OASIS Cyber Threat Intelligence (CTI) TC

Join This TC (/committees/join)   **TC Members Page** (/apps/org/workgroup/cti/)

Send A Comment (/committees/comments/index.php?wg_abbrev=cti)

Defining a set of information representations and protocols to support automated information sharing for cybersecurity situational awareness, real-time network defense, and sophisticated threat analysis.

Richard Struse, Richard.Struse@HQ.DHS.GOV (mailto:Richard.Struse@HQ.DHS.GOV) , Chair
Alexander Foley, Secretary

Table of Contents

Announcements

Tweet #STIX   **Tweet #TAXII**   **Tweet #CybOX**

See new OASIS press release announcing CTI TC (https://www.oasis-open.org/news/pr/oasis-advances-automated-cyber-threat-intelligence-sharing-with-stix-taxii-cybox) and CTI coverage in *OECD ITAC News* (https://www.internetac.org/archives/2328) and *Dark Reading* (http://darkmatters.norsecorp.com/2015/07/29/dhs-transitions-stix-taxii-and-cybox-standards-to-oasis/) .

The first meeting of the OASIS Cyber Threat Intelligence (CTI) Technical Committee was held via teleconference on 18 June 2015 at 17:00 UTC, with over 100 persons total in attendance. Richard Struse (DHS Office of Cybersecurity and Communications - CS&C) was elected TC Chair.

Participation in the OASIS CTI TC (https://www.oasis-open.org/committees/cti/) is open to all interested parties. Contact join@oasis-open.org (mailto:join@oasis-open.org) for more information.

Overview

The OASIS Cyber Threat Intelligence (CTI) TC was chartered to define a set of information representations and protocols to address the need to model, analyze, and share cyber threat intelligence. In the initial phase of TC work, three specifications will be 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 will:

- 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

For more information on the CTI TC, see the TC Charter (http://www.oasis-open.org/committees/cti/charter.php) .

Subcommittees

- CTI STIX Subcommittee (https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=cti-stix) , with list archives from OASIS (https://lists.oasis-open.org/archives/cti-stix/) and MarkMail (http://markmail.org/browse/org.oasis-open.lists.cti-stix)
- CTI TAXII Subcommittee (https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=cti-taxii) , with list archives from OASIS (https://lists.oasis-open.org/archives/cti-taxii/) and MarkMail (http://markmail.org/browse/org.oasis-open.lists.cti-taxii)
- CTI CybOX Subcommittee (https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=cti-cybox) , with list archives from OASIS (https://lists.oasis-open.org/archives/cti-cybox/) and MarkMail (http://markmail.org/browse/org.oasis-open.lists.cti-cybox)
- CTI Interoperability Subcommittee (https://www.oasis-open.org/committees/cti-interoperability/) , with list archives from OASIS (https://lists.oasis-open.org/archives/cti-interoperability/) and MarkMail (http://markmail.org/browse/org.oasis-open.lists.cti-interoperability)
- CTI Marketing Group (https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=cti-marketing)

TC Liaisons

No TC Liaisons have been announced for this TC.

TC Tools and Approved Publications

- TC Wiki (https://wiki.oasis-open.org/cti/) (STIX (https://wiki.oasis-open.org/cti/stix) , TAXII (https://wiki.oasis-open.org/cti/taxii) , CybOX (https://wiki.oasis-open.org/cti/cybox))
- WebConf Meeting Management (http://webconf.soaphub.org/conf/room/OASIS-CTI)

Technical Work Produced by the Committee

This Committee has not produced technical work yet.

Expository Work Produced by the Committee

There are no approved expository work products for this TC yet.

