ETSI TR 103 331 V1.1.1 (2016-08)

CYBER;
Structured threat information sharing

Reference

DTR/CYBER-0009

Keywords

security, threat analysis, threat intelligence

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Important notice

The present document can be downloaded from:
http://www.etsi.org/standards-search

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the only prevailing document is the print of the Portable Document Format (PDF) version kept on a specific network drive within ETSI Secretariat.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at
https://portal.etsi.org/TB/ETSIDeliverableStatus.aspx

If you find errors in the present document, please send your comment to one of the following services:
https://portal.etsi.org/People/CommiteeSupportStaff.aspx

Copyright Notification

Contents

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (https://ipr.etsi.org/).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Some material contained herein is the copyright of, or has been supplied by OASIS and the United States Government.

Foreword

This Technical Report (TR) has been produced by ETSI Technical Committee Cyber Security (CYBER).

Modal verbs terminology

In the present document "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

Executive summary

Cyber threat information sharing - often described as threat intelligence sharing - is one of the most important components of an organization's cyber security program. It can be obtained internally and from external trusted sources. It is collected, analysed, shared, and leveraged. The present document provides a survey of ongoing activities and the resulting platforms that are aimed at structuring and exchanging cyber threat information. These activities range from those developed among the Computer Emergency Response Teams in the 1990s in the IETF, to cutting-edge new initiatives being advanced in OASIS. Some of the platforms are semi-open commercial product communities. It is possible that the OASIS CTI work could bring about significant interoperability if not integration in this area.

Introduction

The importance of cyber threat information sharing has been underscored recently by the European Union and North America enacting into organic law, combined with major executive level and national initiatives. These actions extend across all information, and infrastructure sectors. Some of the more prominent of these recent actions include:

- EU Network Information Security Directive, approved 18 December 2015 [i.1].
- Cybersecurity Information Sharing Act of 2015 (18 December 2015) [i.2].
- CPNI, Threat Intelligence: Collecting, Analysing, Evaluating, 23 March 2015 [i.3].
- Launch of the Canadian Cyber Threat Exchange, 11 December 2015.

Against this backdrop of initiatives that included the scaling of Financial Services Information Sharing and Analysis Center (FS-ISAC) and The Depository Trust & Clearing Corporation (DTCC) activities, the OASIS Cyber Threat Intelligence Technical Committee was formed in 2015 to bring together a broad and rapidly growing array of public and private sector organizations to advance a global set of standards for structured threat information sharing.

The present document describes the known array of existing structured threat information sharing work in diverse bodies, including the developments underway in OASIS TC CYBER which can form the basis for expanded cooperation based on existing ETSI and OASIS collaborative agreements and working relationships among Technical Committees.

1 Scope

The present document provides an overview on the means for describing and exchanging cyber threat information in a standardized and structured manner. Such information includes technical indicators of adversary activity, contextual information, exploitation targets, and courses of action. The existence and creation of organizations for the exchange of this information are out of scope the present document.

2 References

2.1 Normative references

Normative references are not applicable in the present document.

2.2 Informative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

[i.1] Directive of the European Parliament and of the Council concerning measures with a view to achieving for a high common level of security of network and information security systems across the Union, Brussels, 21 April 2016 (5581/16).

[i.2] Guidance to Assist Non-Federal Entities to Share Cyber Threat Indicators and Defensive Measures with Federal Entities under the Cybersecurity Information Sharing Act of 2015 (June 2016).

NOTE: Available at https://www.us-cert.gov/sites/default/files/ais_files/Non-Federal_Entity_Sharing_Guidance_%28Sec%20105%28a%29%29.pdf.

[i.3] Center for the Protection of National Infrastructure (CPNI): "Threat Intelligence: Collecting, Analysing, Evaluating".

NOTE: Available at https://www.cpni.gov.uk/Documents/Publications/2015/23-March-2015-MWR_Threat_Intelligence_whitepaper-2015.pdf.

[i.4] OASIS Specifications, STIX 1.2.1, TAXII 1.1.1, CybOX 2.1.1; draft Specifications STIX 2.0, TAXII 2.0, CybOX 3.0; draft CybOX 3.0 Roadmap, CybOX 3.0 Visualization.

NOTE 1: Available at https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=cti.

NOTE 2: See also, OASIS Cyber Threat Intelligence (CTI) TC Wiki, https://wiki.oasis-open.org/cti/; Sean Barnum, Standardizing Cyber Threat Intelligence Information with the Structured Threat Information eXpression (STIX™), MITRE (February 20, 2014).

[i.5] OASIS. Cyber Threat Intelligence (CTI) TC Meeting Notes, OASIS Cyber Threat Intelligence (CTI) TC Documents.

NOTE: Available at https://www.oasis-open.org/apps/org/workgroup/cti/documents.php?folder_id=2978.

[i.6] Internet Engineering Task Force (IETF): "Managed Incident Lightweight Exchange (mile) Working Group".

NOTE: Available at https://datatracker.ietf.org/wg/mile/documents/.

[i.7] Recommendation ITU-T X.1500-Series: "Cybersecurity information exchange".

NOTE: Available at https://www.itu.int/itu-t/recommendations/index.aspx?ser=X.

[i.8] ETSI ISG ISI (Information Security Indicators) initial Terms of Reference.

NOTE: Available at https://portal.etsi.org/ISI/ISI_ISG_ToR_Sep2011.pdf.

[i.9] ETSI GS ISI 001-1: "Information Security Indicators (ISI); Indicators (INC); Part 1: A full set of operational indicators for organizations to use to benchmark their security posture".

[i.10] ETSI GS ISI 001-2: "Information Security Indicators (ISI); Indicators (INC); Part 2: Guide to select operational indicators based on the full set given in part 1".

