Network Course Of Action Specification Version 1.0

Working Draft 01

DD Month 2015

Technical Committee:

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

Chair:

Richard Struse ([Richard.Struse@HQ.DHS.GOV](mailto:Richard.Struse@HQ.DHS.GOV)), [DHS Office of Cybersecurity and Communications (CS&C)](http://www.dhs.gov/office-cybersecurity-and-communications)

Editor:

Jyoti Verma ([jyoverma@cisco.com](mailto:jyoverma@cisco.com)), [Cisco Systems Inc.](http://www.cisco.com)

Additional artifacts:

This prose specification is one component of a Work Product that also includes:

* XML schemas: (list file names or directory name)
* Other parts (list titles and/or file names)

Related work:

This specification replaces or supersedes:

* Specifications replaced by this specification (hyperlink, if available)

This specification is related to:

* Related specifications (hyperlink, if available)

Declared XML namespaces:

* list namespaces declared within this specification

Abstract:

To accelerate the response to newly detected incidents and new types of threat indicators, we need ways to express detailed recommended actions.  In this specification, the STIX Structured CourseOfAction field is extended in order to provide actionable details that can be used to carry out investigation, remediation, or mitigation of threats. By combing machine and human readable elements, the extensions provide IT security professionals with actionable details to go along with the threat information provided by STIX, making it easier for them to select and initiate an appropriate response to an incident.

Status:

This [Working Draft](https://www.oasis-open.org/policies-guidelines/tc-process#dWorkingDraft) (WD) has been produced by one or more TC Members; it has not yet been voted on by the TC or [approved](https://www.oasis-open.org/policies-guidelines/tc-process#committeeDraft) as a Committee Draft (Committee Specification Draft or a Committee Note Draft). The OASIS document [Approval Process](https://www.oasis-open.org/policies-guidelines/tc-process#standApprovProcess) begins officially with a TC vote to approve a WD as a Committee Draft. A TC may approve a Working Draft, revise it, and re-approve it any number of times as a Committee Draft.

URI patterns:

Initial publication URI:  
http://docs.oasis-open.org/cti/Network-COA/v1.0/csd01/Network-COA-v1.0-csd01.docx

Permanent “Latest version” URI:  
http://docs.oasis-open.org/cti/Network-COA/v1.0/Network-COA-v1.0.docx

(Managed by OASIS TC Administration; please don’t modify.)

Copyright © OASIS Open 2016. All Rights Reserved.

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](https://www.oasis-open.org/policies-guidelines/ipr) may be found at the OASIS website.

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.

Table of Contents

[1 Introduction 4](#_Toc409437255)

[1.1 Terminology 4](#_Toc409437256)

[1.2 Normative References 4](#_Toc409437257)

[1.3 Non-Normative References 4](#_Toc409437258)

[2 Section Title 5](#_Toc409437259)

[2.1 Level 2 section title 5](#_Toc409437260)

[2.1.1 Level 3 section title 5](#_Toc409437261)

[2.1.1.1 Level 4 section title is usually deepest for Table of Contents 5](#_Toc409437262)

[3 Conformance 6](#_Toc409437263)

[Appendix A. Acknowledgments 7](#_Toc409437264)

[Appendix B. Example Title 8](#_Toc409437265)

[B.1 Subsidiary section 8](#_Toc409437266)

[B.1.1 Sub-subsidiary section 8](#_Toc409437267)

[B.1.1.1 Sub-sub-subsidiary section 8](#_Toc409437268)

[Appendix C. Revision History 9](#_Toc409437269)

# Introduction

[All text is normative unless otherwise labeled]

## Terminology

The key words “MUST”, “MUST NOT”, “REQUIRED”, “SHALL”, “SHALL NOT”, “SHOULD”, “SHOULD NOT”, “RECOMMENDED”, “MAY”, and “OPTIONAL” in this document are to be interpreted as described in [[RFC2119](#RFC2119)].

## Normative References

[RFC2119] Bradner, S., “Key words for use in RFCs to Indicate Requirement Levels”, BCP 14, RFC 2119, March 1997. <http://www.ietf.org/rfc/rfc2119.txt>.

[Reference] [Full reference citation]

## Non-Normative References

[Reference] [Full reference citation]

(Remove Non-Normative References section if there are none. Remove this note and text below before submitting for publication.)

Recommended approach: Set up [Reference] label elements as "Bookmarks", then use hyperlinks to them within the document. Use the "Ref" paragraph style to format references.

**NOTE: The proper format for citation of technical work produced by an OASIS TC (whether Standards Track or Non-Standards Track) is:**

[Citation Label] Work Product [title](http://docs.oasis-open.org/specGuidelines/ndr/namingDirectives.html#workProductName) (italicized). Edited by Albert Alston, Bob Ballston, and Calvin Carlson. Approval date (DD Month YYYY). OASIS [Stage](http://docs.oasis-open.org/specGuidelines/ndr/namingDirectives.html#stage) Identifier and [Revision](http://docs.oasis-open.org/specGuidelines/ndr/namingDirectives.html#revision) Number (*e.g.*, OASIS Committee Specification Draft 01). Principal URI ([version-specific URI](http://docs.oasis-open.org/specGuidelines/ndr/namingDirectives.html#this-version), *e.g*., with stage component: somespec-v1.0-csd01.html). Latest version: ([latest version URI](http://docs.oasis-open.org/specGuidelines/ndr/namingDirectives.html#latest-version), without stage identifiers).

For example:

**[OpenDoc-1.2]** *Open Document Format for Office Applications (OpenDocument) Version 1.2*. Edited by Patrick Durusau and Michael Brauer. 19 January 2011. OASIS Committee Specification Draft 07. <http://docs.oasis-open.org/office/v1.2/csd07/OpenDocument-v1.2-csd07.html>. Latest version: <http://docs.oasis-open.org/office/v1.2/OpenDocument-v1.2.html>.

# Section Title

text

## Level 2 section title

text

### Level 3 section title

text

#### Level 4 section title is usually deepest for Table of Contents

text

##### Level 5 or deeper may be included in TOC with TC approval

text

# Conformance

The last numbered section in the specification must be the Conformance section. Conformance Statements/Clauses go here.

See “Guidelines to Writing Conformance Clauses”:   
<http://docs.oasis-open.org/templates/TCHandbook/ConformanceGuidelines.html>.

1. Acknowledgments

The following individuals have participated in the creation of this specification and are gratefully acknowledged:

Participants:

[Participant Name, Affiliation | Individual Member]

[Participant Name, Affiliation | Individual Member]

1. Example Title

text

* 1. Subsidiary section

text

* + 1. Sub-subsidiary section

Text

* + - 1. Sub-sub-subsidiary section

text

* + - * 1. Sub-sub-sub-subsidiary section

text

1. Revision History

|  |  |  |  |
| --- | --- | --- | --- |
| **Revision** | **Date** | **Editor** | **Changes Made** |
| [Rev number] | [Rev Date] | [Modified By] | [Summary of Changes] |