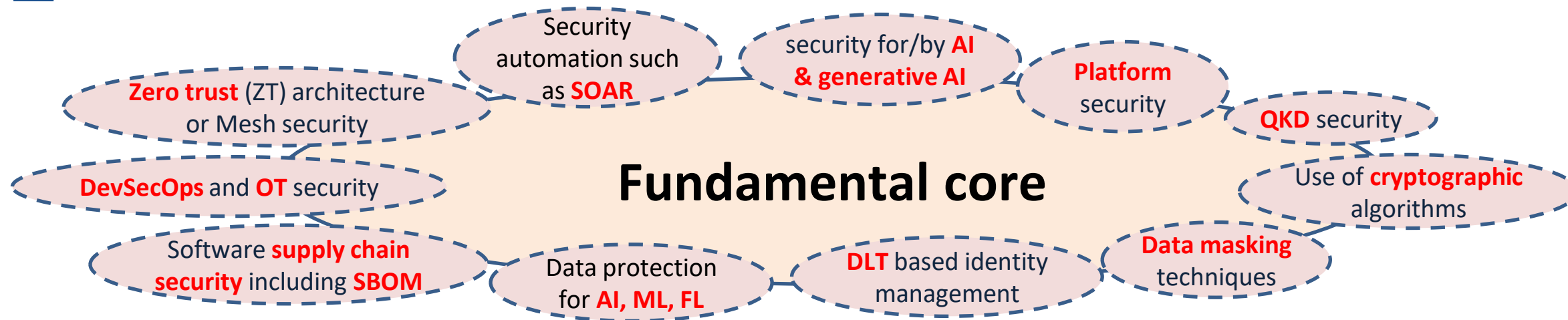


02. ITU-T SG17 표준화 동향 - Potential Hot Topics (1)



#	Potential topics	Source	Area	Impact on
ET #1	Metaverse (immersive virtual universe) security and PII protection	C233 , TD849	Application/Sector specific	Single Question
ET #2	Future network security such as 6G (IMT for 2030 and beyond) security	C233 , TD849	Application/Sector specific	Single Question
ET #3	Security for smart entities	C233 , TD849	Application/Sector specific	Single question
ET #4	Digital twin security and PII protection	C233 , TD849	Application/Sector specific	Multiple questions
ET #5	Simulation security	TD931	Application/Sector specific	Multiple questions
ET #6	Security for RNSS, satellite, AIS, NTN, including security for converged networks	TD1215R1	Application/Sector specific	Single question
ET #7	V2X security and autonomous driving security	TD1215R1	Application/Sector specific	Single question
ET #8	Endpoint Security (and Mobile Endpoint Security)	TD931	Device security	Single question

