Homeland
Security

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.

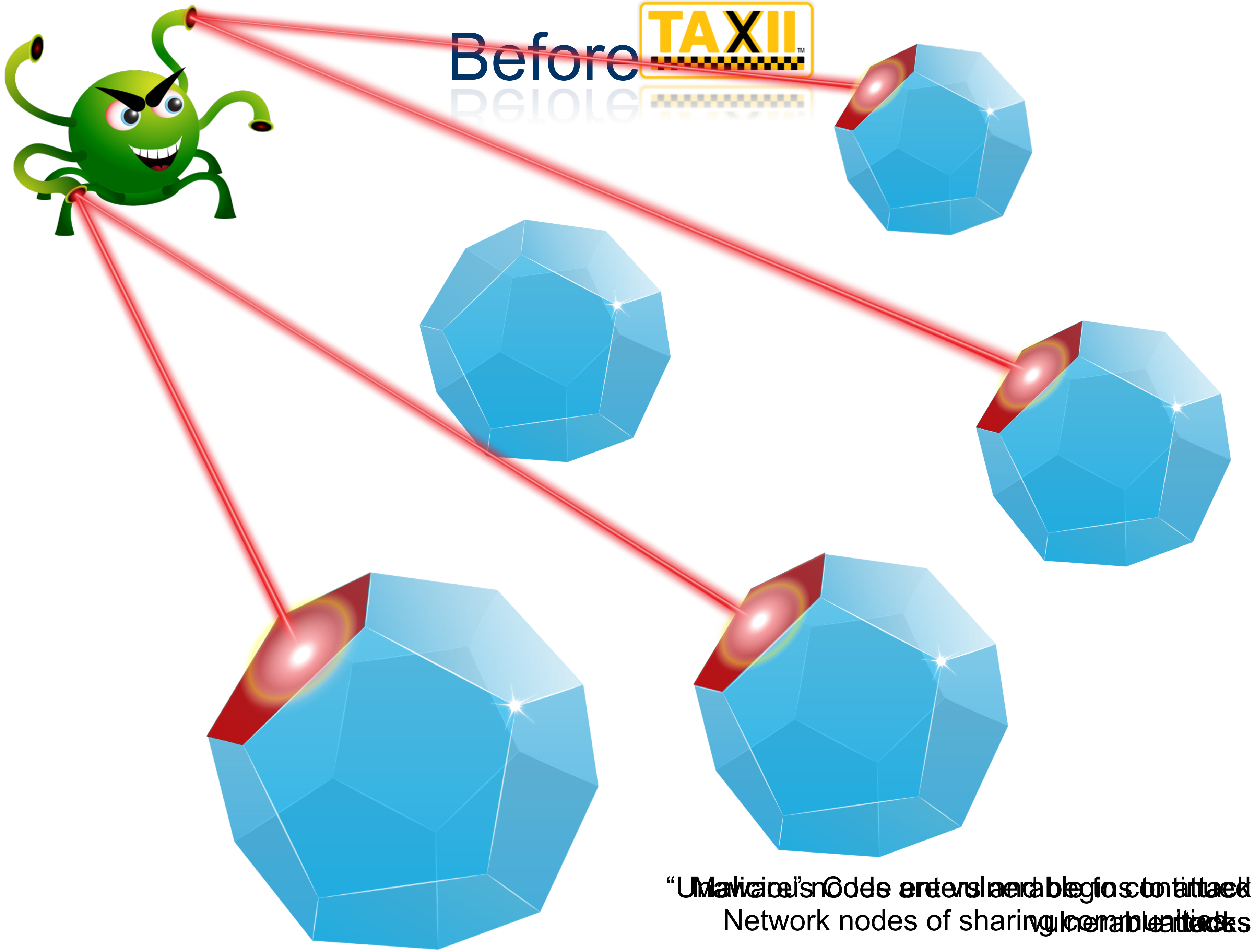
The display of the DHS official seal or other DHS visual identities, including the US-CERT or ICS-CERT name or logo shall not be interpreted to provide any person or organization the authorization to use the official seal, insignia or other visual identities of the Department of Homeland Security, including 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.

