A Funny Thing Happened On The Way To OASIS: From Specifications to Standards

Richard Struse
Chief Advanced Technology Officer, NCCIC
US Department of Homeland Security
Disclaimer

This presentation is intended for informational and discussion purposes only.

The Department of Homeland Security (DHS) does not provide any warranties of any kind regarding this information. In no event shall the United States Government or its contractors or subcontractors be liable for any damages, including but not limited to, direct, indirect, special or consequential damages, arising out of, resulting from, or in any way connected with this information, whether or not based upon warranty, contract, tort, or otherwise, whether or not arising out of negligence, and whether or not injury was sustained from, or arose out of the results of, or reliance upon the information.

The display of the DHS official seal or other DHS visual identities, including the US-CERT or ICS-CERT name or logo shall not be interpreted to provide any person or organization the authorization to use the official seal, insignia or other visual identities of the Department of Homeland Security, including US-CERT and ICS-CERT. The DHS seal, insignia, or other visual identities shall not be used in any manner to imply endorsement of any commercial product or activity by DHS, US-CERT, ICS-CERT or the United States Government. Use of the DHS seal without proper authorization violates federal law (e.g., 18 U.S.C. §§ 506, 701, 1017), and is against DHS policies governing usage of its seal.

This presentation is Traffic Light Protocol (TLP): WHITE. Recipients may share TLP: WHITE information without restriction, subject to copyright controls. For more information on the TLP, see http://www.us-cert.gov/tlp.

DHS does not endorse any commercial product or service, including any subjects of analysis. Any reference to specific commercial products, processes, or services by service mark, trademark, manufacturer, or otherwise, does not constitute or imply their endorsement, recommendation, or favoring by DHS.
Our Goal...

Create an ecosystem where actionable cyber threat intelligence is automatically shared in real-time to enable real-time defense – the detection, prevention and mitigation of cyber threats \textit{before or as they occur}\footnote{The TAXII and STIX logos are included.}
My Detection Becomes Your Prevention
Malicious Code enters a network of sharing communities.

“Unaware” nodes are vulnerable to continued attacks.
Remember those nodes? The chain of information continues until all nodes are safe from that attack. Malicious code enters again and attempts an attack. With the nodes now protected, the attack is thwarted. The first node hit shares information about the attack with other nodes.
Guiding Principles: STIX and TAXII

1. Early and consistent engagement with the private sector, especially critical infrastructure

2. Leverage US Government’s position to move the marketplace further, faster than it would otherwise

3. Iterative approach focused on delivering early value and rapid transition to practice

4. Demonstrate value first and then pursue standardization

5. Ensure today’s problems are being solved while providing a path for future evolution
Turning Back Time: 2011

• Standards for cybersecurity information sharing in existence were not being used for sharing between communities.
• Standards that were in use emphasized structure for exchange, but not automated operation.
• Standards were also focused on particular types of incidents and/or abuse notifications.
• Threat actors, tactics/techniques/procedures (TTPs), campaigns, or courses of action were not easily expressed
Timeline: 2012 - 2015

