ETSI TR 103 331 V2.1.1 (2022-12)

Cyber Security (CYBER);
Structured threat information sharing

Reference
RTR/CYBER-0085

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 - APE 7112B
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° w061004871

Contents

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The declarations pertaining to these essential IPRs, if any, are 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 Directives including the ETSI IPR Policy, no investigation regarding the essentiality of IPRs, 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.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

DECT™, **PLUGTESTS™**, **UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its Members. **3GPP™** and **LTE™** are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners. **oneM2M™** logo is a trademark of ETSI registered for the benefit of its Members and of the oneM2M Partners. **GSM®** and the GSM logo are trademarks registered and owned by the GSM Association.

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. Ultimately, the Malware Information Sharing Platform (MISP) started in 2011 and significantly evolved by a combination of largely EU entities combined with the global CERT/CSIRT community, has emerged as the principal open source threat intelligence sharing platform in widespread use.

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 6 July 2016 [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.

The version 2 edition of the present document updates several of the longstanding platforms, but most significantly takes account of the emergence of MISP as the most widely used threat sharing platform. MISP Threat Sharing (MISP) is an open source threat intelligence platform [i.32]. The MISP project develops utilities and documentation for more effective threat intelligence, by sharing indicators of compromise. Multiple organizations run MISP instances, including a FIRST information sharing SIG, contribute indicators of compromise, and develop the standards and tools specified [i.33].

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 (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union.

NOTE: Available at https://eur-lex.europa.eu/eli/dir/2016/1148/oj.

[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 (October 2020).

NOTE: Available at https://www.cisa.gov/sites/default/files/publications/Non-Federal%20Entity%20Sharing%20Guidance%20under%20the%20Cybersecurity%20Information%20Sharing%20Act%20of%202015_1.pdf.

[i.3] National Cyber Security Centre: "An introduction to threat intelligence", October 2016.

NOTE: Available at https://www.ncsc.gov.uk/files/An-introduction-to-threat-intelligence.pdf.

[i.4] OASIS Specifications, STIX™ 2.1 (June 2021), TAXII™ 2.1 (June 2021).

NOTE: Available at STIX™ V2.1 and TAXII™ V2.1 OASIS Standards are published - OASIS Open (oasis-open.org).

[i.5] Struse: "STIX 2 - Putting Cyber Threat Intelligence to Work", MITRE, May 2018.

NOTE: See also ATT&CK® at https://attack.mitre.org.

[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 Information Security Indicators (ISI) 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 7970: "The Incident Object Description Exchange Format Version 2".

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

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

[i.18] Void.

[i.19] Void.

[i.20] Void.

[i.21] Void.

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

[i.23] Void.

[i.24] Void.

[i.25] Void.

[i.26] Void.

[i.27] Void.

[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".

[i.32] MISP Threat Sharing.

NOTE: Available at https://www.misp-project.org/.

[i.33] MISP Standard.

NOTE: Available at https://www.misp-standard.org/.

[i.34] FIRST Malware Information Sharing Platform (MISP) instance.

NOTE: Available at https://www.first.org/global/sigs/information-sharing/misp.

[i.35] MANRS Primer: CSIRTS.

NOTE: Available at https://www.manrs.org/resources/primers/csirts/.

[i.36] ENISA Telecom Security Forum: "The MANRS Project".

NOTE: Available at https://www.enisa.europa.eu/events/enisa-telecom-security-forum/manrs-enisa-telecom-security-forum.pdf.

[i.37] OASIS Specification: "CSAF Common Vulnerability Reporting Framework (CVRF) Version 1.2".

NOTE: Available at http://docs.oasis-open.org/csaf/csaf-cvrf/v1.2/cs01/csaf-cvrf-v1.2-cs01.html.

[i.38] European Union Agency for Cybersecurity (ENISA): "Orchestration of CSIRT tools", December 2019.

NOTE: Available at https://www.enisa.europa.eu/topics/training-and-exercises/trainings-for-cybersecurity-specialists/online-training-material/documents/orchestration-of-csirt-tools-1/orchestration-of-csirt-tools-tools-analyst.pdf.

3 Definition of terms, symbols and abbreviations

3.1 Terms

Void.

3.2 Symbols

Void.