My Detection Becomes Your Prevention

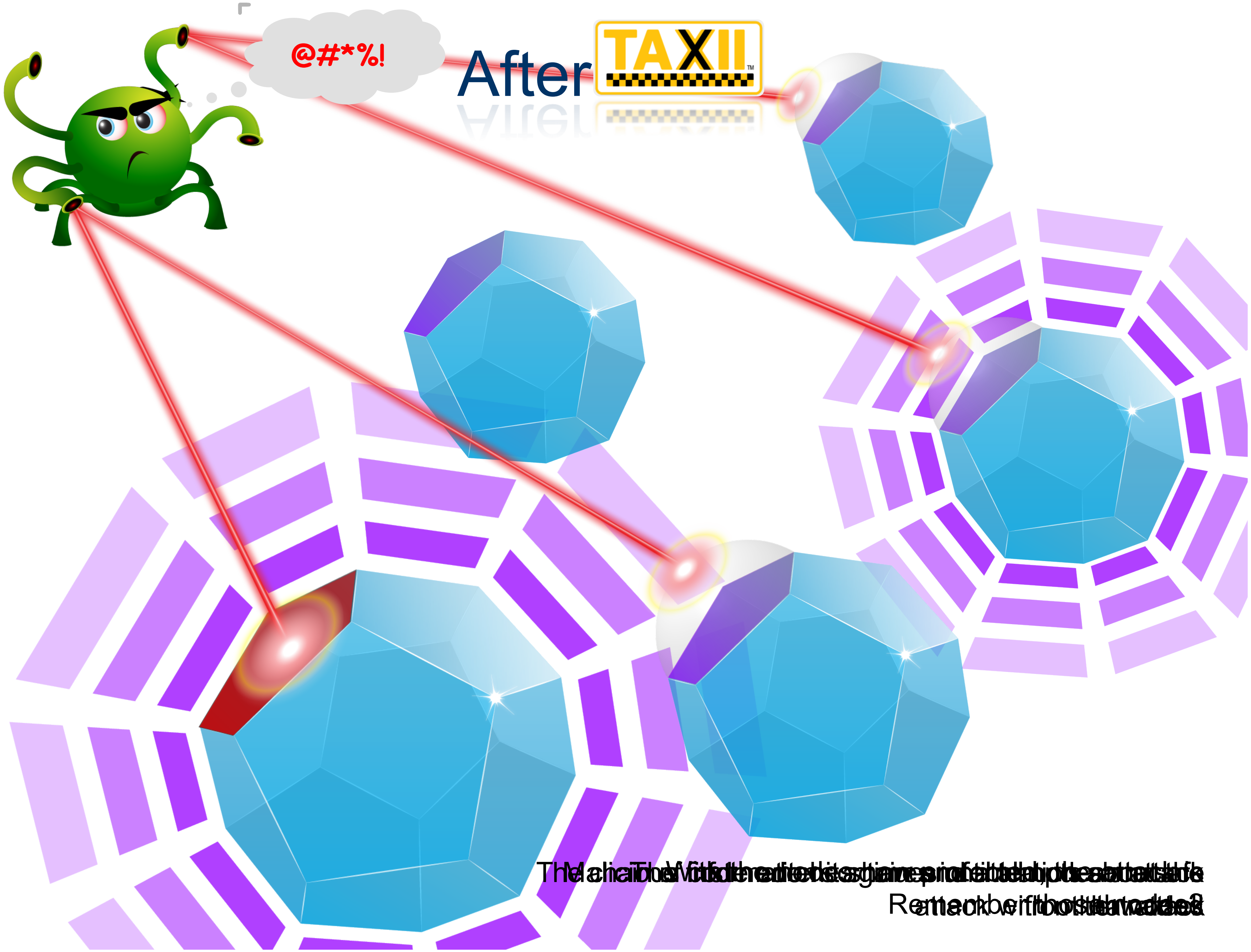
Before TAXII



Malicious Code enters and begins to attack
Network nodes of sharing communities

“Unaware’s” nodes are vulnerable to continued
vulnerable attacks

After TAXII



[illegible]

Remember [illegible]