04. ITU-T SG17 표준화 동향 - Potential Hot Topics (2)

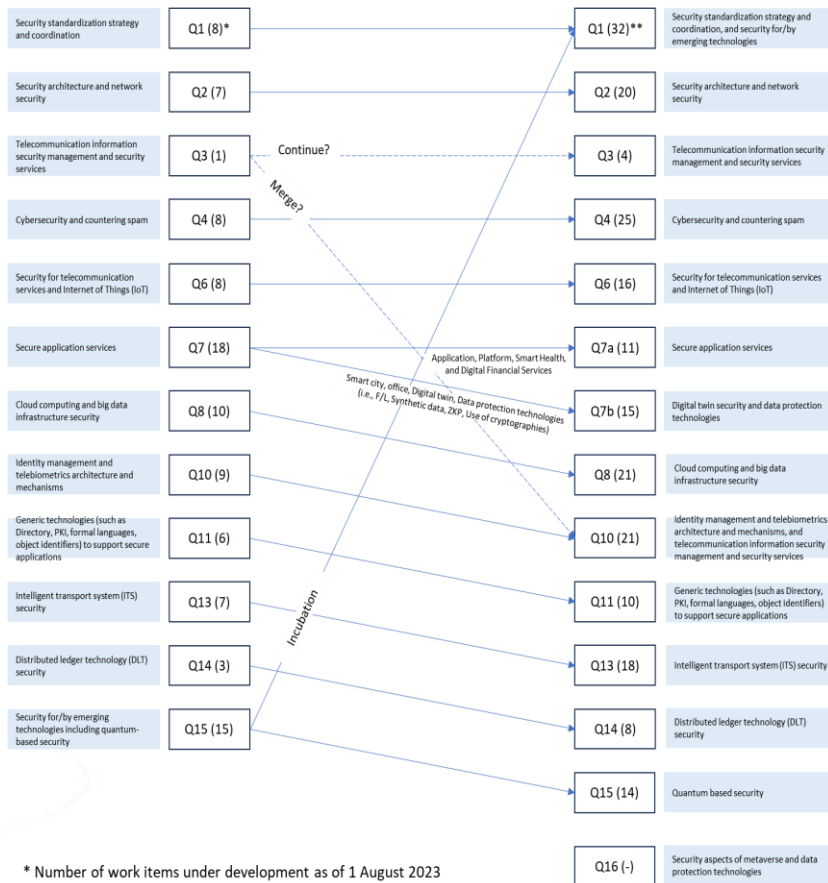


#	Potential topics	Source	Area	Impact on
ET #1	Software supply chain security including SBOM (Software Bill of Materials)	C233 , TD849	Fundamental core	Multiple Questions
ET #2	Intrinsic security such as DevSecOps (Development, Security and Operations) and OT security	C233 , TD849	Fundamental core	Multiple Questions
ET #3	Future security models such as Zero trust (ZT) architecture or Mesh	C233 , TD849	Fundamental core	Multiple Questions
ET #4	Security automation such as SOAR (Security Orchestration, Automation, and Response)	C233 , TD849	Fundamental core	Multiple Questions
ET #5	Operational aspects for data protection for AI, Machine Learning and Federated Learning (FL)	C233 , TD849	Fundamental core	Multiple Questions
ET #6	Use of cryptographic algorithms for data protection	C233 , TD849	Fundamental core	Multiple Questions
ET #7	Data masking techniques	C233 , TD849	Fundamental core	Multiple Questions
ET #8	DLT based identity management (DPKI)	C233 , TD849	Fundamental core	Multiple questions
ET #9	Platform security	TD931	Fundamental core	Multiple questions
ET #10	Security around AI (security for/by AI), Generative AI for security, security for generative AI	TD1215R1	Fundamental core	Multiple questions
ET #11	QKD security	TD1215R1	Fundamental core	Single question

02. ITU-T SG17 표준화 동향 - 연구반 구조 조정(안)

Proposal for Question structure of ITU-T SG17 for the next study period (2025-2028)

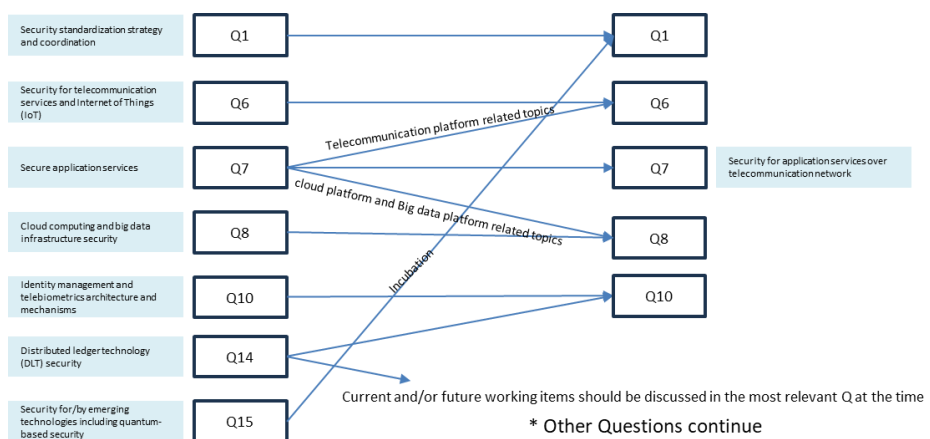
Korea's proposal for SG17 Question structure