[i.11] ETSI GS ISI 002: "Information Security Indicators (ISI); Event Model A security event classification model and taxonomy".

[i.12] ETSI GS ISI 003: "Information Security Indicators (ISI); Key Performance Security Indicators (KPSI) to evaluate the maturity of security event detection".

[i.13] ETSI GS ISI 004: "Information Security Indicators (ISI); Guidelines for event detection implementation".

[i.14] ETSI GS ISI 005: "Information Security Indicators (ISI); Guidelines for security event detection testing and assessment of detection effectiveness".

[i.15] IETF RFC 5070: "The Incident Object Description Exchange Format".

[i.16] IETF RFC 6545: "Real-time Inter-network Defense (RID)".

[i.17] IETF RFC 6546: "Transport of Real-time Inter-network Defense (RID) Messagesover HTTP/TLS".

[i.18] IETF RFC 6684: "Guidelines and Template for Defining Extensions to the Incident Object Description Exchange Format (IODEF)".

[i.19] IETF RFC 6685: "Expert Review for Incident Object Description Exchange Format (IODEF) Extensions in IANA XML Registry".

[i.20] IETF RFC 7203: "An Incident Object Description Exchange Format (IODEF) Extension for Structured Cybersecurity Information".

[i.21] IETF RFC 7495: "Enumeration Reference Format for the Incident Object Description Exchange Format (IODEF)".

[i.22] IETF RFC 6046: "Transport of Real-time Inter-network Defense (RID) Messages".

[i.23] draft-ietf-mile-implementreport-09: "MILE Implementation Report".

[i.24] draft-ietf-mile-iodef-guidance-06: "IODEF Usage Guidance".

[i.25] draft-ietf-mile-rfc5070-bis-25: "The Incident Object Description Exchange Format v2".

[i.26] draft-ietf-mile-rolie-03: "Resource-Oriented Lightweight Information Exchange".

[i.27] draft-ietf-mile-xmpp-grid-00: "XMPP Protocol Extensions for Use with IODEF".

[i.28] ISO/IEC 27001: "Information technology -- Security techniques -- Information security management systems -- Requirements".

[i.29] ISO/IEC 27002: "Information technology -- Security techniques -- Code of practice for information security controls".

[i.30] ISO/IEC 27004: "Information technology -- Security techniques -- Information security management -- Measurement".

[i.31] ETSI TR 103 305: "CYBER; Critical Security Controls for Effective Cyber Defence".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the following terms and definitions apply. Reference figure 2, below.

campaign: STIX Campaign represents a set of TTPs, Incidents, or Threat Actors that together express a common intent or desired effect [i.4]

course of action: STIX Course of Action (COA) is used to convey information about courses of action that may be taken either in response to an attack or as a preventative measure prior to an attack [i.4]

exploit target: STIX Exploit Target conveys information about a vulnerability, weakness, or misconfiguration in software, systems, networks, or configurations that may be targeted for exploitation by an adversary [i.4]

incident: STIX Incident corresponds to sets of related security events affecting an organization, along with information discovered or decided during an incident response investigation [i.4]

indicators: STIX Indicator data model conveys specific Observable patterns combined with contextual information intended to represent artifacts and/or behaviors of interest within a cyber security contex [i.4]

observables: STIX Observable represents stateful properties or measurable events pertinent to the operation of computers and networks, and may consist of Observable instances and Observable Patterns [i.4]

observable instances: represent actual specific observations that took place in the cyber domain [i.4]

observable patterns: represent conditions for a potential observation that may occur in the future or may have already occurred and exists in a body of observable instances [i.4]

report: STIX Report defines a contextual wrapper for a grouping of STIX content, which could include content specified using any of the other eight top-level constructs, or even other related Reports [i.4]

Tactics, Techniques and Procedures (TTP): STIX Tactics, Techniques, and Procedures (TTP) are used to represent the behavior or modus operandi of cyber adversaries [i.4]

threat actor: STIX Threat Actor is a characterization of malicious actor (or adversary) representing a cyber attack threat including presumed intent and historically observed behavior [i.4]

3.2 Abbreviations

For the purposes of the present document, the following abbreviations apply:

ACDC	Advanced Cyber Defence Centre
AS	Autonomous System
CERT	Computer Emergency Response Team
CIF	Collection Intelligence Framework
COBIT	Control OBjectives for Information and related Technology
CPNI	Centre for the Protection of National Infrastructure
CSIRT	Computer Security Incidence Response Team
CTI	Cyber Threat Intelligence
CYBEX	Cybersecurity Information Exchange
CybOX™	Cyber Observable Expression
DHS	Department of Homeland Security
DoS	Denial of Service
DTCC	Depository Trust & Clearing Corporation
ENISA	European Union Agency for Network and Information Security
EU	European Union
FIRST	Forum of Incident Response and Security Teams
FS-ISAC	Financial Services ISAC
GS	Group Specification
HTTP	Hypertext Transfer Protocol

IANA	Internet Assigned Numbers Authority
IDS	Identification Detection System
IETF	Internet Engineering Task Force
INC	INdiCators
INCH	INCident Handling
IODEF	Incident Object Description Exchange Format
IP	Internet Protocol
ISAC	Information Sharing and Analysis Center
ISACA	Information Systems Audit and Control Association
ISG	Industry Specification Group
ISI	Information Security Indicators
IT	Information Technology
ITU-T	International Telecommunication Union Telecommunication Standardization
JSON	JavaScript Object Notation
KPSI	Key Performance Security Indicators
MAEC™	Malware attribute enumeration and characterization
MILE	Managed Incident Lightweight Exchange
NIS	Network and Information Security
NREN	National Research and Education Network
OASIS	Organization for the Advancement of Structured Information Standards
OMG	Object Management Group
OSSIM	Open Source Security Information Management
OTX	Open Threat eXchange
RID	Real-time Inter-network Defense
STIX™	Structured Threat Information Expression
TAXII™	Trusted Automated Exchange of Indicator Information
TTP	Tactics, Techniques and Procedures
US	United States
VERIS	Vocabulary for Event Recording and Incident Sharing
XML	Extensible Markup Language
XMPP	Extensible Messaging and Presence Protocol

