# 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.docx (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.pdf

**Previous stage:**
N/A

**Latest stage:**
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.pdf

**Technical Committee:**
OASIS Cyber Threat Intelligence (CTI) TC

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

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

**Related work:**

- *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.

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.
- *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.
- *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.

**Abstract:**
This document provides Errata for the OASIS Standard STIX Version 2.1. It corrects non-material issues identified or reported by participants to the TC, listed in the Github issues system, and discussed during CTI TC working call sessions.

### 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://groups.oasis-open.org/communities/tc-community-home2?CommunityKey=c6c33da0-d1ee-42dd-9427-018dc7d32277.

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 by following the instructions listed here: https://groups.oasis-open.org/communities/community-home?CommunityKey=d682c16c-d20d-45c1-ac8e-018f5aa7b6ae.

This specification is provided under the Non-Assertion Mode of the OASIS IPR Policy, 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).

Note that any machine-readable content (Computer Language Definitions) 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:

**[STIX-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.html Latest stage: https://docs.oasis-open.org/cti/stix/v2.1/errata01/stix-v2.1-errata01.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

## 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 10.13 - 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. Latest stage: https://docs.oasis-open.org/cti/stix/v2.1/stix-v2.1.html.

# Appendix B. Acknowledgements

**STIX Subcommittee 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:

Kai Li, 360 Enterprise Security Group

shu li, 360 Enterprise Security Group

qian yin, 360 Enterprise Security Group

Xinhua Zheng, 360 Enterprise Security Group

Robert Coderre, Accenture

Kyle Maxwell, Accenture

David Crawford, Aetna

Marcos Orallo, Airbus Group SAS

Roman Fiedler, AIT Austrian Institute of Technology

Florian Skopik, AIT Austrian Institute of Technology

Ryan Clough, Anomali

Nicholas Hayden, Anomali

Wei Huang, Anomali

Russell Matbouli, Anomali

Angela Nichols, Anomali

Hugh Njemanze, Anomali

Katie Pelusi, Anomali

Patrick Maroney, AT&T

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

Radu Marian, Bank of America

Sounil Yu, Bank of America

Vicky Laurens, Bank of Montreal

Bret Jordan, Broadcom

Trey Darley, CCB/CERT.be

Alexandre Dulaunoy, CIRCL

Andras Iklody, CIRCL

Christian Studer, CIRCL

Raphaël Vinot, CIRCL

Syam Appala, Cisco Systems

Ted Bedwell, Cisco Systems
Pavan Reddy, Cisco Systems
Omar Santos, Cisco Systems
Sam Taghavi Zargar, Cisco Systems
Jyoti Verma, Cisco Systems
Jart Armin, Cyber Threat Intelligence Network, Inc. (CTIN)
Doug DePeppe, Cyber Threat Intelligence Network, Inc. (CTIN)
Jane Ginn, Cyber Threat Intelligence Network, Inc. (CTIN)
Ben Ottoman, Cyber Threat Intelligence Network, Inc. (CTIN)
David Powell, Cyber Threat Intelligence Network, Inc. (CTIN)
Andreas Sfakianakis, Cyber Threat Intelligence Network, Inc. (CTIN)
Anuj Goel, Cyware Labs
Avkash Kathiriya, Cyware Labs
Jaeden Hampton, DarkLight, Inc.
Ryan Hohimer, DarkLight, Inc.
Ryan Joyce, DarkLight, Inc.
Shawn Riley, DarkLight, Inc.
Ian Roberts, DarkLight, Inc.
Andrew Byrne, Dell
Jeff Odom, Dell
Sreejith Padmajadevi, Dell
Ravi Sharda, Dell
Will Urbanski, Dell
David Ailshire, DHS Office of Cybersecurity and Communications (CS&C)
Steven Fox, DHS Office of Cybersecurity and Communications (CS&C)
Taneika Hill, DHS Office of Cybersecurity and Communications (CS&C)
Evette Maynard-Noel, DHS Office of Cybersecurity and Communications (CS&C)
Jackie Eun Park, DHS Office of Cybersecurity and Communications (CS&C)
Sean Sobieraj, DHS Office of Cybersecurity and Communications (CS&C)
Marlon Taylor, DHS Office of Cybersecurity and Communications (CS&C)
Preston Werntz, DHS Office of Cybersecurity and Communications (CS&C)
Jörg Abraham, EclecticIQ
wouter bolsterlee, EclecticIQ
Adam Bradbury, EclecticIQ
Marko Dragoljevic, EclecticIQ
Oliver Gheorghe, EclecticIQ
Joep Gommers, EclecticIQ
Caitlin Huey, EclecticIQ

Christopher O'Brien, EclecticIQ

Sergey Polzunov, EclecticIQ

Rutger Prins, EclecticIQ

Aukjan van Belkum, EclecticIQ

Raymon van der Velde, EclecticIQ

Tom Vaughan, EclecticIQ

Joseph Woodruff, EclecticIQ

Ben Sooter, Electric Power Research Institute (EPRI)

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

Sean Barnum, FireEye, Inc.