* Number of work items under development as of 1 August 2023

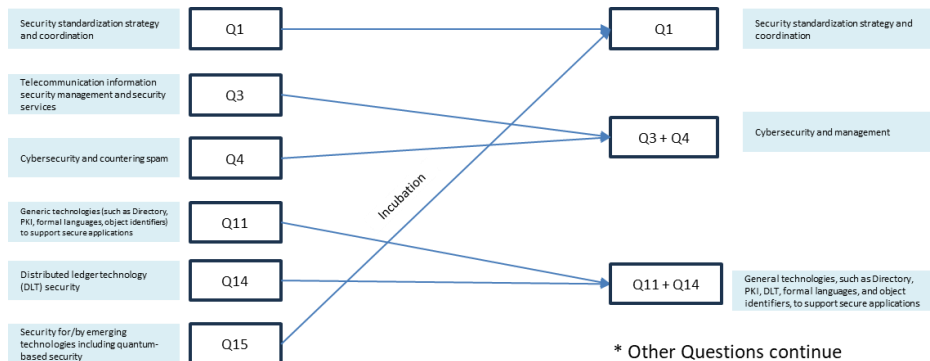
** Expected texts to be developed during next study (2025-2028)

Japan's proposal for SG17 Question structure



* Other Questions continue

Canada's proposal for SG17 Question structure



* Other Questions continue

03. Q4/17 소개 - Cybersecurity 정의

Definition of Cybersecurity (ref. Rec. ITU-T X.1205, Overview of cybersecurity)

Cybersecurity is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets.

Organization and user's assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment.

Cybersecurity strives to ensure the attainment and maintenance of the security properties of the organization and user's assets against relevant security risks in the cyber environment.

The general security objectives comprise the following:

- Availability
- Integrity, which may include authenticity and non-repudiation
- Confidentiality.

03. Q4/17 소개 - 연구주제 및 구성

Question 4/17 - Cybersecurity and countering spam

Q4/17 consists of two main parts:

- Cybersecurity
 - Lead group in ITU-T on cybersecurity in support of WTSA Resolution 50 (Cybersecurity)
 - In the last study period, developed 9 new and 3 revised Recommendations, 8 new Amendments, and 2 new and 1 revised Supplements.
- Countering spam
 - Lead group in ITU-T on countering spam by technical means in support of WTSA Resolution 52 (Countering and combating spam)
 - In the last study period, developed 2 new Recommendations (X.1246, X.1247), one Corrigendum (X.1243 Cor.1), and two new Supplements (X.Suppl.25, X.Suppl.28).
- Responsible for
 - X.1205, X.1206, X.1207, X.1208, X.1209, X.1210, X.1211, X.1212, X.1213, X.1214, X.1215, X.1216, X.1217, X.1218, X.1219, X.1231, X.1232, X.1233, X.1234, X.1235, X.1240, X.1241, X.1242, X.1243, X.1244, X.1245, X.1246, X.1247, X.1248, X.1249, X.1303, X.1303bis, X.1500, X.1500.1, X.1520, X.1521, X.1524, X.1525, X.1526, X.1528, X.1528.1, X.1528.2, X.1528.3, X.1528.4, X.1541, X.1542, X.1544, X.1546, X.1550, X.1570, X.1580, X.1581, X.1582; X.Suppl.6, X.Suppl.8, X.Suppl.9, X.Suppl.10, X.Suppl.11, X.Suppl.12, X.Suppl.14, X.Suppl.18, X.Suppl.20, X.Suppl.25, X.Suppl.28, X.Suppl.29, X.Suppl.33, X.Sup.37 and Technical Report TR.usm
- Rapporteurs: **Mr Jong Hyun KIM** and Mr Yanbin ZHANG