NOTE: CybOX™, MAEC™, STIX™ and TAXII™ are trademarks of The MITRE Corporation operating as a non-profit Federally Funded Research and Development Center (FFRDC) of the U.S. Department of Homeland Security. See http://stixproject.github.io/legal/. This information is given for the convenience of users of the present document and does not constitute an endorsement by ETSI of the product named. Equivalent products may be used if they can be shown to lead to the same results.

4 Means for exchanging structured cyber threat intelligence

4.1 Introduction

The need for the exchange of structured cyber threat intelligence grew in the 1990s in conjunction with increasing numbers of discovered exploits of network vulnerabilities and attacks. This led to a diverse array of initiatives and projects to develop structured expressions and associated protocols for the trusted exchange of information concerning those vulnerabilities and attacks, and remediation steps - which are described in the following clauses. These efforts and the resulting platforms have moved forward (or not) at significantly different scales, and involve specialized and sometimes vendor-oriented communities. The Financial Services Information Sharing and Analysis Center (FS-ISAC) and The Depository Trust & Clearing Corporation (DTCC) communities are especially significant and one of the EU NIS essential services sectors. The largest related standards activity - now consists of OASIS Technical Committee on Cyber Threat Intelligence (TC CTI) - and is still rapidly growing and evolving.

4.2 OASIS Cyber Threat Intelligence Technical Committee (TC CTI)

4.2.1 Introduction

The OASIS Cyber Threat Intelligence (CTI) TC was chartered to define a set of information representations and protocols to address the need to model, analyze, and share cyber threat intelligence. In the initial phase of TC work, three specifications were transitioned from the US Department of Homeland Security (DHS) for development and standardization under the OASIS open standards process: STIX^{TM} (Structured Threat Information Expression), TAXII^{TM} (Trusted Automated Exchange of Indicator Information), and CybOX^{TM} (Cyber Observable Expression). The OASIS CTI Technical Committee remit includes:

- define composable information sharing services for peer-to-peer, hub-and-spoke, and source subscriber threat intelligence sharing models;
- develop standardized representations for campaigns, threat actors, incidents, tactics techniques and procedures (TTPs), indicators, exploit targets, observables, and courses of action;
- develop formal models that allow organizations to develop their own standards-based sharing architectures to meet specific needs.

TC CTI consists of a significant number of companies, government agencies, and institutes from around the world. New OASIS versions of the three initial platforms (STIX^{TM}, TAXII^{TM}, and CybOX™) were produced and next generation versions being produced. Rather considerable material including running code is hosted on multiple design GitHubs. (https://github.com/STIXProject, https://github.com/TAXIIProject, https://github.com/CybOXProject, https://github.com/MAECProject/. It is expected that MAEC™ will be conflated into the TAXII^{TM}. As of June 2016, the deliverables consist of:

- STIX™ 1.2.1 Specification, August 2016.
- STIX™ 2.0 Specification [target Q1 2017].
- TAXII™ 1.1.1 Specification, August 2016.
- TAXII™ 2.0 Specification [target Q1 2017].
- CybOX™ 2.1.1 Specification, [September 2016].
- CybOX™ 3.0 Specification [target Q1 2017].
- CybOX™ 3.0 Roadmap.
- CybOX™ 3.0 Visualisation.
- Interoperability Guidelines.
- Interoperability Demonstration Policy.

The platforms have significant potential use within Network Functions Virtualization environments. The degree of activity and importance of this work merits more detailed treatment of the principal CTI subcommittees and their work. It presently has four active subcommittees dedicated to specific deliverables that are described below. There is an additional Marketing Group within the TC as well as several informal ad hoc "mini working groups".

4.2.2 CTI STIX Subcommittee

The objective of the Structured Threat Information Expression (STIX™) effort is to specify, characterize, and capture cyber threat information. STIX addresses a full range of cyber threat use cases - including threat analysis, capture and specification of indicators, management of response activities, and information sharing - to improve consistency, efficiency, interoperability, and overall situational awareness.

The four active work products include STIX V1.2.1 language specifications, XML binding specification for STIX V1.2.1, STIX and v2.0 language specifications, including the STIX 1.2.1 JSON Binding Specification 1.0 [i.4]. The STIX use cases are depicted in figure 1, the intelligence model and expression groups in figure 2 and examples in figure 3.