Phillip Boles, FireEye, Inc.

Prasad Gaikwad, FireEye, Inc.

Haripriya Gajendran, FireEye, Inc.

Will Green, FireEye, Inc.

Rajeev Jha, FireEye, Inc.

Gary Katz, FireEye, Inc.

Anuj Kumar, FireEye, Inc.

James Meck, FireEye, Inc.

Shyamal Pandya, FireEye, Inc.

Paul Patrick, FireEye, Inc.

Remko Weterings, FireEye, Inc.

Tim Jones, ForeScout

Ryusuke Masuoka, Fujitsu Limited

Daisuke Murabayashi, Fujitsu Limited

Derek Northrope, Fujitsu Limited

Toshitaka Satomi, Fujitsu Limited

Koji Yamada, Fujitsu Limited

Kunihiko Yoshimura, Fujitsu Limited

Robert van Engelen, Genivia

Eric Burger, Georgetown University

Allison Miller, Google Inc.

Mark Risher, Google Inc.

Yoshihide Kawada, Hitachi, Ltd.

Jun Nakanishi, Hitachi, Ltd.

Kazuo Noguchi, Hitachi, Ltd.

Akihito Sawada, Hitachi, Ltd.

Yutaka Takami, Hitachi, Ltd.

Masato Terada, Hitachi, Ltd.

Adrian Bishop, Huntsman Security

Eldan Ben-Haim, IBM

Allen Hadden, IBM

Sandra Hernandez, IBM

Jason Keirstead, IBM

Chenta Lee, IBM

John Morris, IBM

Devesh Parekh, IBM

Emily Ratliff, IBM

Nick Rossmann, IBM

Laura Rusu, IBM

Ron Williams, IBM

Paul Martini, iboss, Inc.

Vasileios Mavroeidis, IFI

Kamer Vishi, IFI

Joerg Eschweiler, Individual

Elysa Jones, Individual

Terry MacDonald, Individual

Tim Casey, Intel Corporation

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

Pamela Smith, Johns Hopkins University Applied Physics Laboratory

Vivek Jain, JPMorgan Chase Bank, N.A.

Subodh Kumar, JPMorgan Chase Bank, N.A.

David Laurance, JPMorgan Chase Bank, N.A.

Russell Culpepper, Kaiser Permanente

Beth Pumo, Kaiser Permanente

Michael Slavick, Kaiser Permanente

Daniel Ben-Chitrit, LookingGlass

Wesley Brown, LookingGlass

Dennis Hostetler, LookingGlass

Himanshu Kesar, LookingGlass

Matt Pladna, LookingGlass

Vlad Serban, LookingGlass

Allan Thomson, LookingGlass

Chris Wood, LookingGlass

Kent Landfield, McAfee
Jonathan Baker, Mitre Corporation
Desiree Beck, Mitre Corporation
Michael Chisholm, Mitre Corporation
Sam Cornwell, Mitre Corporation
Sarah Kelley, Mitre Corporation
Ivan Kirillov, Mitre Corporation
Michael Kouremetis, Mitre Corporation
Chris Lenk, Mitre Corporation
Nicole Parrish, Mitre Corporation
Richard Piazza, Mitre Corporation
Larry Rodrigues, Mitre Corporation
Jon Salwen, Mitre Corporation
Charles Schmidt, Mitre Corporation
Richard Struse, Mitre Corporation
Alex Tweed, Mitre Corporation
Emmanuelle Vargas-Gonzalez, Mitre Corporation
John Wunder, Mitre Corporation
James Cabral, MTG Management Consultants, LLC.
Scott Algeier, National Council of ISACs (NCI)
Denise Anderson, National Council of ISACs (NCI)
Josh Poster, National Council of ISACs (NCI)
Mike Boyle, National Security Agency
Jessica Fitzgerald-McKay, National Security Agency
David Kemp, National Security Agency
Shaun McCullough, National Security Agency
Jason Romano, National Security Agency
John Anderson, NC4
Michael Butt, NC4
Mark Davidson, NC4
Daniel Dye, NC4
Michael Pepin, NC4
Natalie Suarez, NC4
Benjamin Yates, NC4
Sarah Brown, NCI Agency
Oscar Serrano, NCI Agency
Daichi Hasumi, NEC Corporation
Takahiro Kakumaru, NEC Corporation