3.3 Abbreviations

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

ACDC	Advanced Cyber Defence Centre
AIL	Analysis Information Leak
AS	Autonomous System
ATT&CK®	Adversarial Tactics, Techniques, and Common Knowledge
CERT	Computer Emergency Response Team
CIF	Collection Intelligence Framework
CIRC	Computer Incident Response Center
COBIT	Control OBjectives for Information and related Technology
CPNI	Centre for the Protection of National Infrastructure
CSAF	Common Security Advisory Framework
CSIRT	Computer Security Incident Response Team
CTI	Cyber Threat Intelligence
CVE	Common Vulnerabilities and Exposures
CVRF	Common Vulnerability Reporting Framework
CVSS	Common Vulnerability Scoring System
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
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
MANRS	Mutually Agreed Norms for Routing Security
MILE	Managed Incident Lightweight Exchange
MISP	Malware Information Sharing Project
NATO	North Atlantic Treaty Organization
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
PISAX	Pan-European Information Sharing and Analysis Center
RID	Real-time Inter-network Defense
SIG	Special Interest Group
STIX™	Structured Threat Information Expression
TAXII™	Trusted Automated Exchange of Indicator Information
TC	Technical Committee
TCP	Transmission Control Protocol
TTP	Tactics, Techniques and Procedures
US	United States
VERIS	Vocabulary for Event Recording and Incident Sharing

NOTE: CybOX™, STIX™ and TAXII™ are trademarks of the U.S. Government, licensed to OASIS. See https://www.oasis-open.org/committees/cti/ipr.php. MAEC™ is a trademark 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://maecproject.github.io/Legal/.

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. For example, the Financial Services Information Sharing and Analysis Center (FS-ISAC) and The Depository Trust & Clearing Corporation (DTCC) communities are especially significant within one of the EU NIS essential services sectors. In 2014, MITRE published a white paper proposing a new generic threat intelligence sharing model designated STIX which was taken up by new OASIS Technical Committee on Cyber Threat Intelligence (TC CTI).

Another project initiated in Europe in 2011 known as the Malware Information Sharing Project - generally known as MISP - was undertaken as a unifying platform among all the different threat intelligence sharing mechanisms. MISP Threat Sharing (MISP) [i.32] is an open source threat intelligence platform that has achieved broad acceptance and is used today. MISP and the related FIRST Information Sharing SIG are described in clauses 4.14 and 4.15 below.

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, analyse, and share cyber threat intelligence. Three specifications were transitioned from the US Department of Homeland Security (DHS) for development and standardization under the OASIS open standards process: Structured Threat Information Expression (STIX™), Trusted Automated Exchange of Indicator Information (TAXII™), and Cyber Observable Expression (CybOX™). 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™, TAXII™, and CybOX™) were produced. Rather considerable material including running code is hosted on multiple design GitHubs. CybOX and MAEC™ were conflated into the TAXII™ and STIX 2.1 is under development STIX and TAXII versions 1.x have been depreciated. As of June 2022, the principal adopted standards [i.4] consist of:

- STIX™ 2.1 Specification, June 2021.
- TAXII™ 2.1 Specification, June 2021.

The principal resource sites are:

- Documentation and examples, https://oasis-open.github.io/cti-documentation/
- TC Resources and Roadmap, https://oasis-open.github.io/cti-documentation/resources.html
- OASIS CTI TC, https://www.oasis-open.org/committees/cti/
- ATT&CK in STIX 2, https://github.com/mitre/cti

The value of STIX lies in its JSON language to describe Cyber Threat Intelligence, being designed for sharing, its very active and diverse community of developers and analysts, and publication of freely-available international standards by OASIS.

4.2.2 STIX 2.0

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 STIX use cases are depicted in figure 4.1, the intelligence model and expression groups in figure 4.2 and examples in figure 4.3.