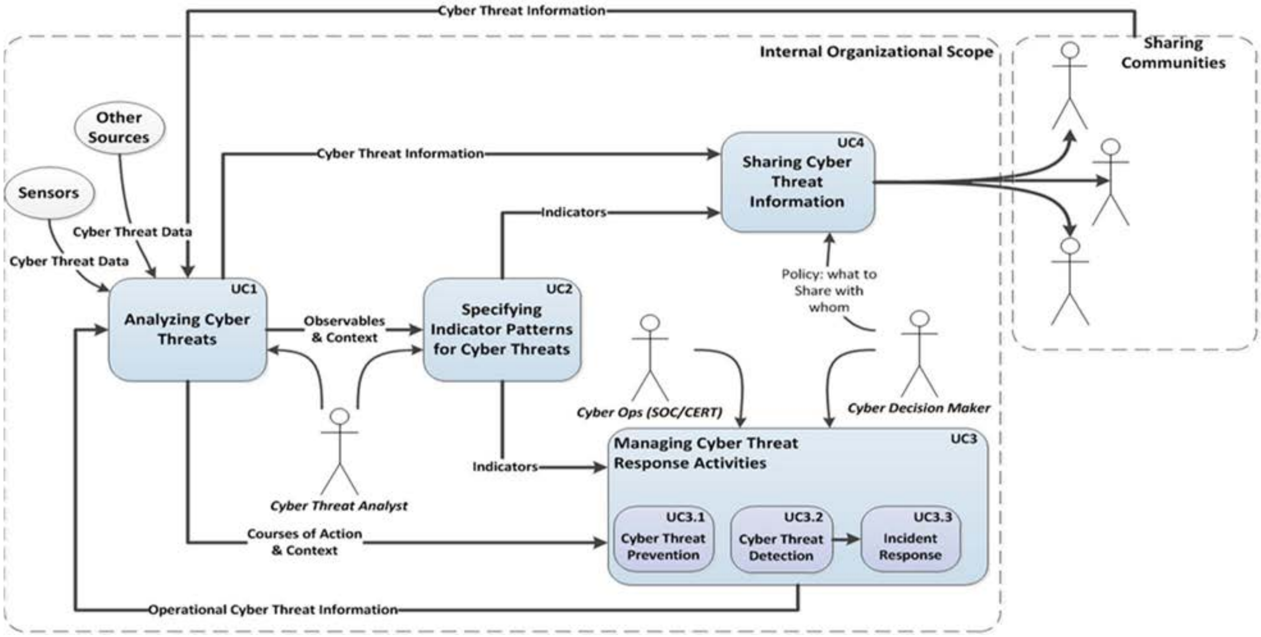


Figure 1: STIX use cases [i.4]

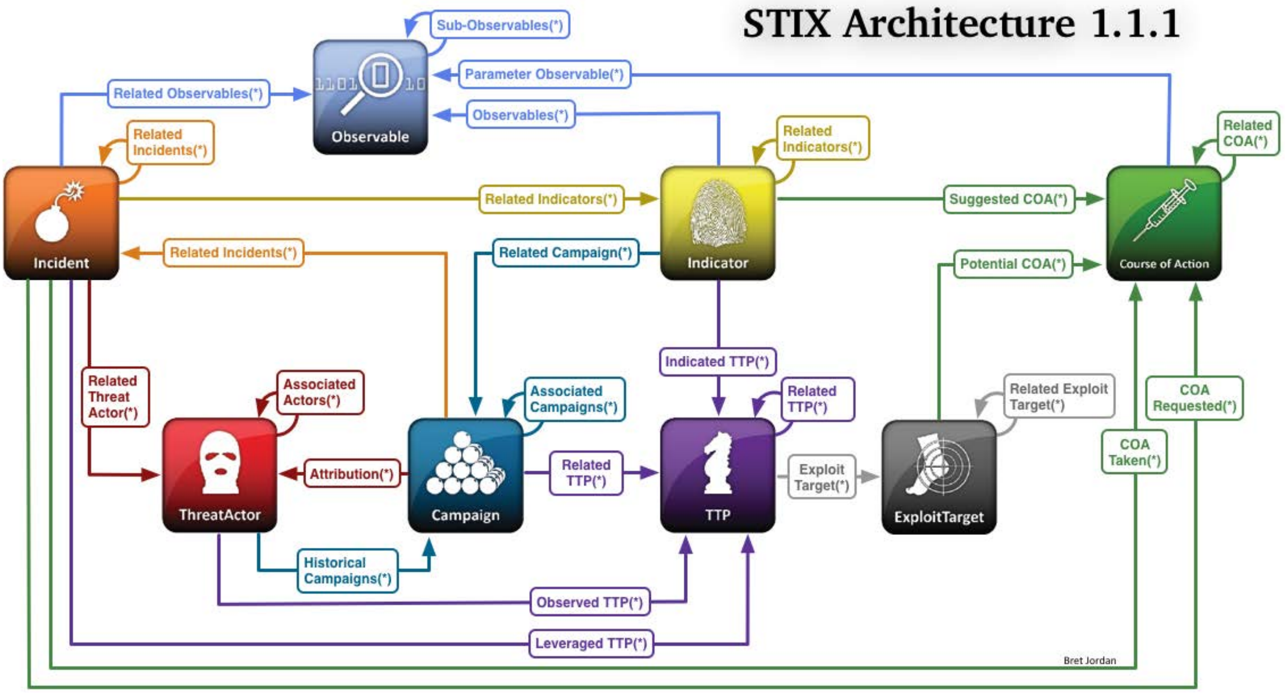


Figure 2: STIX Package encompasses the STIX individual component data models [i.4]

