cti message

[Date Prev] | [Thread Prev] | [Thread Next] | [Date Next] -- [Date Index] | [Thread Index] | [List Home]

Subject: Call for Participation: OASIS Cyber Threat Intelligence (CTI) Technical Committee

- *From*: Chet Ensign <chet.ensign@oasis-open.org>
- *To*: tc-announce@lists.oasis-open.org, members@lists.oasis-open.org, cti@lists.oasis-open.org
- *Date*: Wed, 20 May 2015 19:28:36 -0400

OASIS members & interested parties,

A new OASIS Technical Committee is being formed. The OASIS Cyber Threat Intelligence (CTI) Technical Committee (TC) has been proposed by the members of OASIS listed in the charter below. The TC name, statement of purpose, scope, list of deliverables, audience, IPR mode and language specified in the proposal will constitute the TC's official charter. Submissions of technology for consideration by the TC, and the beginning of technical discussions, may occur no sooner than the TC's first meeting.

The eligibility requirements for becoming a participant in the TC at the first meeting are:

(a) you must be an employee or designee of an OASIS member organization or an individual member of OASIS, and

(b) you must join the Technical Committee, which members may do by using the Roster "join group: link on the TC's web page at [a].

To be considered a voting member at the first meeting:

(a) you must join the Technical Committee at least 7 days prior to the first meeting (on or before 12 June 2015) and

(b) you must attend the first meeting of the TC, at the time and date fixed below (18 June 2015).

Participants also may join the TC at a later time. OASIS and the TC welcomes all interested parties.

Non-OASIS members who wish to participate may contact us about joining OASIS [b]. In addition, the public may access the information resources maintained for each TC: a mail list archive, document repository and public comments facility, which will be linked from the TC's public home page at [c].

Please feel free to forward this announcement to any other appropriate lists. OASIS is an open standards organization; we encourage your participation.

----

[a] https://www.oasis-open.org/apps/org/workgroup/cti/

[b] See http://www.oasis-open.org/join/

[c] http://www.oasis-open.org/committees/cti/

CALL FOR PARTICIPATION
OASIS Cyber Threat Intelligence (CTI) Technical Committee Charter

The charter for this TC is as follows.

Section 1: TC Charter

(1)(a) TC Name

OASIS Cyber Threat Intelligence (CTI) Technical Committee

(1)(b) Statement of Purpose

Traditional approaches for cyber security that focus inward on understanding and addressing vulnerabilities, weaknesses, and configurations are necessary but insufficient in today's dynamic cyber landscape. Effective defense against current and future threats also requires the addition of an outward focus on understanding the adversary's behavior, capability, and intent. Only through a balanced understanding of both the adversary and ourselves can we understand enough about the true nature of the threats we face to make intelligent defensive decisions. The development of this understanding is known as cyber threat intelligence (CTI).

Cyber threat intelligence itself poses a challenge in that no single organization can have enough information to create and maintain accurate situational awareness of the threat landscape. This limitation is overcome by sharing of relevant cyber threat information among trusted partners and communities. Through information sharing, each sharing partner can achieve a more complete understanding of the threats they face and how to defeat them.

The purpose of the Cyber Threat Intelligence (CTI) Technical Committee is to define a set of information representations and protocols to address the need to model, analyze, and share cyber threat intelligence. A composable set of information sharing services will be defined to enable peer-to-peer, hub and spoke, and source subscriber threat intelligence sharing models. These services will not dictate one architecture, but strive to allow for organizations to develop standards-based sharing architectures that meet their needs. Standardized representations will be developed for campaigns, threat actors, incidents, tactics techniques and procedures (TTPs), indicators, exploit targets, observables, and courses of action. These core components and their inter-relationships together will enable robust cyber threat analysis and intelligence sharing.

The TC will base its efforts on the Structured Threat Information _expression_ (STIX) and Trusted Automated Exchange of Indicator Information (TAXII) specifications developed and contributed to the TC by U.S. Department of Homeland Security (DHS). Prior to creation of the CTI TC, the STIX and TAXII initiatives have been led by DHS through development based on open community collaboration. STIX and TAXII, as well as STIX's dependent specification of Cyber Observable _expression_ (CybOX), have already achieved significant international adoption among threat intelligence vendors, end-user organizations, and cyber threat information sharing communities.

By building upon the success of these existing specifications, the CTI TC can offer immediate value as well as provide a solid foundation on which to base future development.