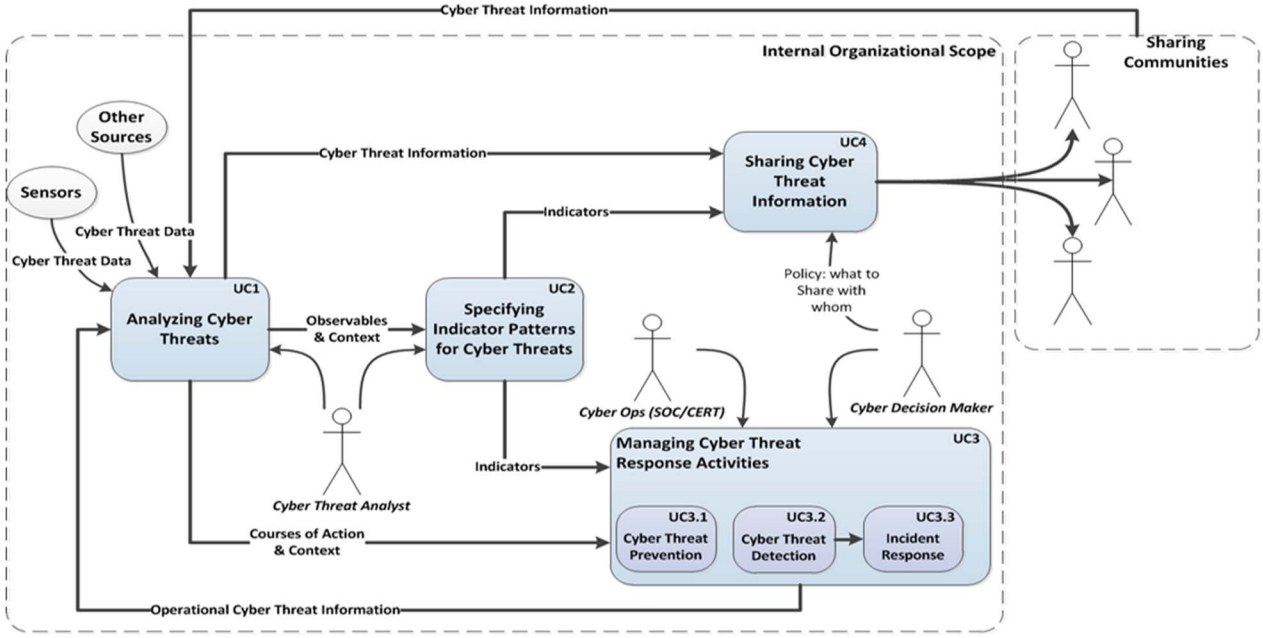


Figure 4.1: STIX use cases [i.4]

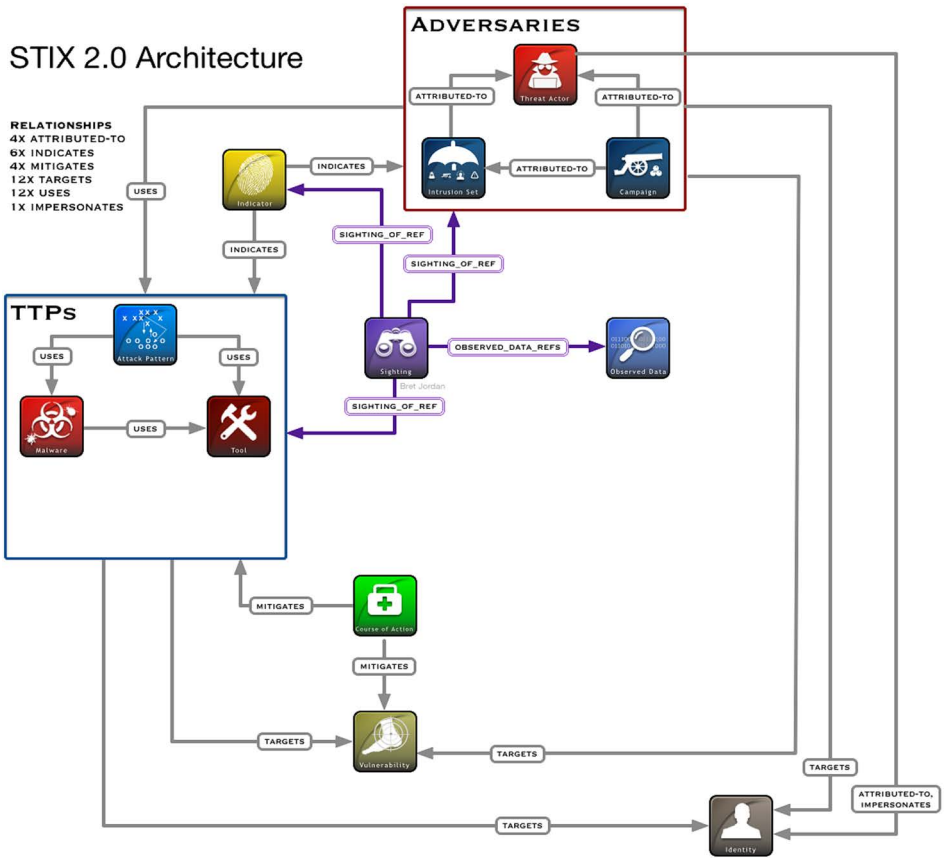


Figure 4.2: STIX 2.0 Architecture [i.5]