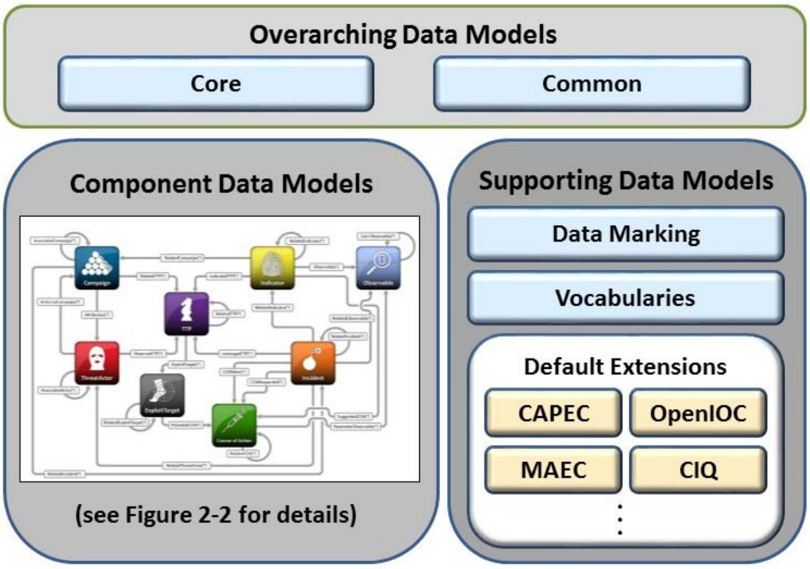
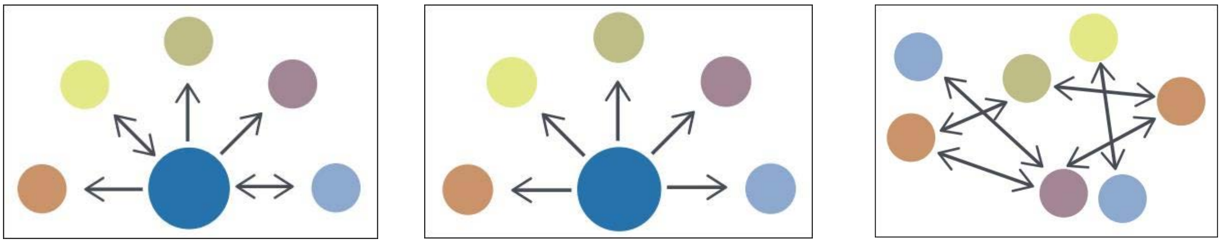


Figure 3: STIX architecture [i.4]

STIX 2.0 features being considered include JSON expressions, Sightings/Observation/Indicator, Versioning, Indicator Type Vocabulary, Common Object Properties, Packaging, Campaign, TTPs [i.5].

4.2.3 CTI TAXII Subcommittee

Trusted Automated eXchange of Indicator Information (TAXII™) defines a set of services and message exchanges that, when implemented, sharing of actionable cyber threat information across organization and product/service boundaries. TAXII, through its member specifications, defines concepts, protocols and messages to exchange cyber threat information for the detection, prevention, and mitigation of cyber threats. The models supported by V1.1.1 as well as the specification components are shown in figures 4 and 5.



Hub and Spoke **Source/ Subscriber** **Peer to Peer**

Figure 4: TAXII models supported [i.4]

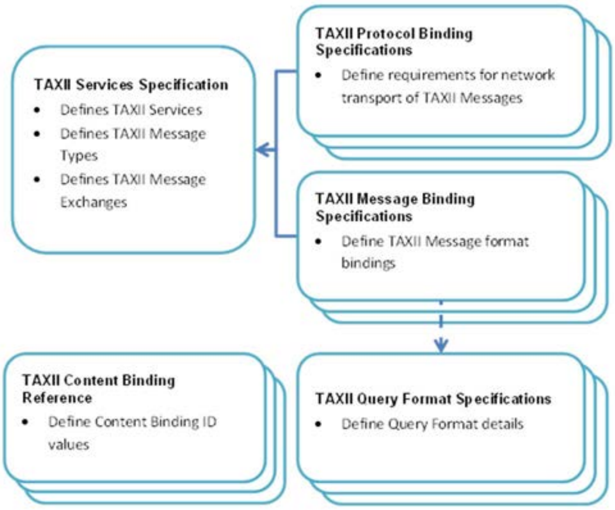

TAXII Services Specification
Defines TAXII Services
Defines TAXII Message Types
Defines TAXII Message Exchanges
TAXII Protocol Binding Specifications
Define requirements for network transport of TAXII Messages
TAXII Message Binding Specifications
Define TAXII Message format bindings
TAXII Content Binding Reference
Define Content Binding ID values
TAXII Query Format Specifications
Define Query Format details

Figure 5: TAXII specification components [i.4]

TAXII 2.0 features being considered include: Publish and Subscribe model over an HTTP RESTful interface; TAXII Servers are plumbing for CTI between TAXII Clients; each TAXII Server has some defined out-of-the box channels that clients can publish or subscribe. The model is depicted in figure 6.

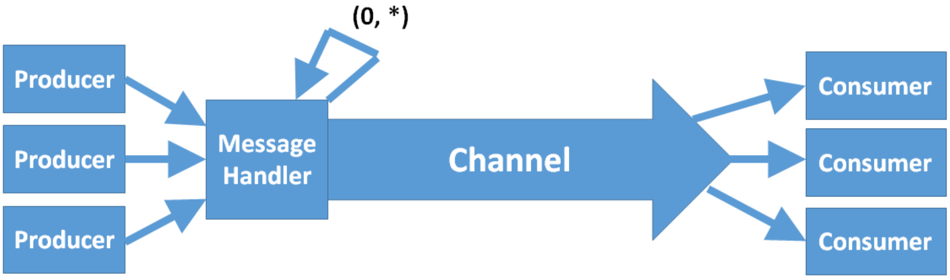


Figure 6: TAXII 2.0 proposed channel architecture [i.5]

4.2.4 CTI CybOX™ Subcommittee

CybOX™ provides a common structure for representing cyber observables across and among the operational areas of enterprise cyber security that improves the consistency, efficiency, and interoperability of deployed tools and processes, as well as increases overall situational awareness by enabling the potential for detailed automatable sharing, mapping, detection, and analysis heuristics. The CybOX™ V2.1.1 objects and relationships are depicted in figure 7.