(1)(c) Scope

In order to leverage existing value of STIX/TAXII/CybOX in the CTI community while working towards future capabilities and advancements, the OASIS CTI TC work will be divided into two phases: in phase one, existing input specifications contributed by the United States Department of Homeland Security (DHS) will be formally codified as OASIS specifications. In the second phase, continued development of STIX, TAXII, and CybOX will begin based on the needs identified by the CTI TC Members.

Phase One Scope:

* Specifications identified in Section (2)(h) (STIX 1.2, TAXII 1.1, and CybOX 2.1) will be contributed to the OASIS CTI TC by DHS

* The TC will use these contributions as the basis for corresponding OASIS Standards Track Work Products. A key objective of the TC will be to limit changes to the input specifications in order to minimize impacts on existing implementations

* The OASIS CTI TC will develop the specifications under the OASIS TC Process with the goal of submitting them at the appropriate time to the membership of the organization for consideration as OASIS Standards

Other contributions will be accepted for consideration without any prejudice or restrictions and evaluated based on technical merit insofar as they conform to this charter.

Phase Two Scope:

Phase two will take the specifications defined in phase one and evolve them under the direction of the OASIS CTI TC. Further work related to information representations for codifying, analyzing, or sharing of cyber threat intelligence that was not included in the input specifications is also in scope.

In addition to Standards Track Work Products, the OASIS CTI TC work products in both phase one and phase two may include supporting documentation, open source tooling, and any other materials deemed necessary to encourage the adoption of the TC's specifications.

(1)(d) Deliverables

The OASIS CTI TC will establish three Subcommittees to develop and refine the specifications and supporting materials of the TC:

* The STIX Subcommittee
* The TAXII Subcommittee
* The CybOX Subcommittee

In phase one, each Subcommittee will submit initial draft deliverables to the OASIS CTI TC for approval based on making minimal changes to the input specification as necessary conform to OASIS publication formats and support OASIS CTI TC design requirements:

* The STIX Subcommittee will submit STIX 1.2.1
* The TAXII Subcommittee will submit TAXII 1.1.1
* The CybOX Subcommittee will submit CybOX 2.1.1

In phase two, the OASIS CTI TC will make substantive additions and other changes to the specifications to correct errors and evolve capabilities based on requirements and capabilities identified by OASIS TC members. Deliverables will include updated versions of the specifications (STIX, TAXII, CybOX, and possibly others) as deemed appropriate by the Subcommittees and by the OASIS CTI TC as a whole.

In addition to the specification deliverables, the OASIS CTI TC may deliver supporting documentation and open source tooling on an ongoing basis in support of the CTI TC's published standards.

(1)(e) IPR Mode

This TC will operate under the Non-Assertion IPR mode as defined in Section 10.3 of the OASIS IPR Policy document.

(1)(f) Audience

The anticipated audience for this work includes:

* Vendors of products and services that produce, consume, or process cyber threat intelligence, in particular that which is expressed via STIX/CybOX and shared via TAXII

* Organizations that produce or consume cyber threat intelligence, in particular that which is expressed via STIX or CybOX and shared via TAXII

* Organizations that purchase or may purchase products that support STIX, TAXII, or CybOX

* Information Sharing and Analysis Organizations (ISAOs), including Information Sharing and Analysis Centers (ISACs)

(1)(g) Language

TC business will be conducted in English. The output documents will be written in (US) English. Translations to other languages may be made based on interest and ability.

Section 2: Additional Information

(2)(a) Identification of Similar Work

Similar efforts include:

* IODEF/RID/RID-T (RFC 5070, RFC 6545, RFC 6546): IODEF, RID, and RID-T are IETF specifications (https://tools.ietf.org/wg/mile/) to describe and share incident information. They have a much narrower scope than STIX/TAXII and therefore are often not adequate to most potential users of STIX/TAXII.

* OpenIOC (http://www.openioc.org): OpenIOC is a specification developed by FireEye (a commercial company) to describe Indicators of Compromise and made available for public use. OpenIOC addresses a narrow use case (observable patterns for Indicators of Compromise) and represents a partial solution to part of the overall cyber threat information problem, but does not fully address the needs of a holistic cyber threat intelligence information model. Additionally, though OpenIOC is developed as a public specification by FireEye it is not a consensus standard in an international standards body.