Object	Description
Attack Pattern	A type of Tactics, Techniques, and Procedures (TTP) that describes ways threat actors attempt to compromise targets.
Campaign	A grouping of adversarial behaviors that describes a set of malicious activities or attacks that occur over a period of time against a specific set of targets.
Course of Action	An action taken to either prevent an attack or respond to an attack.
Identity	Individuals, organizations, or groups, as well as classes of individuals, organizations, or groups.
Indicator	Contains a pattern that can be used to detect suspicious or malicious cyber activity.
Intrusion Set	A grouped set of adversarial behaviors and resources with common properties believed to be orchestrated by a single threat actor.

Object	Description
Malware	A type of TTP, also known as malicious code and malicious software, used to compromise the confidentiality, integrity, or availability of a victim's data or system.
Observed Data	Conveys information observed on a system or network (e.g., an IP address).
Report	Collections of threat intelligence focused on one or more topics, such as a description of a threat actor, malware, or attack technique, including contextual details.
Threat Actor	Individuals, groups, or organizations believed to be operating with malicious intent.
Tool	Legitimate software that can be used by threat actors to perform attacks.
Vulnerability	A mistake in software that can be directly used by a hacker to gain access to a system or network.

Figure 4.3: STIX 2.0 Domain Objects [i.5]

STIX 2.0 disambiguates between Cyber Observable instances and patterns and defines a new patterning language, is based on SQL-92, bound to the STIX 2.0 Cyber Observable data model, and allows for the expression of a range of patterns, from very simple to more complex (including temporal logic). STIX 2.0 also introduces test-based validation that divides personas for different use cases and each persona will pass a series of tests to be found compatible.

4.2.3 STIX 2.1

STIX continues to evolve, and new capabilities being included in version 2.1 are depicted in figure 4.4.

Completed New Objects	Completed New Features
• Location • Malware (expanded from stub) • Note • Opinion	• Confidence • Internationalization • Time-bounded Relationships

In Progress
• Assertion (threat level, categorization, etc.) • COA • Grouping • IEP • Infrastructure • Patterning updates/changes • STIX "Extension" Mechanism

Figure 4.4: STIX 2.1 New Features [i.5]

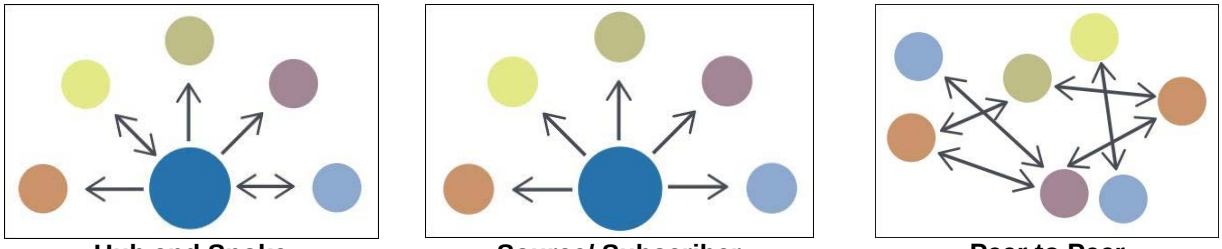
4.2.4 Adversarial Tactics, Techniques, and Common Knowledge in STIX 2.1

Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK®) is a globally-accessible knowledge base of adversary tactics and techniques, based on real-world observations of adversaries' operations and is increasingly being used by the community as a common way to describe adversary behavior.

With ATT&CK, developers can use the well-known and documented STIX 2.1 object model, and can leverage APIs such as the Python STIX APIs to manipulate ATT&CK content. It also enables existing tools to be able to process data (e.g. visualization tools), and access via TAXII 2.1.

4.2.5 TAXII 2.1

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 4.5 and 4.6.