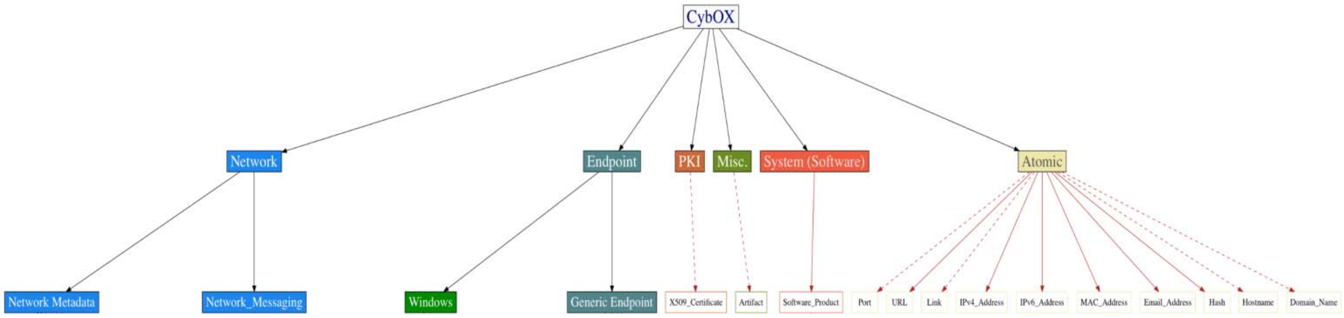


Figure 7: CybOX™ 2.1.1 objects and relationships [i.4]

CybOX™ 3.0 features being considered include: High-level Change to create: 1)a Core/Common set (Separation of Patterns and Instances, First-class Relationships, Cryptographic Hash Capture Refactoring) and 2) Object-related Changes Object Refactoring for Semantic Accuracy, Expansion of "Atomic" Objects) [i.5].

4.2.5 CTI Interoperability Subcommittee

The subcommittee helps guide adherence to CTI TC-promulgated standards and interoperability between CTI TC standards-based implementations, while encouraging standards maturity throughout the industry. It also develops parameters and processes to allow CTI TC members to test/ validate, and where possible measure the maturity of another organization's implementation. It identifies opportunities and approaches to promoting interoperability with externally-defined cyber threat intelligence standards and frameworks [i.5].

Its deliverables include guidelines, parameters and processes for testing, validating and measuring implementations' adherence to CTI standards, as well as proposals for promoting interoperability with other, externally-defined cyber threat intelligence standards and frameworks.

4.3 IETF Managed Incident Lightweight Exchange Working Group (mile)

In the 1990s, the various network Computer Emergency Response Teams under the leadership of the Carnegie Mellon CERT, FIRST, SurfNet Netherlands, and similar organizations focussed on the need to structure threat information for exchanging among themselves. Circa 2006 an IETF working group known as INCH (Extended Incident Handling) was established for the purposes of developing specifications. It developed a number of guideline Internet Drafts for an incident description language, transport protocols, and other capabilities that were advanced under the name The Incident Object Description Exchange Format or IODEF. IODEF was also replicated by ITU-T.

In 2011, in response to an increasing need for updates and extensions to IODEF and related new tools, the Managed Incident Lightweight Exchange Working Group (mile) was chartered and has been active since. The working group develops standards to support computer and network security incident management. It describes its role as:

> "*The Managed Incident Lightweight Exchange (MILE) working group develops standards to support computer and network security incident management; an incident is an unplanned event that occurs in an information technology (IT) infrastructure. An incident could be a benign configuration issue, IT incident, a system compromise, socially engineered phishing attack, or a denial-of-service (DoS) attack, etc. When an incident is detected, or suspected, there may be a need for organizations to collaborate. This collaboration effort may take several forms including joint analysis, information dissemination, and/or a coordinated operational response. Examples of the response may include filing a report, notifying the source of the incident, requesting that a third party resolve/mitigate the incident, sharing select indicators of compromise, or requesting that the source be located. By sharing indicators of compromise associated with an incident or possible threat, the information becomes a proactive defense for others that may include mitigation options" [i.6].*

Platforms approved within IETF include the following [i.6]:

- IETF RFC 5070 [i.15]: "Incident Object Description Exchange Format (IODEF)".
- IETF RFC 6545 [i.16]: "Real-time Inter-network Defense (RID)".
- IETF RFC 6546 [i.17]: "Transport of Real-time Inter-network Defense (RID) Messages over HTTP/TLS".
- IETF RFC 6684 [i.18]: "Guidelines and Template for Defining Extensions to IODEF".
- IETF RFC 6685 [i.19]: "Expert Review for Incident Object Description Exchange Format (IODEF) Extensions in IANA XML Registry".
- IETF RFC 7203 [i.20]: "IODEF-extension for structured cybersecurity information".
- IETF RFC 7495 [i.21]: "IODEF Enumeration Reference Format".

The ITU-T Study Group 17 replicated IETF RFC 6046 [i.22] (RID) as Recommendation ITU-T X.1581 and IETF RFC 6046 [i.22] (RID) as Recommendation ITU-T X.1581 [i.7].

Current new platforms being developed by the IETF mile group include the following [i.6]:

- MILE Implementation Report, draft-ietf-mile-implementreport-09 [i.23].
- IODEF Usage Guidance, draft-ietf-mile-iodef-guidance-06 [i.24].

- The Incident Object Description Exchange Format v2, draft-ietf-mile-rfc5070-bis-25 [i.25].
- Resource-Oriented Lightweight Indicator Exchange, draft-ietf-mile-rolie-03 [i.26].
- XMPP Protocol Extensions for Use with IODEF, draft-ietf-mile-xmpp-grid-00 [i.27].

The Implementation Report is useful in understanding the extent to which the IODEF platform has been used.