03. Q4/17 소개 - Current Work Items

Question 4/17 - Cybersecurity and countering spam

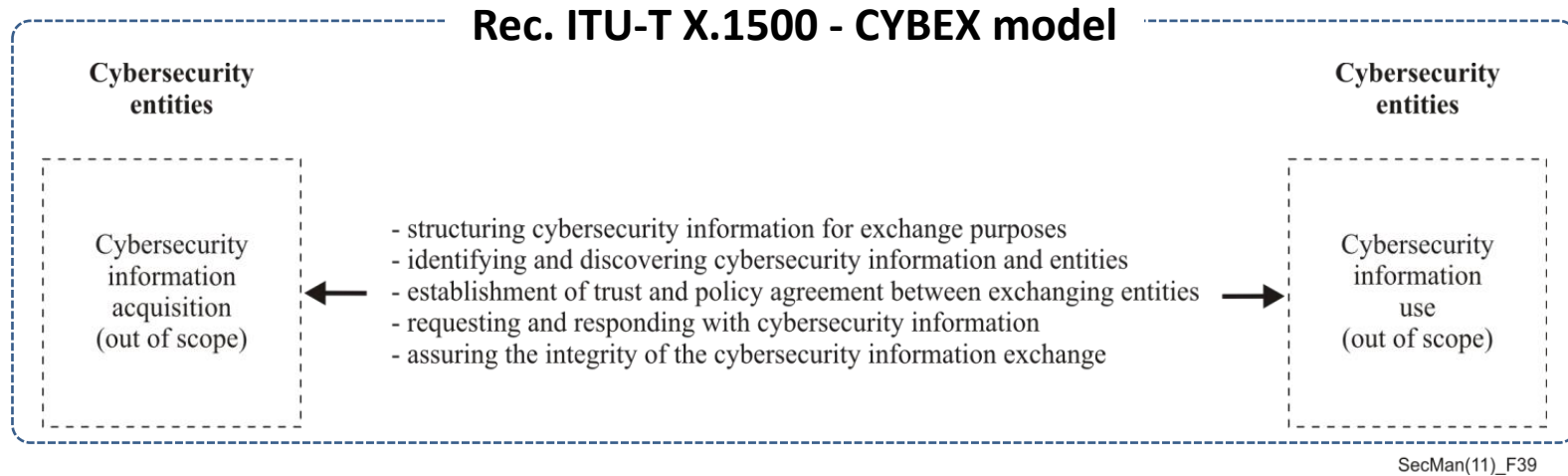
Recommendations currently under study :

- For Consent • **X.1220(X.spmoh)**, Security framework for storage protection against malware attacks on hosts
- For Consent • **X.1236(X.sr-ctea)**, Security requirements and countermeasures for targeted email attacks
- For TAP determination • **X.1221(X.stie)**, OASIS STIX Version 2.1
- For TAP determination • **X.1222(X.taeii)**, OASIS TAXII Version 2.1
- **X.tsfpp**, Technical security framework for the protection of users' personal information while countering mobile messaging spam
- **X.sgc_rcs**, Guidelines for countering spam over rich communication service (RCS) messaging
- **X.st-ssc**, Security threats of software supply chain
- **TR.verm**, Technical Report: Framework for Verification of Messages
- NWI at Sept. 2023 • **X.sf-dtea**, Security framework for detecting targeted email attacks

04. Q4/17 주요이슈 - Cybex

CYBERSECURITY INFORMATION EXCHANGE (CYBEX)

- Overview of cybersecurity information exchange ([Rec. ITU-T X.1500](#))