External Resources

Although not produced by the OASIS CTI TC, the following information offers useful insights into its work:

- News about STIX, TAXII, CybOX, and MAEC (http://stixproject.tumblr.com/)
- Implementations: Support for STIX/TAXII (http://stixproject.github.io/supporters/)
- STIX/TAXII Standards Transition FAQ (https://stixproject.github.io/oasis-faq.pdf)

Mailing Lists and Comments

cti: the discussion list used by CTI TC members to conduct Committee work. TC membership (http://www.oasis-open.org/committees/join.php?wg_abbrev=cti) is required to post, and TC members (http://www.oasis-open.org/committees/membership.php?wg_abbrev=cti) are automatically subscribed. The public may view the OASIS list archives (http://lists.oasis-open.org/archives/cti/) , also mirrored by MarkLogic at MarkMail.org (http://markmail.org/browse/org.oasis-open.lists.cti) .

cti-publicmirror: a read-only public mirror of the CTI TC discussion list. Anyone may subscribe to this list by sending an email subscription request (a blank message) to cti-publicmirror-subscribe@lists.oasis-open.org (mailto:cti-publicmirror-subscribe@lists.oasis-open.org)

cti-users: a public forum for asking questions, offering answers, and discussing topics of interest on STIX, TAXII, and CybOX. Users and developers of solutions that leverage those cybersecurity specifications are invited to participate. Anyone may subscribe to this list by sending an email subscription request (a blank message) to cti-users-subscribe@lists.oasis-open.org (mailto:cti-users-subscribe@lists.oasis-open.org) . The public may view the OASIS list archives (http://lists.oasis-open.org/archives/cti-users/) , also mirrored by MarkLogic at MarkMail.org (http://markmail.org/browse/org.oasis-open.lists.cti-users)

cti-stix-publicmirror: a read-only public mirror of the CTI STIX Subcommittee (https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=cti-stix) discussion list. Anyone may subscribe to this list by sending an email subscription request (a blank message) to cti-stix-publicmirror-subscribe@lists.oasis-open.org (mailto:cti-stix-publicmirror-subscribe@lists.oasis-open.org)

cti-taxii-publicmirror: a read-only public mirror of the CTI TAXII Subcommittee (https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=cti-taxii) discussion list. Anyone may subscribe to this list by sending an email subscription request (a blank message) to cti-taxii-publicmirror-subscribe@lists.oasis-open.org (mailto:cti-taxii-publicmirror-subscribe@lists.oasis-open.org)

cti-cybox-publicmirror: a read-only public mirror of the CTI CybOX Subcommittee (https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=cti-cybox) discussion list. Anyone may subscribe to this list by sending an email subscription request (a blank message) to cti-cybox-publicmirror-subscribe@lists.oasis-open.org (mailto:cti-

cybox-publicmirror-subscribe@lists.oasis-open.org)

cti-comment: a public mailing list for providing feedback on the technical work of the OASIS CTI TC. Send a comment (http://www.oasis-open.org/committees/comments/form.php?wg_abbrev=cti) or view the OASIS comment list archives (http://lists.oasis-open.org/archives/cti-comment/) , also mirrored by MarkLogic at MarkMail.org (http://markmail.org/browse/org.oasis-open.lists.cti-comment) .

Press Coverage and Commentary

- "United we stand: Protecting against cyber threats with standards for sharing" (https://www.internetac.org/archives/2328) ; *OECD ITAC News*, 27 Jul 2015
- "DHS Transitions STIX, TAXII and CybOX Standards to OASIS" (http://darkmatters.norsecorp.com/2015/07/29/dhs-transitions-stix-taxii-and-cybox-standards-to-oasis/) ; *DarkMatters*, 29 July 2015
- "OASIS Advances Automated Cyber Threat Intelligence Sharing with STIX, TAXII, CybOX (https://www.oasis-open.org/news/pr/oasis-advances-automated-cyber-threat-intelligence-sharing-with-stix-taxii-cybox) "; *Boeing, Check Point, Cisco, Dell, EMC, eSentire, Fortinet, Fujitsu, IBM, iboss, iSIGHT Partners, NEC, New Context, Palo Alto Networks, Resilient, Securonix, Soltra, TELUS, ThreatQuotient, ThreatStream, TruSTAR, US DHS Office of Cybersecurity and Communications, US NIST, ViaSat, and Others Collaborate on International Standards to Prevent and Defend Against Cyber Attack*; 17 July 2015

Additional Information

Providing Feedback: OASIS welcomes feedback (/committees/comments/index.php?wg_abbrev=cti) on its technical activities from potential users, developers, and others to better assure the interoperability and quality of OASIS work.