4.4 CSIRTGadgets Collective Intelligence Foundation (CIF)

The CSIRT Gadgets Foundation was founded with a mission to directly engage both public and private sector CSIRTs as a means for evolving the internet into a more secure and resilient ecosystem. The Foundation has been organized as a non-profit organization in the United States. The Foundation promotes the development and stewardship of assets such as software, algorithms and best common practices that enable CSIRTs execute their missions. One of its existing initiatives is known as the Collective Intelligence Framework funded by the U.S. National Science Foundation for use and development among the university educational community.

CIF allows to combine known malicious threat information from many sources and use that information for identification (incident response), detection (IDS) and mitigation (null route). The most common types of threat intelligence warehoused in CIF are IP addresses, domains and URLs that are observed to be related to malicious activity. CIF is used by the Research and Education Networking Information Sharing and Analysis Center (REN-ISAC) and the Anti-Phishing Working Group. A Foundation information site is available at http://csirtgadgets.org/.

4.5 EU Advanced Cyber Defence Centre (ACDC)

On an even larger scale than the CIF project described in clause 4.4, the European Commission helped initiate and fund the Advanced Cyber Defence Centre project from early 2013 to mid-2015. The objective was to establish a sustainable European centre for cyber defence, building on 8 networked support centres and one clearing house deployed during the project and enlarging the cyber-protection scope beyond botnets. ACDC unites a community of 28 organizations from 14 countries, including Internet Service Providers, CERTs, law enforcement agencies, IT providers, National Research and Education Networks (NRENs), academia and critical infrastructure operators.

In the initial phase of the projects, there was an active threat information sharing specifications group that made use of existing platforms via a Tool Group. The project ended in July 2015, but Delft University of Technology maintains an information site at http://www.tbm.tudelft.nl/en/research/projects/research-review/advanced-cyber-defense-center-acdc/.

4.6 AbuseHelper

AbuseHelper is an open-source project initiated by CERT.FI and CERT.EE with Clarified Networks to automatically process incidents notifications. Its use has been encouraged by ENISA as a modular, potentially scalable and robust framework to help in abuse handling. With Abuse Helper one can retrieve Internet Abuse Handling related information via several sources, one can then aggregate that information based on different keys, such as numbers or country codes and send out reports in different formats, via different transports and using different timings. An instructive site is available at www.abusehelper.be.

4.7 OMG Threat Modelling Working Group

The Object Management Group has several initiatives related to the sharing of cyber threat information. The most prominent is a proposal for a combined risk-threat information model that incorporates STIX (among other things). It is expected to cover a broader scope (cyber and physical, threat and risk) in order to coordinate across these domains but does not seek to re-define a model within the domain to the low level that STIX and CybOX™. A cross domain Threat and Risk Community site that builds on OASIS CTI platforms exists at www.threatrisk.org.

4.8 ITU-T SG17

The Cybersecurity Rapporteur group within ITU-T Study Group 17 began in 2009 to develop a comprehensive initiative to identify and in some cases replicate structured cybersecurity information sharing platforms. The general framework was designated CYBEX (Cybersecurity Information Exchange) and an extensive series of specifications have been prepared [i.7]:

- X.1500: "Overview of cybersecurity information exchange".
- X.1500.1: "Procedures for the registration of arcs under the object identifier arc for cybersecurity information exchange".
- X.1520: "Common vulnerabilities and exposures".
- X.1521: "Common vulnerability scoring system".
- X.1524: "Common weakness enumeration".
- X.1525: "Common weakness scoring system".
- X.1526: "Language for the open definition of vulnerabilities and for the assessment of a system state".
- X.1528: "Common platform enumeration".
- X.1528.1: "Common platform enumeration naming".
- X.1528.2: "Common platform enumeration name matching".
- X.1528.3: "Common platform enumeration dictionary".
- X.1528.4: "Common platform enumeration applicability language".
- X.1541: "Incident object description exchange format".
- X.1544: "Common attack pattern enumeration and classification".
- X.1546: "Malware attribute enumeration and characterization".
- X.1570: "Discovery mechanisms in the exchange of cybersecurity information".
- X.1580: "Real-time inter-network defence".
- X.1581: "Transport of real-time inter-network defence messages".
- X.1582: "Transport protocols supporting cybersecurity information exchange".

Current new threat information exchange platforms being developed by the ITU-T Cybersecurity group include the following [i.7]:

- X.1542: "Session information message exchange format".
- X.cogent, Design considerations for improved end-user perception of trustworthiness indicators.
- X.metric, Metrics for evaluating threat and resilience in cyberspace.
- X.nessa, Access control models for incidents exchange networks.

4.9 Open Threat Exchange™ (OTX™)

AlienVault is the developer of the Open Source Security Information Management (OSSIM). Its vision is for companies and government agencies to gather and share relevant, timely, and accurate information about new or ongoing cyberattacks and threats as quickly as possible to avoid major breaches (or minimize the damage from an attack). AlienVault's Open Threat Exchange™ (OTX) is its principle platform.

NOTE: Open Threat Exchange™ is the trade name of a product supplied by AlienVault. This information is given for the convenience of users of the present document and does not constitute an endorsement by ETSI of the product named. Equivalent products may be used if they can be shown to lead to the same results."

AlienVault OTX™ provides open access to a global community of threat researchers and security professionals. It delivers community-generated threat data, enables collaborative research, and automates the process of updating a security infrastructure with threat data from any source. OTX enables anyone in the security community to actively discuss, research, validate, and share the latest threat data, trends, and techniques, strengthening defences while helping others do the same.