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

Figure 4.5: TAXII models supported [i.4]

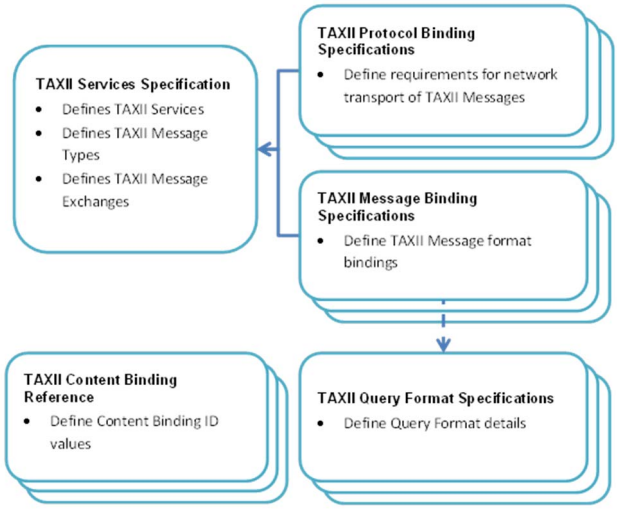


Figure 4.6: TAXII specification components [i.4]

TAXII 2.1 features 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 4.7. The latest version was published in June 2021.

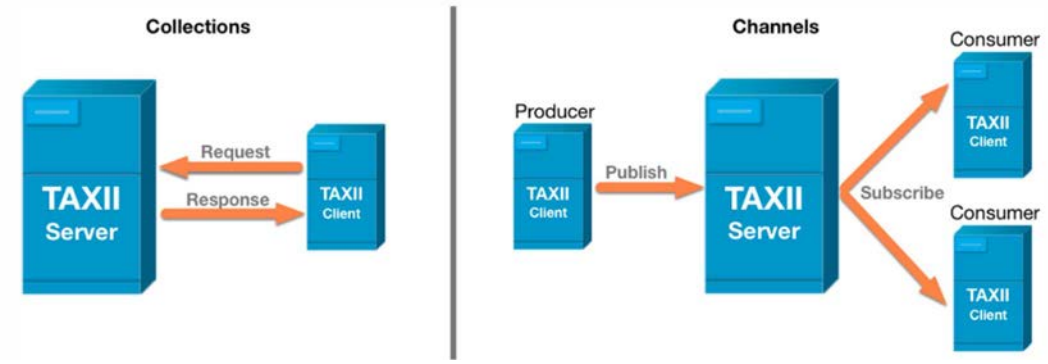


Figure 4.7: TAXII 2.1 channel architecture [i.4]

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 Extended INCident Handling (INCH) 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].

The Incident Object Description Exchange Format (IODEF) defines an information framework to represent computer and network security incidents [i.6]:

- IETF RFC 7970 [i.15]: "Incident Object Description Exchange Format (IODEF) Version 2".
- IETF RFC 6545 [i.16]: "Real-time Inter-network Defense (RID)" defines a protocol to facilitate sharing computer and network security incidents.
- IETF RFC 6546 [i.17]: "Transport of Real-time Inter-network Defense (RID) Messages over HTTP/TLS".

The ITU-T Study Group 17 replicated IETF RFC 6545 [i.16] (RID) as Recommendation ITU-T X.1580 [i.7] and IETF RFC 6046 [i.22] (RID) as Recommendation ITU-T X.1581 [i.7].

4.4 CSIRT Gadgets 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.

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. See https://en.wikipedia.org/wiki/AbuseHelper.

4.7 OMG Threat Modelling Working Group

The Object Management Group had several initiatives related to the sharing of cyber threat information. The most prominent was a proposal for a combined risk-threat information model that incorporates STIX (among other things). The group is no longer active. See https://www.omg.org/hot-topics/threat-modeling.htm.

4.8 ITU-T SG17

The Cybersecurity Rapporteur group within ITU-T Study Group 17 [i.7] 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 Cybersecurity Information Exchange (CYBEX) and an extensive series of specifications have been prepared:

- 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.1542: "Session information message exchange format".
- X.1544: "Common attack pattern enumeration and classification".
- X.1546: "Malware attribute enumeration and characterization".
- X.1550: "Access control models for incidents exchange networks".
- 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".