Lauri Korts-Parn, NEC Corporation
Kelly Cullinane, New Context Services, Inc.
John-Mark Gurney, New Context Services, Inc.
Christian Hunt, New Context Services, Inc.
Danny Purcell, New Context Services, Inc.
Daniel Riedel, New Context Services, Inc.
Andrew Storms, New Context Services, Inc.
Drew Varner, NineFX, Inc.
Stephen Banghart, NIST
David Darnell, North American Energy Standards Board
James Crossland, Northrop Grumman
Robert Van Dyk, Northrop Grumman
Cheolho Lee, NSRI
Cory Casanave, Object Management Group
Joel Myhre, Pacific Disaster Center
Vishaal Hariprasad, Palo Alto Networks
Stephan Relitz, Peraton
Brad Bohen, Perch
Aharon Chernin, Perch
Zach Kanzler, Perch
Michael Lane, Perch
Michael Riggs, Perch
Sean O'Brien, Purism SPC
John Tolbert, Queralt Inc.
Forrest Hare, Science Application International
Duncan Sparrell, sFractal Consulting LLC
Thomas Schreck, Siemens AG
Adam Wyner, Swansea University
Bret Jordan, Symantec Corp.
Robert Keith, Symantec Corp.
Curtis Kostrosky, Symantec Corp.
Chris Larsen, Symantec Corp.
Michael Mauch, Symantec Corp.
Aubrey Merchant, Symantec Corp.
Efrain Ortiz, Symantec Corp.
Mingliang Pei, Symantec Corp.
Kenneth Schneider, Symantec Corp.
Arnaud Taddei, Symantec Corp.

Brian Witten, Symantec Corp.

Greg Reaume, TELUS

Alan Steer, TELUS

Crystal Hayes, The Boeing Company

Andrew Gidwani, ThreatConnect, Inc.

Cole Iliff, ThreatConnect, Inc.

Andrew Pendergast, ThreatConnect, Inc.

Jason Spies, ThreatConnect, Inc.

Ryan Trost, ThreatQuotient, Inc.

David Girard, Trend Micro

Brandon Niemczyk, Trend Micro

Eric Shulze, Trend Micro

Patrick Coughlin, TruSTAR Technology

Chris Roblee, TruSTAR Technology

ADHAM ALBAKRI, University of Kent

Jeffrey Mates, US Department of Defense (DoD)

Evette Maynard-Noel, US Department of Homeland Security

Lee Chieffalo, Viasat

Wilson Figueroa, Viasat

Andrew May, Viasat

Ales Cernivec, XLAB

Anthony Rutkowski, Yanna Technologies LLC

# Appendix C. Notices



All capitalized terms in the following text have the meanings assigned to them in the OASIS Intellectual Property Rights Policy (the "OASIS IPR Policy"). The full Policy may be found at the OASIS website: [https://www.oasis-open.org/policies-guidelines/ipr/].

This document and translations of it may be copied and furnished to others, and derivative works that comment on or otherwise explain it or assist in its implementation may be prepared, copied, published, and distributed, in whole or in part, without restriction of any kind, provided that the above copyright notice and this section are included on all such copies and derivative works. However, this document itself may not be modified in any way, including by removing the copyright notice or references to OASIS, except as needed for the purpose of developing any document or deliverable produced by an OASIS Technical Committee (in which case the rules applicable to copyrights, as set forth in the OASIS IPR Policy, must be followed) or as required to translate it into languages other than English.

The limited permissions granted above are perpetual and will not be revoked by OASIS or its successors or assigns.

This document and the information contained herein is provided on an "AS IS" basis and OASIS DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY OWNERSHIP RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. OASIS AND ITS MEMBERS WILL NOT BE LIABLE FOR ANY DIRECT, INDIRECT, SPECIAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF ANY USE OF THIS DOCUMENT OR ANY PART THEREOF.

As stated in the OASIS IPR Policy, the following three paragraphs in brackets apply to OASIS Standards Final Deliverable documents (Committee Specifications, OASIS Standards, or Approved Errata).

[OASIS requests that any OASIS Party or any other party that believes it has patent claims that would necessarily be infringed by implementations of this OASIS Standards Final Deliverable, to notify OASIS TC Administrator and provide an indication of its willingness to grant patent licenses to such patent claims in a manner consistent with the IPR Mode of the 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.]

The name "OASIS" is a trademark of OASIS, the owner and developer of this document, and should be used only to refer to the organization and its official outputs. OASIS welcomes reference to, and implementation and use of, documents, while reserving the right to enforce its marks against misleading uses. Please see https://www.oasis-open.org/policies-guidelines/trademark/ for above guidance.