* VERIS (http://veriscommunity.net): The VERIS Framework is a set of metrics designed to provide a common language for describing security incidents. VERIS addresses a narrow use case and represents a partial solution to part of the overall cyber threat information problem but does not fully address the needs of a holistic cyber threat intelligence information model. Additionally, though VERIS is a published format

available on GitHub, it is developed at the sole discretion of the VERIS community rather than as a consensus standard in an international standards body.

* OMG Threat Modeling Working Group (http://www.omg.org/hot-topics/threat-modeling.htm): The Object Management Group (OMG) has issued a proposal for a combined risk-threat information model that incorporates STIX (among other things). That model is expected to cover a broader scope (cyber and physical, threat and risk) in order to coordinate across these domains but does not seek to re-define a model within the domain to the low level that STIX and CybOX do.

(2)(b) First TC Meeting

The first TC meeting will be held on 18 June 2015 at 17:00 UTC / 1:00 PM EDT / 10:00 AM PDT via teleconference. The teleconference infrastructure will be Microsoft Lync hosted by The MITRE Corporation.

(2)(c) Ongoing Meeting Schedule

The full OASIS CTI TC plans to meet monthly via a teleconference hosted via MITRE Lync. Subcommittees will set their own meeting schedules, initially meeting bi-weekly by teleconference hosted via MITRE Lync.

(2)(d) TC Proposers

* James Routh, Aetna, RouthJ@aetna.com

* Alexander Foley, Bank of America, alexander.foley@bankofamerica.com

* Yogesh Mudgal, Bloomberg L.P., ymudgal@bloomberg.net

* Bret Jordan, Blue Coat Systems Inc, bret.jordan@bluecoat.com

* Adnan Baykal, Center for Internet Security, Adnan.Baykal@cisecurity.org

* Jeff Williams, Dell, jeffrey_williams1@dell.com

* Richard Struse, Department of Homeland Security, Richard.Struse@hq.dhs.gov

* Robert Griffin, EMC/RSA, robert.griffin@rsa.com

* Joel J. Fleck, Hewlett-Packard, joel.fleck@hp.com

* Peter Allor, IBM, pallor@us.ibm.com

* Terry MacDonald, Individual member, terry.macdonald@threatloop.com

* Patrick Maroney, Individual member, pmaroney@specere.org

* Joep Gommers, Intelworks, joep@intelworks.com

* Pam Smith, Johns Hopkins University Applied Physics Laboratory (JHU/APL), pam.smith@jhuapl.edu

* Mark Moss, Johns Hopkins University Applied Physics Laboratory (JHU/APL), mark.moss@jhuapl.edu

* Terrence Driscoll, JPMorgan Chase, terrence.p.driscoll@jpmchase.com

* David Laurance, JPMorgan Chase, david.c.laurance@jpmorgan.com

* Paul McKitrick, Microsoft, pmckit@microsoft.com

* Sean Barnum, The MITRE Corporation, sbarnum@mitre.org

* Mark Davidson, The MITRE Corporation, mdavidson@mitre.org

* John Wunder, The MITRE Corporation, jwunder@mitre.org

* Vishaal Hariprasad, Palo Alto Networks, vhariprasad@paloaltonetworks.com

* Rick Howard, Palo Alto Networks, rhoward@paloaltonetworks.com

* Igor Baikalov, Securonix, ibaikalov@securonix.com

* Aharon Chernin, Soltra, achernin@soltra.com

* Richard Freeman, Symantec Corporation, richard_freeman@symantec.com

* Rob Walters, Symantec Corporation, Rob_Walters@symantec.com

* Chris Calvert, TELUS, Chris.calvert@telus.com

* Nick Deshpande, TELUS, Nick.Deshpande@telus.com

* Jayson Henkel, TELUS, Jayson.Henkel@telus.com

* Greg Reaume, TELUS, Greg.reaume@telus.com

* Alan Steer, TELUS, Alan.Steer@telus.com

* Tyron Miller, Threat Intelligence Pty Ltd, ty.miller@threatintelligence.com

* Andrew van der Stock, Threat Intelligence Pty Ltd, andrew.vanderstock@threatintelligence.com

* Wei Huang, ThreatStream, wei.huang@threatstream.com

* Hugh Njemanze, ThreatStream, hugh.njemanze@threatstream.com

* Adam Cooper, UK Cabinet Office, adam.cooper@digital.cabinet-office.gov.uk

* Chris O' Brien, UK Cabinet Office, COBrien@cert.gov.uk

* Mona Magathan, US Bancorp, mona.magathan@usbank.com

* Mark Angel, US Bancorp, mark.angel@usbank.com

* Chris Houser, Wells Fargo, Christopher.Houser@wellsfargo.com

* Tony Rutkowski, Yaana Technologies, LLC, tony@yaanatech.com

(2)(e) Primary Representatives' Support

* Eileen Bridges, BridgesE@Aetna.com: As Aetna's Primary Representative to OASIS, I confirm our support for the OASIS Cyber Threat Intelligence (CTI) Technical Committee charter and our intention to participate in the TC.