Additional threat information exchange platforms developed by the ITU-T Security group [i.7] include the following:

- X.1215: "Use Cases for Structured Threat Information Expression".
- X.1217: "Guidelines for applying threat intelligence in telecommunication network operation".

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 https://fireeye.market/apps/211404.

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 Information Security Indicators (ISI) 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. The ISI group subsequently was concluded and the specifications brought into TC CYBER.

- 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 4.8.

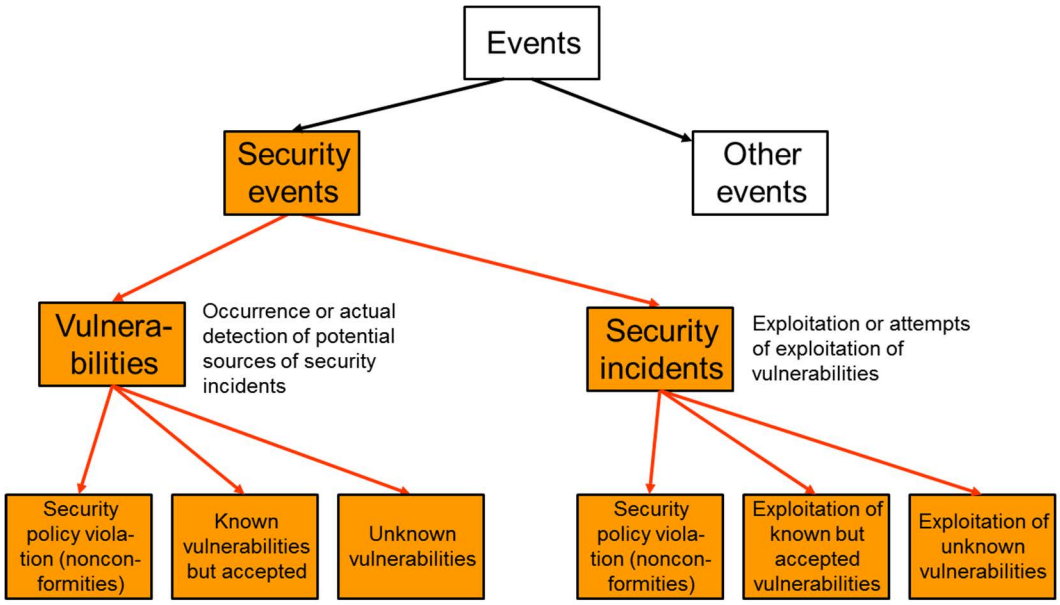


Figure 4.8: Relationships between different kinds of events, ETSI GS ISI 001-1 [i.9]

4.13 OASIS Common Security Advisory Framework (CSAF) Technical Committee

The OASIS Common Security Advisory Framework (CSAF) Technical Committee was created in 2017 to further develop the Common Vulnerability Reporting Framework (CVRF) developed through an industry consortium. Several technology vendors (including major Internet backbone providers) have produced advisories in the CVRF format, and many organizations successfully consume this information https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=csaf. CSAF subsequently published CVRF version 1.2 in September 2017 [i.37] at http://docs.oasis-open.org/csaf/csaf-cvrf/v1.2/cs01/csaf-cvrf-v1.2-cs01.html. The CVRF language which supports creation, update, and interoperable exchange of security advisories as structured information on products, vulnerabilities and the status of impact and remediation among interested parties. Open respositories of the documentation and code are available https://oasis-open.github.io/csaf-documentation/.

CVRF features compatibility with other extensively used vulnerability standards such as CVE and CVSS. It is also being integrated into the STIX Framework.

4.14 MISP Project and MISP Standards

The Malware Information Sharing Project (MISP) has become the leading Open Source Threat Intelligence Platform, including an open standard [i.33] for powering intelligence and information exchange, sharing and modelling among a number of different fields. Those fields include cybersecurity intelligence, threat intelligence, financial fraud, vulnerability information, digital forensic and incident response, among others.

MISP began in 2011 in Belgium, expanded within NATO, and then further expanded among most of the CERT and CSIRT communities. It is funded by the European Union and Luxembourg CIRC and pursuing next-generation information sharing building blocks and has a semi-formal organization. See figure 4.9.

