STIX Version 2.1 Errata 01

Committee Specification Draft 01

02 April 2025

This stage:

https://docs.oasis-open.org/cti/stix/v2.1/errata01/csd01/stix-v2.1-errata01-csd01.md (https://docs.oasis-open.org/cti/stix/v2.1/errata01/csd01/stix-v2.1-errata01-csd01.md) (Authoritative)
https://docs.oasis-open.org/cti/stix/v2.1/errata01/csd01/stix-v2.1-errata01-csd01.html (https://docs.oasis-open.org/cti/stix/v2.1/errata01/csd01/stix-v2.1-errata01-csd01.html)
https://docs.oasis-open.org/cti/stix/v2.1/errata01/csd01/stix-v2.1-errata01-csd01.pdf (https://docs.oasis-open.org/cti/stix/v2.1/errata01/csd01/stix-v2.1-errata01-csd01.pdf)

Previous stage:

N/A

Latest Stage:

https://docs.oasis-open.org/cti/stix/v2.1/errata01/stix-v2.1-errata01.docx (https://docs.oasis-open.org/cti/stix/v2.1/errata01/stix-v2.1-errata01.docx) (Authoritative)
https://docs.oasis-open.org/cti/stix/v2.1/errata01/stix-v2.1-errata01.html (https://docs.oasis-open.org/cti/stix/v2.1/errata01/stix-v2.1-errata01.html)
https://docs.oasis-open.org/cti/stix/v2.1/errata01/stix-v2.1-errata01.pdf (https://docs.oasis-open.org/cti/stix/v2.1/errata01/stix-v2.1-errata01.pdf)

Technical Committee:

OASIS Cyber Threat Intelligence (CTI) TC (https://www.oasis-open.org/committees/cti/)

Chairs:

Marlon Taylor (marlon.taylor@cisa.dhs.gov), DHS Office of Cybersecurity and Communications (http://www.cisa.gov/)
Alexandre Dulaunoy (alexandre.dulaunoy@x.circl.lu), CIRCL (https://www.circl.lu/)

Editors:

Rich Piazza (rpiazza@mitre.org), MITRE Corporation (http://www.mitre.org/)
Emily Ratliff (emily.ratliff@ibm.com), IBM (http://www.ibm.com/)
Stephan Relitz (stephan.relitz@peraton.com), Peraton (https://www.peraton.com/)
Christian Studer (christian.studer@circl.lu), CIRCL (https://www.circl.lu/)

Related work:

This document describes the changes made to:

- *STIX Version 2.1.* Edited by Bret Jordan, Rich Piazza, and Trey Darley. Latest stage: https://docs.oasis-open.org/cti/stix/v2.1/stix-v2.1.html (https://docs.oasis-open.org/cti/stix/v2.1/stix-v2.1.html).

This specification is related to:

- *TAXII Version 2.1.* Edited by Bret Jordan and Drew Varner. Latest stage: https://docs.oasis-open.org/cti/taxii/v2.1/taxii-v2.1.html (https://docs.oasis-open.org/cti/taxii/v2.1/taxii-v2.1.html).
- *STIX/TAXII 2.0 Interoperability Test Document: Part 1 Version 1.1.* Edited by Allan Thomson and Jason Keirstead. Latest stage: https://docs.oasis-open.org/cti/stix-taxii-2-interop-p1/v1.1/stix-taxii-2-interop-p1-v1.1.html (https://docs.oasis-open.org/cti/stix-taxii-2-interop-p1/v1.1/stix-taxii-2-interop-p1-v1.1.html).
- *STIX/TAXII 2.0 Interoperability Test Document: Part 2 Version 1.0.* Edited by Allan Thomson and Jason Keirstead. Latest stage: https://docs.oasis-open.org/cti/stix-taxii-2-interop-p2/v1.0/stix-taxii-2-interop-p2-v1.0.html (https://docs.oasis-open.org/cti/stix-taxii-2-interop-p2/v1.0/stix-taxii-2-interop-p2-v1.0.html).