* I Abbie Barbir, abbie.barbir@bankofamerica.com, Bank of America primary rep approve adding Alexander Foley as a co-proposer of the OASIS Cyber Threat Intelligence (CTI) Technical Committee.

* I, Kevin Fleming, kpfleming@bloomberg.net, as Bloomberg's Primary Representative

to OASIS, confirm our support for the OASIS Cyber Threat Intelligence (CTI) Technical Committee charter and the participation of Yogesh Mudgal in the TC's formation.

* I, Bret Jordan, bret.jordan@bluecoat.com, as the Blue Coat Systems Primary Representative at OASIS, confirm our support for the proposed OASIS Cyber Threat Intelligence (CTI) Technical Committee charter and endorse our participation as a TC Proposer.

* I, Adnan Baykal, Adnan.Baykal@cisecurity.org, as Primary Representative for the Center for Internet Security approve the CTI TC Charter, and endorse the participation of our proposers listed in (2)(d).

* Ken Blackwell, Ken.Blackwell@software.dell.com: As Dell's Primary Representative to OASIS, I confirm our support for the OASIS Cyber Threat Intelligence (CTI) Technical Committee charter and our intention to participate in the TC. Jeff will be our representative on this committee.

* I, Richard Struse, Richard.Struse@hq.dhs.gov, as the US Department of Homeland Security Office of Cybersecurity and Communications Primary Representative to OASIS, I confirm our support for the proposed OASIS Cyber Threat Intelligence (CTI) Technical Committee charter and endorse our participation as a TC Proposer.

* I, Rob Philpott, robert.philpott@rsa.com, as EMC/RSA's Primary Representative to OASIS, confirm our support for the OASIS Cyber Threat Intelligence (CTI) Technical Committee charter and the participation of our proposer named above.

* As principal representative of Hewlett-Packard at OASIS, I, Joel J. Fleck, joel.fleck@hp.com, am pleased to endorse the creation of a new OASIS Technical Committee on Cyber Threat Intelligence to support, maintain and advance the work on the specifications for the STIX/TAXII protocols.

* I, Dave Ings, ings@ca.ibm.com, as IBM's Primary Representative to OASIS, confirm our support for the proposed OASIS Cyber Threat Intelligence (CTI) Technical Committee charter and support our participants as listed above.

* Raymon van der Velde, Intelworks, raymon@intelworks.com: As Intelwork's Primary Representative to OASIS, I confirm our support for the OASIS Cyber Threat Intelligence (CTI) Technical Committee charter and our intention to participate in the TC.

* I, Tom Smith, tom.smith@jhuapl.edu, as Primary Representative for Johns Hopkins University Applied Physics Laboratory, approve the OASIS Cyber Threat Intelligence Technical Committee Charter, and endorse our proposer, Pam Smith, as listed in (2)(d).

* I, Allan Beck, allan.beck@jpmorgan.com, as JP Morgan Chase Bank's Primary Representative to OASIS, confirm our support for the proposed OASIS Cyber Threat Intelligence (CTI) Technical Committee charter and support our participants as listed above.

* I, Ram Jeyaraman, Ram.Jeyaraman@microsoft.com, as Primary Representative for Microsoft Corporation approve the OASIS Cyber Threat Intelligence Technical Committee Charter, and endorse our Proposer, Paul McKitrick, as listed in section (2)(d).

* I, Raj Rajagopal, rajagop@mitre.org, as Primary Representative for MITRE approve the CTI TC Charter, and endorse our participation as a TC Proposer.

* Rick Howard, Palo Alto Networks, rhoward@paloaltonetworks.com: As Palo Alto Networks' Primary Representative to OASIS, I confirm our company's support for the OASIS Cyber Threat Intelligence (CTI) Technical Committee charter and our intention to participate in the TC.