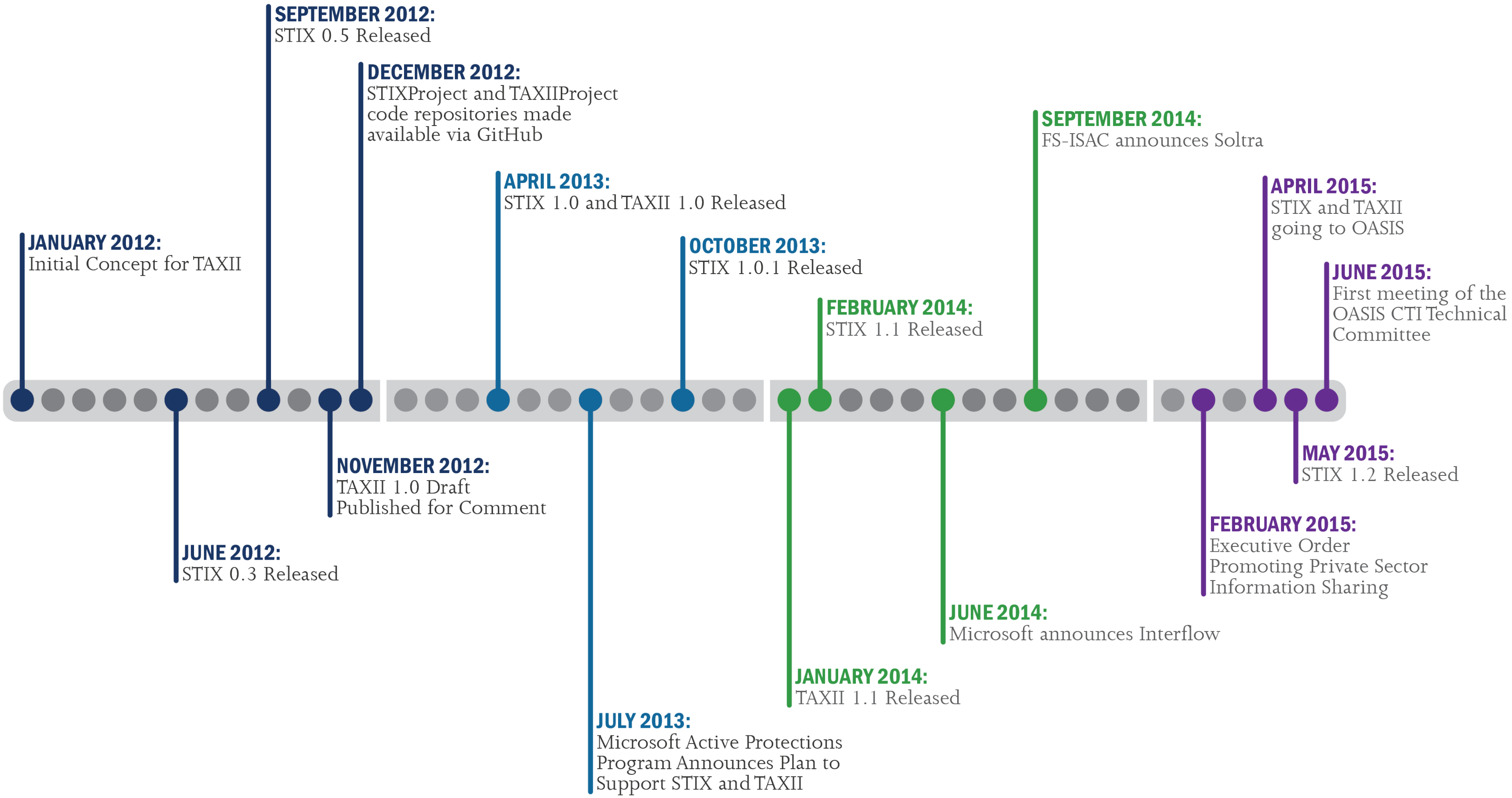
Concepts: STIX and TAXII

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



JANUARY 2012:
Initial Concept for TAXII

JUNE 2012:
STIX 0.3 Released

SEPTEMBER 2012:
STIX 0.5 Released

NOVEMBER 2012:
TAXII 1.0 Draft
Published for Comment

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

APRIL 2013:
STIX 1.0 and TAXII 1.0 Released

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

OCTOBER 2013:
STIX 1.0.1 Released

JANUARY 2014:
TAXII 1.1 Released

FEBRUARY 2014:
STIX 1.1 Released

JUNE 2014:
Microsoft announces Interflow

SEPTEMBER 2014:
FS-ISAC announces Soltra

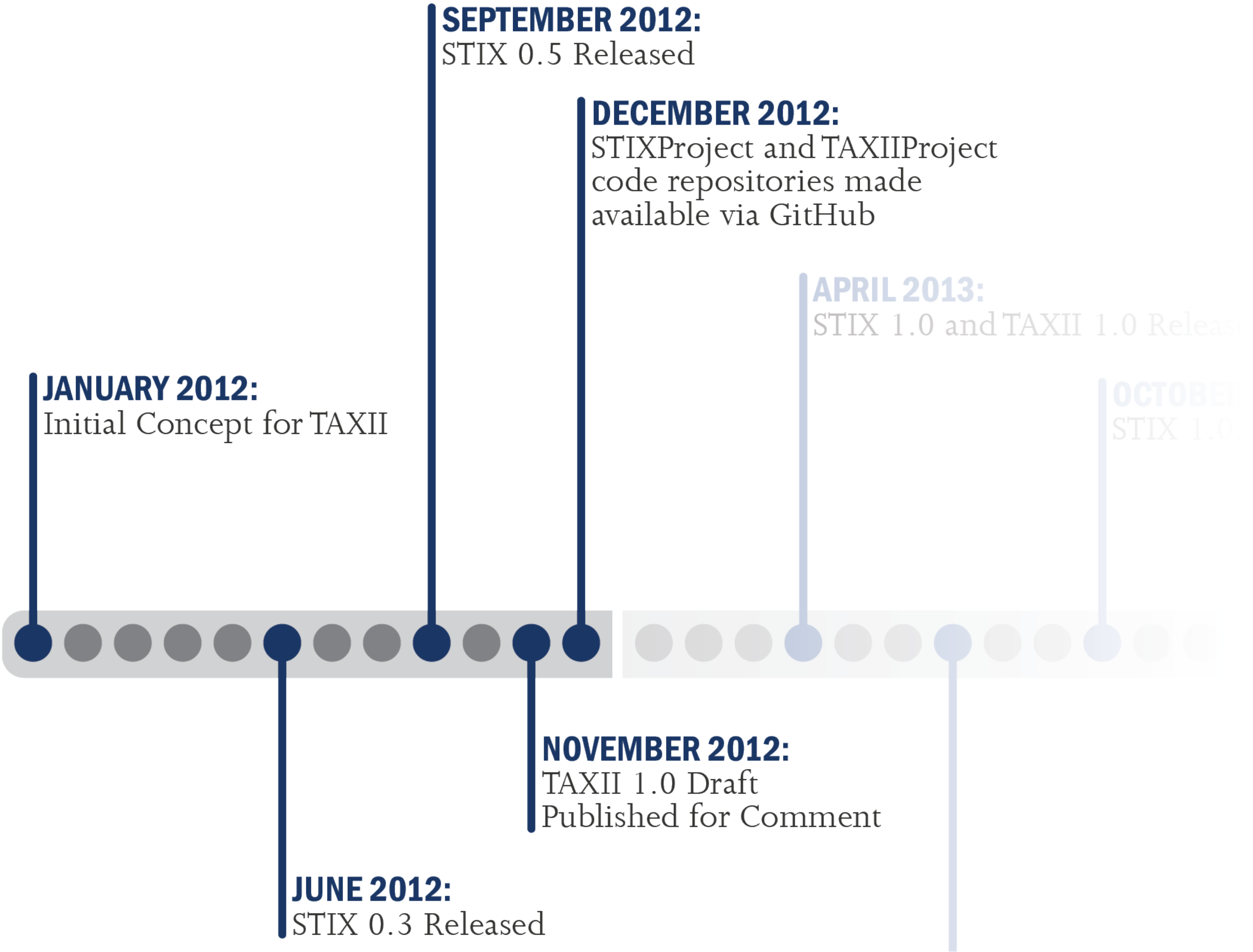
FEBRUARY 2015:
Executive Order
Promoting Private Sector
Information Sharing

APRIL 2015:
STIX and TAXII
going to OASIS

MAY 2015:
STIX 1.2 Released

JUNE 2015:
First meeting of the
OASIS CTI Technical
Committee

2012: Inception



JANUARY 2012:
Initial Concept for TAXII

JUNE 2012:
STIX 0.3 Released

SEPTEMBER 2012:
STIX 0.5 Released

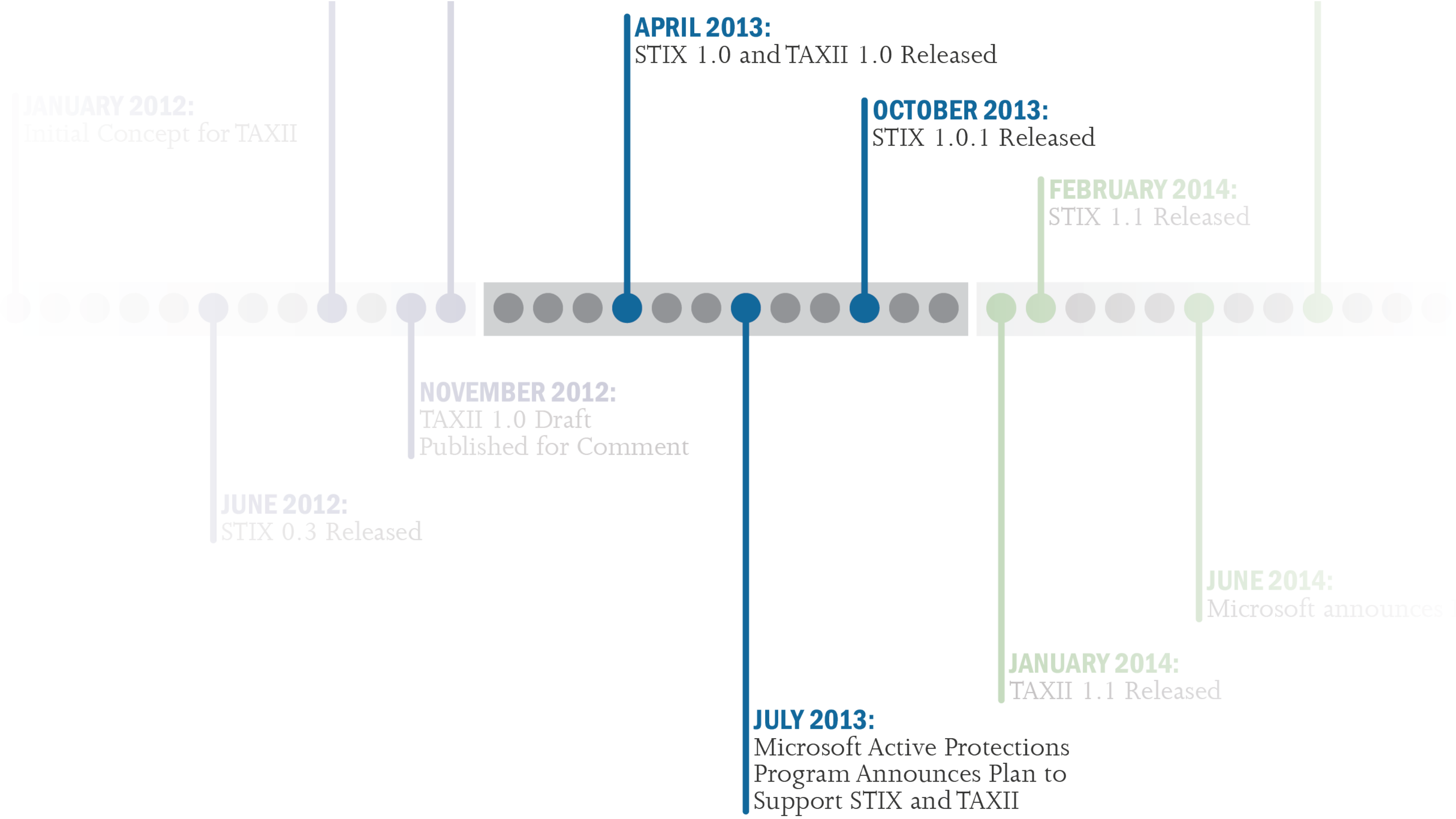
NOVEMBER 2012:
TAXII 1.0 Draft
Published for Comment