Abstract:

Structured Threat Information Expression (STIX) is a language for expressing cyber threat and observable information. This document defines concepts that apply across all of STIX and defines the overall structure of the STIX language.

Status:

This document was last revised or approved by the membership of OASIS on the above date. The level of approval is also listed above. Check the "Latest stage" location noted above for possible later revisions of this document. Any other numbered Versions and other technical work produced by the Technical Committee (TC) are listed at https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=cti#technical (https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=cti#technical).

TC members should send comments on this document to the TC's email list. Others should send comments to the TC's public comment list, after subscribing to it by following the instructions at the "Send A Comment (https://www.oasis-open.org/committees/comments/index.php?wg_abbrev=cti)" button on the TC's web page at https://www.oasis-open.org/committees/cti/ (https://www.oasis-open.org/committees/cti/).

This specification is provided under the Non-Assertion (https://www.oasis-open.org/policies-guidelines/ipr#Non-Assertion-Mode) Mode of the OASIS IPR Policy (https://www.oasis-open.org/policies-guidelines/ipr/), the mode chosen when the Technical Committee was established. For information on whether any patents have been disclosed that may be essential to implementing this specification, and any offers of patent licensing terms, please refer to the Intellectual Property Rights section of the TC's web page (https://www.oasis-open.org/committees/cti/ipr.php (https://www.oasis-open.org/committees/cti/ipr.php)).

Note that any machine-readable content (Computer Language Definitions (https://www.oasis-open.org/policies-guidelines/tc-process-2017-05-26#wpComponentsCompLang)) declared Normative for this Work Product is provided in separate plain text files. In the event of a discrepancy between any such plain text file and display content in the Work Product's prose narrative document(s), the content in the separate plain text file prevails.

Citation format:

When referencing this specification the following citation format should be used:

[STI-v2.1-errata01]

STIX Version 2.1 Errata 01. Edited by Rich Piazza, Emily Ratliff, Stephan Relitz and Christian Studer. 02 April 2025. OASIS

Committee Specification Draft 01. https://docs.oasis-open.org/cti/stix/v2.1/errata01/csd01/stix-v2.1-errata01-csd01-complete.html (https://docs.oasis-open.org/cti/stix/v2.1/errata01/csd01/stix-v2.1-errata01-csd01-complete.html). Latest stage: https://docs.oasis-open.org/cti/stix/v2.1/stix-v2.1.html (https://docs.oasis-open.org/cti/stix/v2.1/stix-v2.1.html).

Notices

Table of Contents

---

1. Introduction

This document lists all the corrections made to STIX Version 2.1.

1.1 Scope of changes

Non-material corrections have been made to the STIX 2.1 specification to address issues identified or reported by participants to the TC, listed in the Github issues system, and discussed during CTI TC working call sessions. Changes provide additional or missing vocabulary values, fix typos, improve descriptions, correct examples or provide links between related sections to enhance navigation through the document.

1.2 Description of changes

STIX 2.1 Errata 01 differs from STIX 2.1 in the following ways:

- Updated Malware Embedded Relationships table with missing property in *section 4.11.2 - Malware Relationships*.
  - **operating_system_refs** is no longer missing in the table.
- Malware Analysis Relationships table fixed with the right relationship type between Malware Analysis and Malware in *section 4.12.2 - Malware Analysis Relationships*.
  - wrong analysis-of is replaced with the right av-analysis-of relationship type.
- Property descriptions fixed in *section 6.6.1 - Email Message Object Properties*.
  - **from_ref**, **sender_ref**, **to_refs**, **cc_refs** and **bcc_refs** properties descriptions now mention the right email-addr type

they are referencing.