* Sharon Vardi, Securonix, svardi@securonix.com: As the Securonix Primary Representative to OASIS, I confirm Securonix's support for the OASIS Cyber Threat Intelligence (CTI) Technical Committee charter and our intention to participate in the TC.

* I, Aharon Chernin, achernin@soltra.com, as Primary Representative for Soltra approve the CTI TC Charter, and endorse all our proposers listed in (2)(d).

* I, Richard Freeman, richard_freeman@symantec.com, as Primary Representative for Symantec Corporation approve the CTI TC Charter, and endorse all our proposers listed in (2)(d). (2)(d) currently consists of myself and Rob Walters Rob_Walters@symantec.com.

* I, Andrew Johnston, andrew.johnston@telus.com, as Primary Representative for TELUS approve the CTI TC Charter, and endorse the participation of our proposers listed in (2)(d).

* Ty Miller,ty.miller@threatintelligence.com: As the Threat Intelligence Primary Representative to OASIS, I confirm our company’ s support for the OASIS Cyber Threat Intelligence Technical Committee charter and our intention to participate in the TC.

* Hugh Njemanze, hugh.njemanze@threatstream.com: As the ThreatStream primary representative to OASIS, I confirm our company’ s support for the OASIS Cyber Threat Intelligence Technical Committee charter and our intention to participate in the TC.

* David Barnes, david.barnes@cabinet-office.x.gsi.gov.uk: As the UK Cabinet Office's Primary Representative to OASIS, I confirm our support for the OASIS Cyber Threat Intelligence (CTI) Technical Committee charter and our intention to participate in the TC.

* As the US Bancorp's Primary Representative at OASIS, I, Mona Magathan, mona.magathan@usbank.com, confirm our support for the proposed OASIS Cyber Threat Intelligence (CTI) Technical Committee charter and endorse our participation as a TC Proposer.

* Garrett N. Macey, Garrett.N.Macey@wellsfargo.com: As Wells Fargo's Primary Representative to OASIS, I confirm our support for the OASIS Cyber Threat Intelligence (CTI) Technical Committee charter and our intention to participate in the TC.

* I, Anthony M. Rutkowski, tony@yaanatech.com, as Primary Representative for Yaana Technologies, LLC, approve the OASIS Cyber Threat Intelligence (CTI) Technical Committee Charter, support this proposal of formation together with the other proposers and are committed to the Charter and projected meeting schedule.

(2)(f) TC Convener

The TC Convener is Richard Struse of the U.S. Department of Homeland Security, Richard.Struse@hq.dhs.gov.

(2)(g) OASIS Member Section

N/A

(2)(h) Anticipated Contributions

The U.S. Department of Homeland Security will contribute the following materials, delivered by the Homeland Security Systems Engineering and Development Institute (operated by The MITRE Corporation):

* STIX 1.2
  - The specification itself, including specification documents, UML, and schemas: http://stix.mitre.org/language/version1.2/
  - Supporting non-normative documentation: http://stixproject.github.io
  - Sample documents: http://stix.mitre.org/language/version1.2/samples.html
  - Profiles and Profile Documentation: http://stix.mitre.org/language/profiles.html
  - Open source tools and utilities: http://github.com/STIXProject/

* TAXII 1.1
  - The specification itself, including specification documents and schemas: http://taxii.mitre.org/specifications/version1.1/
  - Supporting non-normative documentation: http://taxiiproject.github.io
  - Open source tools and utilities: http://github.com/TAXIIProject/

* CybOX 2.1
  - The specification itself, including specification documents, UML, and schemas: http://cybox.mitre.org/language/version2.1/
  - Supporting non-normative documentation: http://cyboxproject.github.io
  - Open source tools and utilities: http://github.com/CybOXProject/

(2)(i) FAQ Document

https://stixproject.github.io/oasis-faq.pdf

(2)(j) Work Product Titles and Acronyms

The OASIS CTI TC will produce material related to the following work products:

* Structured Threat Information _expression_ (STIX)
* Trusted Automated Exchange of Indicator Information (TAXII)
* Cyber Observable _expression_ (CybOX)

--

/chet

Chet Ensign
Director of Standards Development and TC Administration
OASIS: Advancing open standards for the information society
http://www.oasis-open.org

Primary: +1 973-996-2298
Mobile: +1 201-341-1393

[Date Prev] | [Thread Prev] | [Thread Next] | [Date Next] -- [Date Index] | [Thread Index] | [List Home]