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

APRIL 2013:
STIX 1.0 and TAXII 1.0 Releas

OCTOBER
STIX 1.0

2013: Realization



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

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

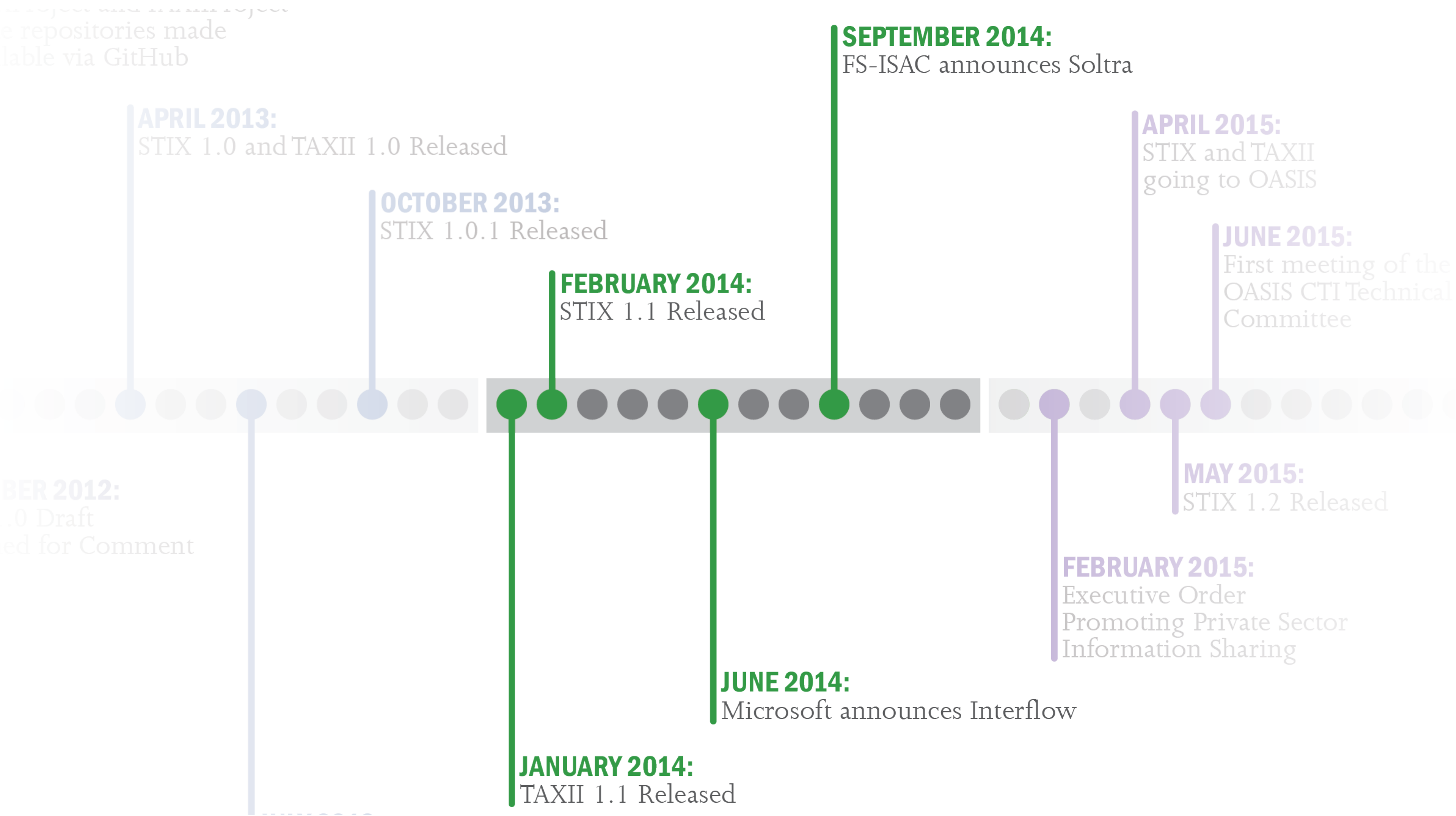
OCTOBER 2013:
STIX 1.0.1 Released

JANUARY 2014:
TAXII 1.1 Released

FEBRUARY 2014:
STIX 1.1 Released

JUNE 2014:
Microsoft announces