- Examples fixed in *section 6.12.2.1 - HTTP Request Extension Properties*.
  - the **request_header** property is now a list of type string in the examples, as expected from the description.
- Example fixed in *section 9.5.1 - Observation Expression Qualifiers*.
  - the example used to illustrate the use of *Observation Expression* WITHIN *x* SECONDS now has the right windows-registry-key Observable type.
- Updated *section 10.9 - Implementation Language Vocabulary*.
  - rust value was added.
- Updated *section 10.11 - Industry Sector Vocabulary*.
  - legal value was added.
- Fixed summary in *section 10.12 - Infrastructure Type Vocabulary*.
  - missing control-system, firewall, routers-switches and workstation values were added to the Summary as they were already described in the Vocabulary table.
- Enhanced descriptions in *section 10.14 - Malware Result Vocabulary*.
  - descriptions for every vocabulary values were improved with more descriptive definitions.
- Fixed missing value in *section 10.22 - Report Type Vocabulary*.
  - incident value was added.
- Updated *section 10.23 - Threat Actor Type Vocabulary*.
  - private-sector value was added.
- Fixed multiple Enumeration headers
  - Enumerations now have the right headers, to differenciate enumerations from vocabularies, including:
    - **Enumeration Name** is now used instead of **Vocabulary Name**
    - **Enumeration Summary** is now used instead of **Vocabulary Summary**
    - **Enumeration Value** is now used instead of **Vocabulary Value**
  - These changes apply on:
    - *section 10.4 - Encryption Algorithm Enumeration*
    - *section 10.5 - Extension Type Enumeration*
    - *section 10.16 - Network Socket Address Family Enumeration*
    - *section 10.17 - Network Socket Type Enumeration*
    - *section 10.18 - Opinion Enumeration*
    - *section 10.27 - Windows™ Integrity Level Enumeration*
    - *section 10.29 - Windows™ Registry Datatype Enumeration*
    - *section 10.30 - Windows™ Service Start Type Enumeration*
    - *section 10.31 - Windows™ Service Type Enumeration*
    - *section 10.32 - Windows™ Service Status Enumeration*
- Updated *Appendix B: Relationship Summary Table*.
  - Duplicated relationship located-at between threat-actor and location has been removed.
  - Misspelled relationship exfiltrates-to between malware and infrastructure has been fixed.
  - Missing relationships have been added, including:
    - remediates between course-of-action and malware
    - remediates between course-of-action and vulnerability
    - uses between tool and infrastructure
    - resolves-to between domain-name and domain-name
    - resolves-to between domain-name and ipv4-addr
    - resolves-to between domain-name and ipv6-addr

        - resolves-to between ipv4-addr and mac-addr
        - belongs-to between ipv6-addr and autonomous-system
        - resolves-to between ipv4-addr and mac-addr
        - belongs-to between ipv6-addr and autonomous-system
- Fixed typos in Extension Definition Additional Examples
    - typos were fixed in titles for *section C.2.2 - Adding properties to an existing STIX object instance* and *section C.2.3 - Adding properties to an existing STIX relationship object instance*.
- Special characters were fixed in some participants names in *Appendix F: Acknowledgments*.
- All SCO ids were updated in examples to agree with the `generate_id` method in *python-stix2* library.
- Included all changes based on ITU recommandations.
- Improved references through the document.
    - missing references to sections were added at different places.
    - some references were fixed to point to the right section.
    - in the description of STIX object properties whose value is either a vocabulary or an enumeration, a reference poiting to the given vocabulary or enumeration was added.

2. Conformance

The conformance requirements stated in the OASIS Standard STIX Version 2.1 [STIX-v2.1] are not changed in any way by the publication of this Errata document.

Appendix A: Normative References

The following documents are referenced in such a way that some or all of their content constitutes requirements of this document.

[STIX-v2.1]

STIX Version 2.1. Edited by Bret Jordan, Rich Piazza, and Trey Darley. 10 June 2021. OASIS Standard. https://docs.oasis-open.org/cti/stix/v2.1/os/stix-v2.1-os.html (https://docs.oasis-open.org/cti/stix/v2.1/os/stix-v2.1-os.html). Latest stage: https://docs.oasis-open.org/cti/stix/v2.1/stix-v2.1.html (https://docs.oasis-open.org/cti/stix/v2.1/stix-v2.1.html).

