



CYBER; Structured threat information sharing

ITeH STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
<https://standards.iteh.ai/catalog/standards/sis/48fa68dd-0096-459e-8e25-9e488c0bdd93/etsi-tr-103-331-v1.2.1-2019-09>

Reference

RTR/CYBER-0032

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 prevailing version of an ETSI deliverable is the one made publicly available in PDF format at www.etsi.org/deliver.

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

No part may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm except as authorized by written permission of ETSI.

The content of the PDF version shall not be modified without the written authorization of ETSI.

The copyright and the foregoing restriction extend to reproduction in all media.

© ETSI 2019.

All rights reserved.

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.

Contents

Intellectual Property Rights	4
Foreword.....	4
Modal verbs terminology.....	4
Executive summary	4
Introduction	5
1 Scope	6
2 References	6
2.1 Normative references	6
2.2 Informative references.....	6
3 Definition of terms, symbols and abbreviations.....	7
3.1 Terms.....	7
3.2 Symbols.....	8
3.3 Abbreviations	8
4 Means for exchanging structured cyber threat intelligence.....	9
4.1 Introduction	9
4.2 OASIS Cyber Threat Intelligence Technical Committee (TC CTI)	9
4.2.1 Introduction.....	9
4.2.2 STIX 2.0	10
4.2.3 STIX 2.1	11
4.2.4 Adversarial Tactics, Techniques and Common Knowledge in STIX 2.0	12
4.2.5 TAXII 2.0	12
4.3 IETF Managed Incident Lightweight Exchange Working Group (mile).....	13
4.4 CSIRTGadgets Collective Intelligence Foundation (CIF).....	14
4.5 EU Advanced Cyber Defence Centre (ACDC)	14
4.6 AbuseHelper.....	15
4.7 OMG Threat Modelling Working Group	15
4.8 ITU-T SG17	15
4.9 Open Threat Exchange™ (OTX™).....	16
4.10 OpenIOC Framework	16
4.11 VERIS Framework	16
4.12 ETSI ISI (Information Security Indicators) ISG	16
4.13 OASIS Common Security Advisory Framework (CSAF) Technical Committee	17
Annex A: Bibliography	18
History	19

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables 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.

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.

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

Figures 4.1, 4.2, 4.3, 4.4, 4.5, 4.6, 4.7 copyright © OASIS Open 2017. All Rights Reserved.

Figures 4.1, 4.2, 4.3, 4.4, 4.5, 4.6, 4.7 copyright © United States Government 2016-2018. All Rights Reserved. Used by permission.

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.

ITeH STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
<https://standards.iteh.ai/catalog/standards/sist/68fa68dd-0096-459e-8e25-9e488c0bdd93/etsi-tr-103-331-v1.2.1-2019-09>

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] National Cyber Security Centre: "Threat Intelligence: Collecting, Analysing, Evaluating", October 2016.

NOTE: Available at https://www.ncsc.gov.uk/content/files/protected_files/guidance_files/MWR_Threat_Intelligence_whitepaper-2015.pdf.

- [i.4] OASIS Specifications, STIX 2.0, TAXII 2.0.

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

- [i.5] Internet Engineering Task Force (IETF): "Managed Incident Lightweight Exchange (mile) Working Group".

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

- [i.6] Recommendation ITU-T X.1500-Series: "Cybersecurity information exchange".

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

- [i.7] ETSI ISG ISI (Information Security Indicators) initial Terms of Reference.

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

- [i.8] 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.9] 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.10] ETSI GS ISI 002: "Information Security Indicators (ISI); Event Model A security event classification model and taxonomy".
- [i.11] ETSI GS ISI 003: "Information Security Indicators (ISI); Key Performance Security Indicators (KPSI) to evaluate the maturity of security event detection".
- [i.12] ETSI GS ISI 004: "Information Security Indicators (ISI); Guidelines for event detection implementation".
- [i.13] ETSI GS ISI 005: "Information Security Indicators (ISI); Guidelines for security event detection testing and assessment of detection effectiveness".
- [i.14] IETF RFC 5070: "The Incident Object Description Exchange Format".
- [i.15] IETF RFC 6545: "Real-time Inter-network Defense (RID)".
- [i.16] IETF RFC 6546: "Transport of Real-time Inter-network Defense (RID) Messages over HTTP/TLS".
- [i.17] Void.
- [i.18] Void.
- [i.19] Void.
- [i.20] Void.
- [i.21] IETF RFC 6046: "Transport of Real-time Inter-network Defense (RID) Messages".
- [i.22] Void.
- [i.23] Void.
- [i.24] Void.
- [i.25] Void.
- [i.26] Void.
- [i.27] ISO/IEC 27001: "Information technology -- Security techniques -- Information security management systems -- Requirements".
- [i.28] ISO/IEC 27002: "Information technology -- Security techniques -- Code of practice for information security controls".
- [i.29] ISO/IEC 27004: "Information technology -- Security techniques -- Information security management -- Measurement".
- [i.30] ETSI TR 103 305: "CYBER; Critical Security Controls for Effective Cyber Defence".

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
AS	Autonomous System
ATT&CK™	Adversarial Tactics, Techniques and Common Knowledge
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
CSAF	Common Security Advisory Framework
CSIRT	Computer Security Incidence Response Team
CTI	Cyber Threat Intelligence
CVRF	Common Vulnerability Reporting Framework
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
MILE	Managed Incident Lightweight Exchange
NIS	Network and Information Security
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

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. 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, 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: STIX™ (Structured Threat Information Expression), TAXII™ (Trusted Automated Exchange of Indicator Information), and CybOX™ (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™, 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 2018, the principal adopted standards consist of:

- STIX™ 2.0 Specification, July 2017 [i.4].
- TAXII™ 2.0 Specification, July 2017 [i.4].

The principal resource sites are:

- Documentation and examples: <https://oasis-open.github.io/cti-documentation/>
- Community tooling: <https://oasis-open.github.io/cti-documentation/resources.html>