2014: Maturation



e repositories made
lable via GitHub

BER 2012:
0 Draft
ed for Comment

APRIL 2013:
STIX 1.0 and TAXII 1.0 Released

OCTOBER 2013:
STIX 1.0.1 Released

JANUARY 2014:
TAXII 1.1 Released

FEBRUARY 2014:
STIX 1.1 Released

JUNE 2014:
Microsoft announces Interflow

SEPTEMBER 2014:
FS-ISAC announces Soltra

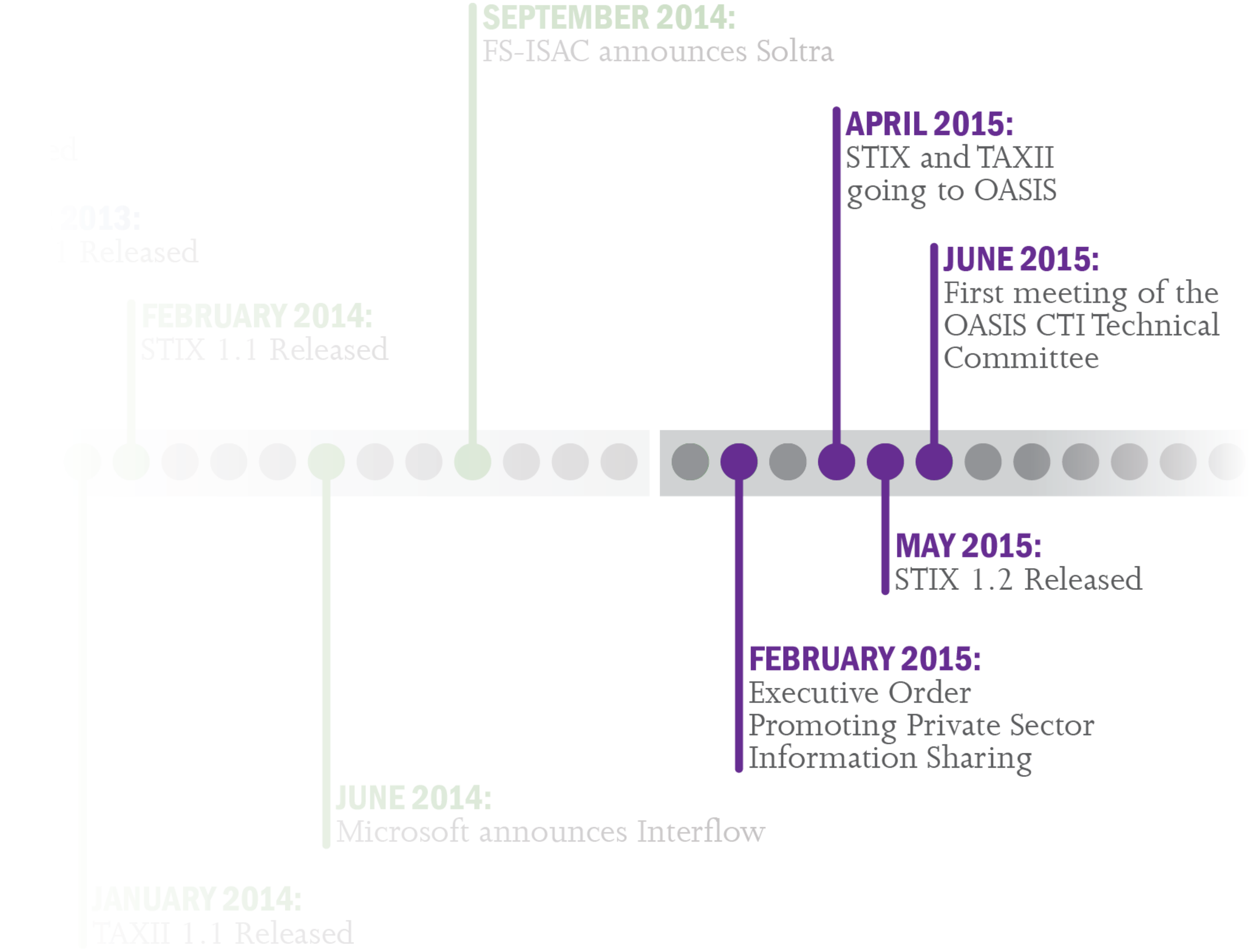
FEBRUARY 2015:
Executive Order
Promoting Private Sector
Information Sharing