**September 2012:**
STIX 0.5 Released

**December 2012:**
STIXProject and TAXIIProject code repositories made available via GitHub

**January 2012:**
Initial Concept for TAXII

**June 2012:**
STIX 0.3 Released

**November 2012:**
TAXII 1.0 Draft Published for Comment

**April 2013:**
STIX 1.0 and TAXII 1.0 Released

**October 2013:**
STIX 1.0.1 Released

**February 2014:**
STIX 1.1 Released

**February 2015:**
Executive Order Promoting Private Sector Information Sharing

**June 2014:**
Microsoft announces Interflow

**January 2014:**
TAXII 1.1 Released

**July 2013:**
Microsoft Active Protections Program Announces Plan to Support STIX and TAXII

**September 2014:**
FS-ISAC announces Soltra

**April 2015:**
STIX and TAXII going to OASIS

**June 2015:**
First meeting of the OASIS CTI Technical Committee

**May 2015:**
STIX 1.2 Released
2012: Inception

**SEPTEMBER 2012:**
STIX 0.5 Released

**DECEMBER 2012:**
STIXProject and TAXIIProject code repositories made available via GitHub

**JANUARY 2012:**
Initial Concept for TAXII

**JUNE 2012:**
STIX 0.3 Released

**NOVEMBER 2012:**
TAXII 1.0 Draft Published for Comment

**APRIL 2013:**
STIX 1.0 and TAXII 1.0 Released

**OCTOBER:**
STIX 1.0
2013: Realization

- **APRIL 2013:** STIX 1.0 and TAXII 1.0 Released
- **OCTOBER 2013:** STIX 1.0.1 Released
- **FEBRUARY 2014:** STIX 1.1 Released
- **JUNE 2012:** STIX 0.3 Released
- **JANUARY 2012:** Initial Concept for TAXII
- **NOVEMBER 2012:** TAXII 1.0 Draft Published for Comment
- **JULY 2013:** Microsoft Active Protections Program Announces Plan to Support STIX and TAXII
- **JUNE 2014:** Microsoft announces...
2014: Maturation

- **FEBRUARY 2014:** STIX 1.1 Released
- **JUNE 2014:** Microsoft announces Interflow
- **APRIL 2013:** STIX 1.0 and TAXII 1.0 Released
- **OCTOBER 2013:** STIX 1.0.1 Released
- **SEPTEMBER 2014:** FS-ISAC announces Soltra
- **APRIL 2015:** STIX and TAXII going to OASIS
- **JUNE 2015:** First meeting of the OASIS CTI Technical Committee
- **MAY 2015:** STIX 1.2 Released
- **FEBRUARY 2015:** Executive Order Promoting Private Sector Information Sharing
2015: Standardization

- **SEPTEMBER 2014:** FS-ISAC announces Soltra
- **APRIL 2015:** STIX and TAXII going to OASIS
  - First meeting of the OASIS CTI Technical Committee
- **MAY 2015:** STIX 1.2 Released
- **FEBRUARY 2015:**
  - Executive Order Promoting Private Sector Information Sharing
- **JUNE 2014:** Microsoft announces Interflow
- **FEBRUARY 2014:** STIX 1.1 Released
- **2013:** Released
Why international standardization?

We promised.
Since 2012, every DHS presentation on STIX and TAXII has stated our goal to “transition the specifications to an international standards body”

US law says we should.
National Technology Transfer and Advancement Act of 1995 directs the use of privately developed, voluntary standards.

It clears up intellectual property concerns.
All work developed in the standards body will be governed by non-assertion rules.
Why not *start* in a standards body?

You only want to standardize good things. Not every country’s national football team plays in the World Cup – not every good idea merits becoming an international standard.

Pre-emptively avoid creating conflict between *de facto* and *de jure* standards

*de facto* addressing vs. *de jure* name@domain

Standards bodies aren’t traditionally “agile” and can crystallize incomplete ideas

This is a *design feature* of SDOs
What is OASIS?

Non-profit consortium founded in 1993
- 5,000+ participants worldwide
- 600+ organizations & individuals in 100+ countries
- Home of 70+ Technical Committees and eight independent groups

Broad portfolio of standards:

Open, democratic, transparent
Why OASIS?

1. Won’t have to re-invent wheels: OASIS TCs demonstrated ability to acknowledge previously completed work as the starting point for OASIS standards.

2. OASIS membership looked very similar to the STIX/TAXII community: broader than just vendors of specific technologies; inclusive of NGOs, government bodies and consumer organizations.

3. Standards are provided free-of-charge in perpetuity, and must be verified by multiple Statements of Use.
Lessons Learned Along The Way

1. De facto is not de jure, and the difference matters.
2. Don’t expect that people are going to implement things from documentation. What are the fundamental building blocks people can re-use (like an API)?
3. Evangelize your community. Don’t assume the work speaks for itself.
4. Include customers early, in addition to vendors
5. Don’t assume the choice of how, when or where to standardize is obvious or easy. Seek diverse opinions from SDO veterans and the community.
OASIS CTI TC Members