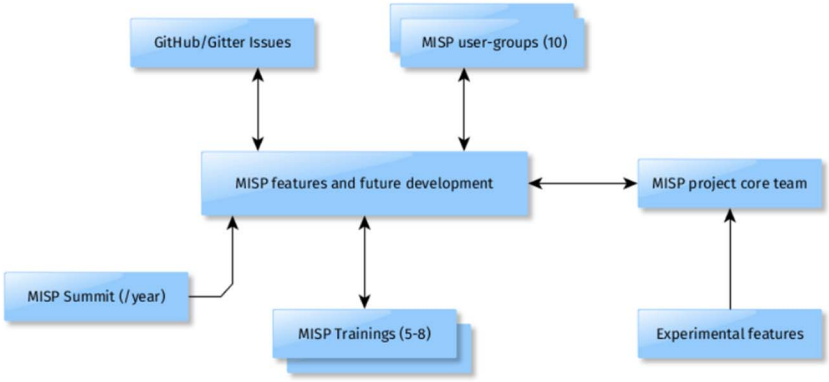


Figure 4.9: MISP Model of Governance [i.32]

There are more than a dozen user communities - both national and global - that contribute to information sharing and development of the platforms, including the FIRST information sharing SIG covered in clause 4.15 below, NATO, PISAX (Pan-European Information Sharing and Analysis Center (ISAC) to IXPs and GRXs), and X-ISAC (Information Sharing and Analysis Center for other ISACs, information sharing communities or CSIRT networks).

In 2016, as part of an effort to enable interoperability and to support integrators, the formats and protocols used by the MISP software began to be documented and more users, contributors and organizations began engaging the the project. In 2017, the MISP format was extended with an object templating system, introducing the ability for anyone to control their own custom data-models without depending on third-party validation or consensus. In order to preserve and foster the standard and its evolution, the MISP project spun off a new structure in 2019, with the aim to standardize the format under the misp-standard.org [i.33]. There are presently 5 official standards: MISP core format, MISP object template format, MISP taxonomy format, MISP galaxy format, and SightingDB format. Tools are available on an open github https://github.com/MISP.

The standards are available as IETF informational Internet-Drafts together with open-source libraries by multiple participating groups accessible from the misp-standards site [i.33]. In addition, there is an array of MISP proprietary and open source software such as The Hive, AIL Framework, and PyMISP. ENISA promotes the use of MISP and its tools for CSIRT orchestration https://www.enisa.europa.eu/topics/trainings-for-cybersecurity-specialists/online-training-material/documents/orchestration-of-csirt-tools-1/orchestration-of-csirt-tools-tools-analyst.pdf [i.38].

4.15 FIRST and the MISP information sharing SIG

FIRST is the Forum of Incident Response and Security Teams. It originated in 1990 as an international extension of the original Carnegie-Mellon University CERT® Coordination Center. Since 1990, it has grown significantly worldwide, and constituted by an array of continuing conferences, technical symposia, workshops, and standards-making SIGs (Special Interest Groups) - that support the incident response and security mission for TCP/IP internets.

The FIRST Information Sharing SIG [i.34] operates a Malware Information Sharing Platform (MISP) instance. The instance is open and automatically enabled for all FIRST members. The FIRST instance allows efficient sharing and storing technical and non-technical information about malware samples, attackers and incidents. It also enables members who have not yet gained experience leveraging threat intelligence to connect with a wider community of organizations, and become familiar with standard information sharing standards and technologies such as STIX. The FIRST MISP instance is also connected with a wider community of incident response organizations and networks, enabling FIRST members to exchange information beyond the boundaries of the FIRST community.

4.16 Mutually Agreed Norms for Routing Security (MANRS)

MANRS is a community of responsible network operators, content providers and Interexchange Providers (IXPs) committed to improving network security and resilience. It offers a set of best practices based on existing norms for network operators to improve the security of the global routing by exchanging information concerning incidents, vulnerabilities, and mitigations. A primer directed at CSIRTs is provided, including outreach to ENISA for meeting NIS2 obligations [i.35] and [i.36].

Annex A: Bibliography

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

NOTE: Available at https://www.sans.org/white-papers/34375/.

- ENISA: "Standards and tools for exchange and processing of actionable information", January 2015.

NOTE: Available at https://www.enisa.europa.eu/publications/standards-and-tools-for-exchange-and-processing-of-actionable-information.

History

Document history		
V1.1.1	August 2016	Publication
V1.2.1	September 2019	Publication
V2.1.1	December 2022	Publication