APRIL 2015:
STIX and TAXII
going to OASIS

MAY 2015:
STIX 1.2 Released

JUNE 2015:
First meeting of the
OASIS CTI Technical
Committee

2015: Standardization



ed

2013:
1 Released

FEBRUARY 2014:
STIX 1.1 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

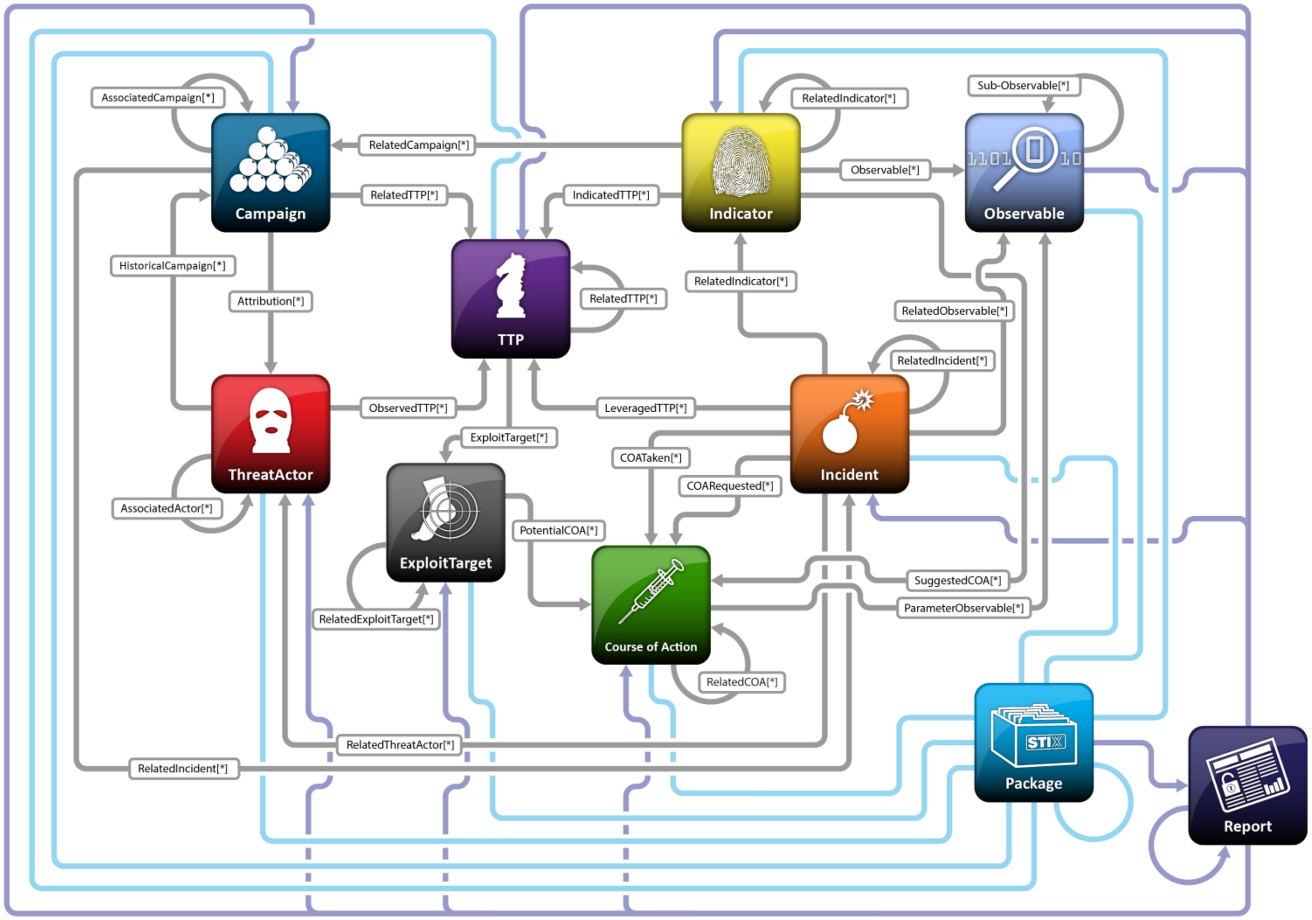
FEBRUARY 2015:
Executive Order Promoting Private Sector Information Sharing