Appendix B: Acknowledgments

STIX Subcommitee Chairs:

Christian Studer, CIRCL

Stephan Relitz, Peraton

Participants:

The following individuals were members of the OASIS CTI Technical Committee during the creation of this specification and their contributions are gratefully acknowledged:

Bret Jordan, Afero

Florian Skopik, AIT Austrian Institute of Technology

Qin Long, Alibaba Cloud Computing Ltd.

Scott Dowsett, Anomali

Wei Huang, Anomali

Patrick Holt, Anomali

Katie Pelusi, Anomali

Patrick Maroney, AT&T Services Inc.

Dean Thompson, Australia and New Zealand Banking Group (ANZ Bank)

Drew Armstrong, Australian Signals Directorate

Jeremy Berthelet, Capgemini

Charles Yarbrough, Carnegie Mellon University

Alexandre Dulaunoy, CIRCL

Andras Iklody, CIRCL

Christian Studer, CIRCL

Raphaël Vinot, CIRCL

Syam Appala, Cisco Systems

Ted Bedwell, Cisco Systems

Andrew Benhase, Cisco Systems

Craig Brozefsky, Cisco Systems

Caitlin Huey, Cisco Systems

Henry Peltokangas, Cisco Systems

Pavan Reddy, Cisco Systems

Omar Santos, Cisco Systems

Thomas Schaffer, Cisco Systems

Michael Simonson, Cisco Systems

Sam Taghavi Zargar, Cisco Systems

Jyoti Verma, Cisco Systems

Andrew Windsor, Cisco Systems

Tim Hudson, Cryptsoft Pty Ltd.

Nick Ascoli, Cyware Labs

Utkarsh Garg, Cyware Labs

Anuj Goel, Cyware Labs

Avkash Kathiriya, Cyware Labs

Joe Laugle, Dell Technologies

Carolina Canales-Valenzuela, Ericsson AB

Chris Ricard, Financial Services Information Sharing and Analysis Center (FS-ISAC)

Daniel Riedel, GL Venture Studio HoldCo LLC

Mark Risher, Google Inc.

Xiaoyu Ge, Huawei Technologies Co., Ltd.

Ho Hock William, Huawei Technologies Co., Ltd.

Dong Huang, Huawei Technologies Co., Ltd.

David Webber, Huawei Technologies Co., Ltd.

Leszek Adamiak, IBM

Eldan Ben-Haim, IBM

Roseann Guttierrez, IBM

Sandra Hernandez, IBM

Chenta Lee, IBM

John Morris, IBM

Emily Ratliff, IBM

Aviv Ron, IBM

Nick Rossmann, IBM

Laura Rusu, IBM

Frank Schaffa, IBM

Garret Taylor, IBM

Sulakshan Vajipayajula, IBM

Ron Williams, IBM

Ashwini Jarral, IJIS Institute

James Cabral, Individual

Jane Ginn, Individual

Rachel James, Individual

Elysa Jones, Individual

Terry MacDonald, Individual

Allan Thomson, Individual

Jorge Aviles, Johns Hopkins University Applied Physics Laboratory

Cory Huyssoon, Johns Hopkins University Applied Physics Laboratory

Karin Marr, Johns Hopkins University Applied Physics Laboratory

Julie Modlin, Johns Hopkins University Applied Physics Laboratory

Mark Moss, Johns Hopkins University Applied Physics Laboratory

Mark Munoz, Johns Hopkins University Applied Physics Laboratory

Nathan Reller, Johns Hopkins University Applied Physics Laboratory

Jonathan Matkowsky, Microsoft Corporation

Jautau White, Microsoft Corporation

Desiree Beck, Mitre Corporation

Jen Burns, Mitre Corporation

Michael Chisholm, Mitre Corporation

Mike Cokus, Mitre Corporation

Sam Cornwell, Mitre Corporation

Kartikey Desai, Mitre Corporation

Pavan Gudimetta, Mitre Corporation

Chris Lenk, Mitre Corporation

Bob Natale, Mitre Corporation

Timothy O'Neill, Mitre Corporation

Nicole Parrish, Mitre Corporation

Richard Piazza, Mitre Corporation

Larry Rodrigues, Mitre Corporation

Zach Rush, Mitre Corporation

Jon Salwen, Mitre Corporation

Charles Schmidt, Mitre Corporation

Matt Scola, Mitre Corporation

Richard Struse, Mitre Corporation

Alex Tweed, Mitre Corporation

Emmanuelle Vargas-Gonzalez, Mitre Corporation

Bryan Worrell, Mitre Corporation

Jackson Wynn, Mitre Corporation

Josh Poster, National Council of ISACs (NCI)