4.10 OpenIOC Framework

The OpenIOC framework is an information exchange specification that describes Indicators of Compromise and is managed by an open developer community. OpenIOC addresses a narrow use case (observable patterns for Indicators of Compromise) and represents a partial solution to part of the overall cyber threat information problem, but does not fully address the needs of a holistic cyber threat intelligence information model. The OpenIOC community site is available at www.openioc.org.

4.11 VERIS Framework

Another common language for describing security incidents is the Vocabulary for Event Recording and Incident Sharing (VERIS). It addresses a narrow use case and represents a partial solution to part of the overall cyber threat information problem but does not fully address the needs of a holistic cyber threat intelligence information model. The VERIS community site is available at www.veriscommunity.net. In addition, the published format is available on GitHub at https://github.com/vz-risk/veris.

4.12 ETSI ISI (Information Security Indicators) ISG

In 2011, an Industry Specification Group was created by ETSI to undertake several activities relating to Information Security Indicators, including a Security Event Classification Model and its implementation [i.8]. Preliminary work on information security indicators was done by the French Club R2GS. The first public set of the ISI standards (security indicators list and event model) were released in April 2013 and now includes a set of five specifications:

- ETSI GS ISI 001-1 [i.9]: "Information Security Indicators (ISI); Indicators (INC); Part 1: A full set of operational indicators for organizations to use to benchmark their security posture".
- ETSI GS ISI 001-2 [i.10]: "Information Security Indicators (ISI); Indicators (INC); Part 2: Guide to select operational indicators based on the full set given in part 1".
- ETSI GS ISI 002 [i.11]: "Information Security Indicators (ISI); Event Model A security event classification model and taxonomy".
- ETSI GS ISI 003 [i.12]: "Information Security Indicators (ISI); Key Performance Security Indicators (KPSI) to evaluate the maturity of security event detection".
- ETSI GS ISI 004 [i.13]: "Information Security Indicators (ISI); Guidelines for event detection implementation".
- ETSI GS ISI 005 [i.14]: "Information Security Indicators (ISI); Guidelines for security event detection testing and assessment of detection effectiveness".

Although the term Information Security Indicator is not defined, an "indicator" is defined as a "measure that provides an estimate or evaluation of specified attributes derived from an analytical model with respect to a defined information need". These indicators provide the basis to switch from a qualitative to a quantitative culture in IT Security Scope of measurements: External and internal threats (attempt and success), user's deviant behaviours, nonconformities and/or vulnerabilities (software, configuration, behavioural, general security framework). ISO/IEC 27001 [i.28], ISO/IEC 27002 [i.29] and ISO/IEC 27004 [i.30], plus ISACA COBIT and the Critical Security Controls found in ETSI TR 103 305 [i.31] are all normative for implementation of the specifications, and the ISI specifications provide useful descriptions of the relationships among the various terminologies and models. A useful summary of basic terminology are provided in figure 8.

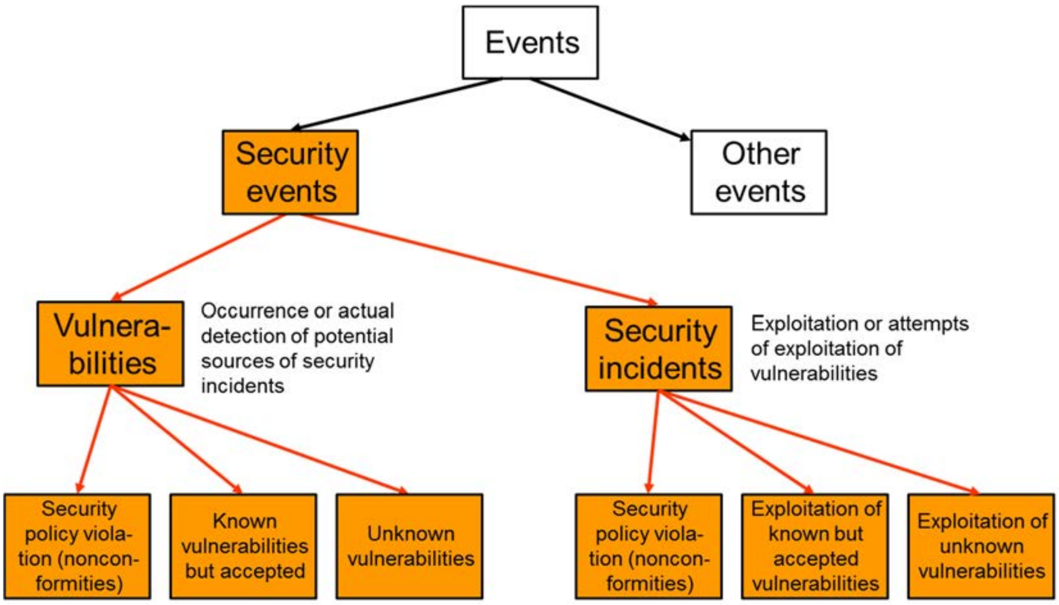

Events
Security events
Other events
Vulnera-bilities
Occurrence or actual detection of potential sources of security incidents
Security incidents
Exploitation or attempts of exploitation of vulnerabilities
Security policy viola-tion (noncon-formities)
Known vulnerabilities but accepted
Unknown vulnerabilities
Security policy viola-tion (noncon-formities)
Exploitation of known but accepted vulnerabilities
Exploitation of unknown vulnerabilities

Figure 8: Relationships between different kinds of events [i.9]

Annex A: Bibliography

- Farnham and Leune, "Tools and Standards for Cyber Threat Intelligence Projects," SANS Institute InfoSec Reading Room, 14 October 2013.

- Northcutt, "A SANS Survey," SANS Institute InfoSec Reading Room, February 2015.

History

Document history		
V1.1.1	August 2016	Publication