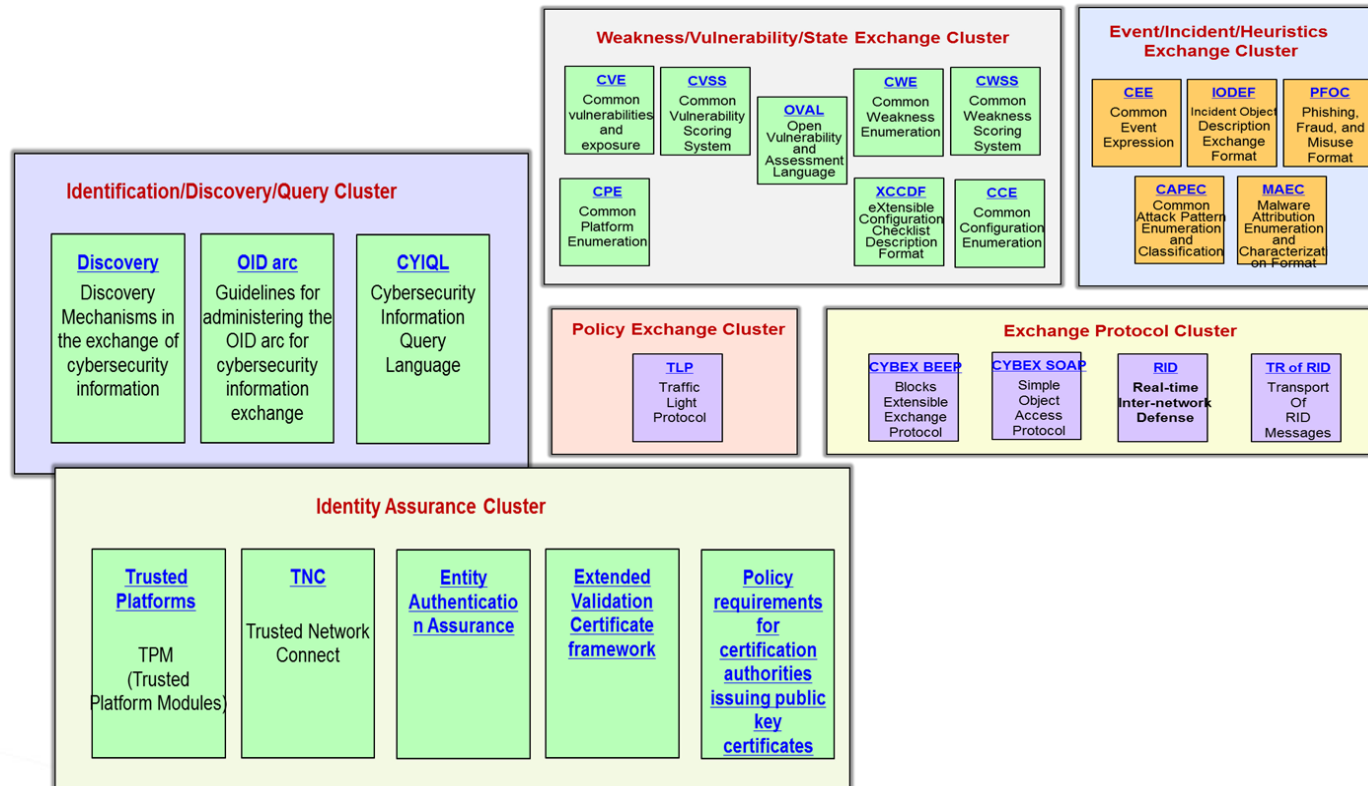
사이버 위협정보 공유 문제점

- 사이버 위협에 대한 표현 체계, 탐지 시스템, 공유 체계, 대응 체계 **불일치**
- 악성코드에 대한 표현 체계, 탐지 엔진, 탐지 결과, 공유 체계, 대응 체계 **불일치**
- 사이버 위협 정보 교환을 위한 표준 지표에 대한 표준화 **부재**

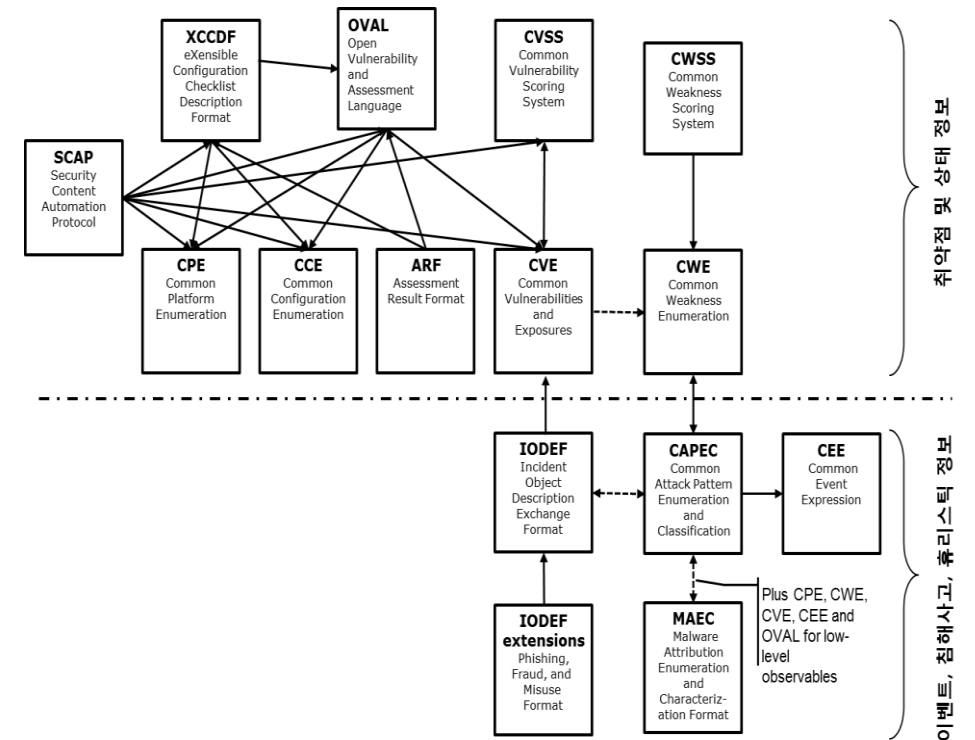


04. Q4/17 주요이슈 - Cybex

CYBERSECURITY INFORMATION EXCHANGE (CYBEX)