Mike Boyle, National Security Agency

Sean Carroll, National Security Agency

Alicia Ellis, National Security Agency

Jessica Fitzgerald-McKay, National Security Agency

David Kemp, National Security Agency

Shaun McCullough, National Security Agency

Michael Rosa, National Security Agency

James Bryce Clark, OASIS

Kelly Cullinane, OASIS

Jane Harnad, OASIS

Mary Beth Minto, OASIS

Holly Petersen, OASIS

Claudia Rauch, OASIS

Sam Czsun, Open Security Alliance

Patrick Bredenberg, Oracle

Johnny Gau, Oracle

Shayam Jayaraman, Oracle

Sunil Ravipati, Oracle

Kirk Dunkelberger, Peraton

Jason Liu, Peraton

Qem Lumi, Peraton

Stephan Relitz, Peraton

Jason Keirstead, Pobal Cyber Ltd

David Bizeul, SEKOIA.IO

Georges Bossert, SEKOIA.IO

Lorraine Desforges, SEKOIA.IO

Marco Caselli, Siemens AG

Jonas Plum, Siemens AG

Manos Athanatos, Technical University of Crete

Vasileios Mavroeidis, University of Oslo

Mateusz Zych, University of Oslo

Kaleb Hines, US Department of Defense (DoD)

Jeffrey Mates, US Department of Defense (DoD)

George Parson, US Department of Defense (DoD)

David Ailshire, US DHS Cybersecurity and Infrastructure Security Agency (CISA)

Steven Fox, US DHS Cybersecurity and Infrastructure Security Agency (CISA)

Taneika Hill, US DHS Cybersecurity and Infrastructure Security Agency (CISA)

Kevin Klein, US DHS Cybersecurity and Infrastructure Security Agency (CISA)

Evette Maynard-Noel, US DHS Cybersecurity and Infrastructure Security Agency (CISA)

Jackie Eun Park, US DHS Cybersecurity and Infrastructure Security Agency (CISA)

Sean Sobieraj, US DHS Cybersecurity and Infrastructure Security Agency (CISA)

Marlon Taylor, US DHS Cybersecurity and Infrastructure Security Agency (CISA)

Preston Werntz, US DHS Cybersecurity and Infrastructure Security Agency (CISA)

Stephen Banghart, US NIST

Appendix C: Notices

OASIS Technical Committee that produced this deliverable.]

[OASIS invites any party to contact the OASIS TC Administrator if it is aware of a claim of ownership of any patent claims that would necessarily be infringed by implementations of this OASIS Standards Final Deliverable by a patent holder that is not willing to provide a license to such patent claims in a manner consistent with the IPR Mode of the OASIS Technical Committee that produced this OASIS Standards Final Deliverable. OASIS may include such claims on its website, but disclaims any obligation to do so.]

[OASIS takes no position regarding the validity or scope of any intellectual property or other rights that might be claimed to pertain to the implementation or use of the technology described in this OASIS Standards Final Deliverable or the extent to which any license under such rights might or might not be available; neither does it represent that it has made any effort to identify any such rights. Information on OASIS' procedures with respect to rights in any document or deliverable produced by an OASIS Technical Committee can be found on the OASIS website. Copies of claims of rights made available for publication and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this OASIS Standards Final Deliverable, can be obtained from the OASIS TC Administrator. OASIS makes no representation that any information or list of intellectual property rights will at any time be complete, or that any claims in such list are, in fact, Essential Claims.]