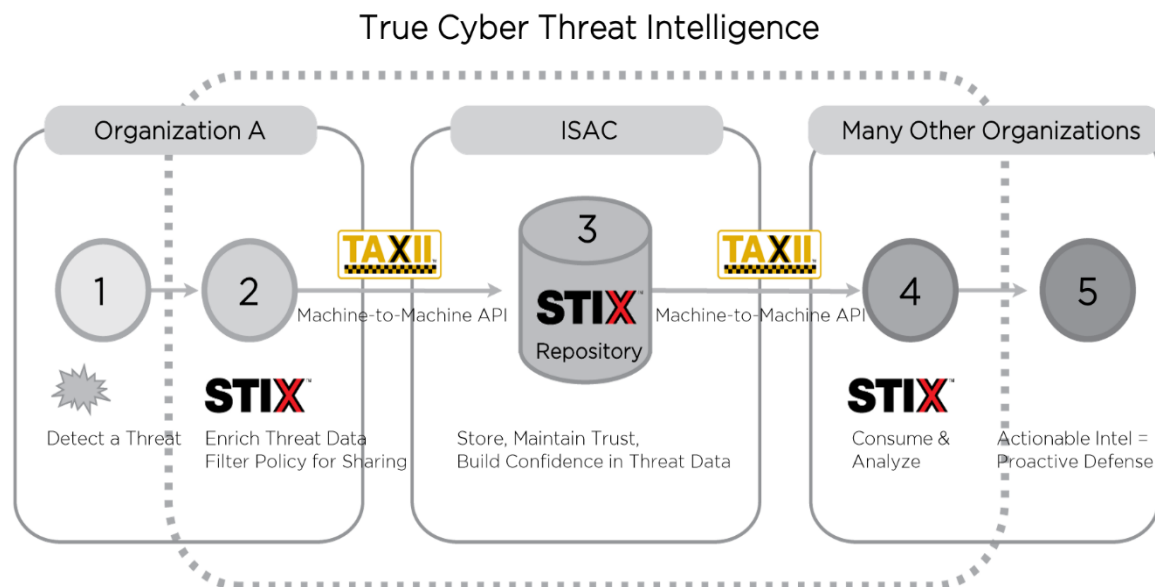
< CYBEX 6가지 분류 체계 구성도 >



< CYBEX 표준 관계도 >

04. Q4/17 주요이슈 - STIX/TAXII

OASIS STIX / TAXII



예시



















- ① A사 : 사이버위협을 탐지
- ② A사 : 위협정보를 STIX로 표현한 후 TAXII를 통해 중계기관으로 자동 전달
- ③ 중계기관(ISAC) : 수신정보를 저장, 진위여부를 파악 후 TAXII로 참여조직들에게 자동 전달
- ④ 참여조직 : 자사에 공유된 위협정보를 적용
- ⑤ 참여조직 : 위협요소 제거 및 사전예방 조치

OASIS STIX/TAXII 정의 및 개발현황

- **STIX(Structured Threat Information eXpression):**
위협정보를 기계가 읽을 수 있는 일관된 형식으로 표현
 - **TAXII(Trusted and Automated eXchange of Intelligence Information):**
STIX 객체를 송수신하는 HTTP Restful 프로토콜
-
- (2013년) 美 DHS(국토안보부)가 MITRE를 통해 STIX/TAXII 1.0 제정
 - (2015년) 비영리 국제표준단체 OASIS에서 STIX/TAXII 담당 및 개발
 - (2017년) STIX/TAXII 2.0 제정
 - ① CybOX(Cyber Observable eXpression) 통합
 - ② XML 언어의 복잡성과 상호운용성 해결을 위해 JSON으로 변경
 - (2021년) STIX/TAXII 2.1 제정
 - ① Opinion, Note, Language-Content, Location 등 신규 객체 추가
 - ② Confidence 개념 추가

04. Q4/17 주요이슈 - STIX/TAXII

STIX 2.1 defines 18 STIX Domain Objects (SDOs):

Object	Name	Description	Object	Name	Description
	Attack Pattern	A type of TTP that describe ways that adversaries attempt to compromise targets.		Malware	A type of TTP that represents malicious code.
	Campaign	A grouping of adversarial behaviors that describes a set of malicious activities or attacks (sometimes called waves) that occur over a period of time against a specific set of targets.		Malware Analysis	The metadata and results of a particular static or dynamic analysis performed on a malware instance or family.
	Course of Action	A recommendation from a producer of intelligence to a consumer on the actions that they might take in response to that intelligence.		Note	Conveys informative text to provide further context and/or to provide additional analysis not contained in the STIX Objects, Marking Definition objects, or Language Content objects which the Note relates to.
	Grouping	Explicitly asserts that the referenced STIX Objects have a shared context, unlike a STIX Bundle (which explicitly conveys no context).		Observed Data	Conveys information about cyber security related entities such as files, systems, and networks using the STIX Cyber-observable Objects (SCOs).
	Identity	Actual individuals, organizations, or groups (e.g., ACME, Inc.) as well as classes of individuals, organizations, systems or groups (e.g., the finance sector).		Opinion	An assessment of the correctness of the information in a STIX Object produced by a different entity.
	Indicator	Contains a pattern that can be used to detect suspicious or malicious cyber activity.		Report	Collections of threat intelligence focused on one or more topics, such as a description of a threat actor, malware, or attack technique, including context and related details.
	Infrastructure	Represents a type of TTP and describes any systems, software services and any associated physical or virtual resources intended to support some purpose (e.g., C2 servers used as part of an attack, device or server that are part of defence, database servers targeted by an attack, etc.).		Threat Actor	Actual individuals, groups, or organizations believed to be operating with malicious intent.
	Intrusion Set	A grouped set of adversarial behaviors and resources with common properties that is believed to be orchestrated by a single organization.		Tool	Legitimate software that can be used by threat actors to perform attacks.
	Location	Represents a geographic location.		Vulnerability	A mistake in software that can be directly used by a hacker to gain access to a system or network.

Ref: <https://oasis-open.github.io/cti-documentation/stix/intro>

04. Q4/17 주요이슈 - 논의쟁점

OASIS STIX / TAXII

Draft Recommendations for TAP Determination

Q	Acronym	Title	New / Revised	Editor(s)	Location of Text	A.5 or A.25 justification	Equivalent e.g., ISO/IEC
4/17	X.1221 (X.stie)	Structured threat information expression	New	Michael ROSA, Duncan SPARRELL	TD1261	TD808	OASIS STIX Version 2.1
4/17	X.1222 (X.taeii)	Trusted automated exchange of intelligence information	New	Michael ROSA, Duncan SPARRELL	TD1262	TD808	OASIS TAXII Version 2.1

Based on Report of Working Party 3/17 (Goyang, 29 August - 8 September 2023)

- WP3 was unable to reach consensus on TAP determination of the two draft Recommendations, X.taeii and X.stie with the following discussion:
- At the Q4/17 meeting, The Russian Federation considers that the document needs serious revision and cannot be decided in its present form.
- At the WP3 meeting, **Russian Federation expressed opposition to the TAP determination** of these draft Recommendations. The reason is that, as verbally expressed in previous SG17 meetings, **terms such as Military, Threat intelligence, Spy, etc. are used in the draft Recommendations**, and the use of these terms is not in line with the ITU-T Recommendations, and they should be removed from the Recommendations.
- In WP3, mainly the **U.S., U.K., and Canada expressed the opinions that these draft Recommendations should proceed to TAP Determination**. Specifically,
 - 1) The conditions for transition to the TAP stipulated in Resolution 1 were satisfied in the deliberation of these draft Recommendations, and the method of proceeding with the deliberation was in accordance with rule in Resolution 1,
 - 2) Although Russian Federation provided verbal explanations, **no specific comments were submitted in the form of written contributions, and there were no contributions and no participations from Russian Federation.**
 - 3) As for the terms such as military, threat intelligence, etc., which are of concern to the Russian Federation, **there is no problem with their use in these draft Recommendations** and other existing Recommendations (X.1060, X.1382...) on the subject of cyber security. From the perspective of effective use of these draft Recommendations, these terms should not be easily deleted because of the need to maintain consistency with other equivalent standards (STIX, TAXII). Furthermore, from a technical perspective, there is nothing wrong with the use of these terms noted, since the purpose of these Recommendations is to protect against cyber attacks.



감사합니다.

김종현 책임, ETRI
jhk@etri.re.kr