JUNE 2014:
Microsoft announces Interflow

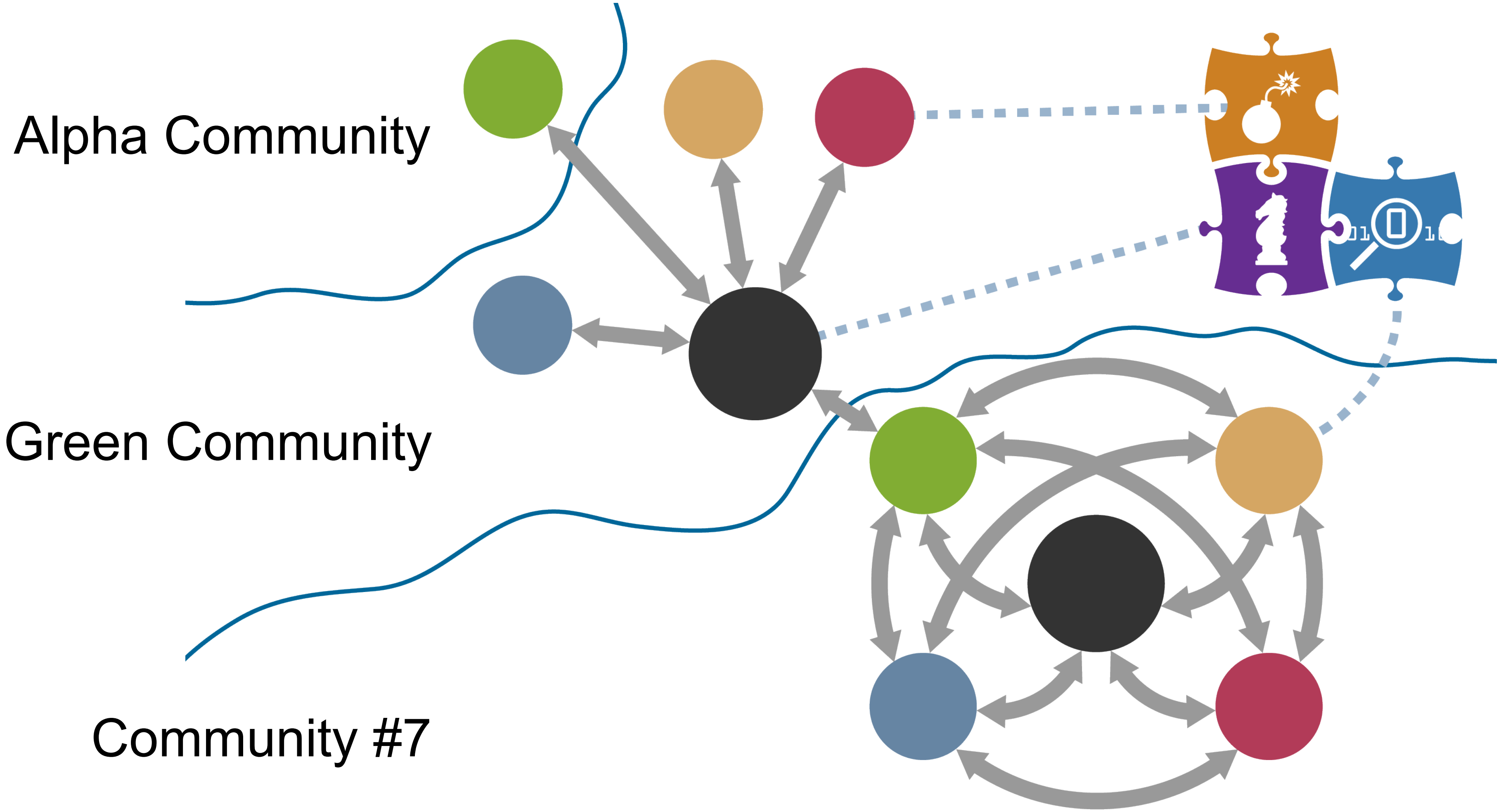
JANUARY 2014:
TAXII 1.1 Released

STIX: Today

Structured Threat Information eXpression (STIX) v1.1.1 Architecture



TAXII: Today



Alpha Community

Green Community

Community #7

Why international standardization?

1. We promised.

   Since 2012, every DHS presentation on STIX and TAXII has stated *“transition the specifications to an international standards body”*

2. US law says we should.

   National Technology Transfer and Advancement Act of 1995 directs the use of privately developed, voluntary standards.

3. 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?

1. 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.

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

   X.400 addressing vs. name@domain

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

   Alternatively, you can wind up with RSS

Standards Development Organizations (SDOs)

ITU-T

ITU-T produces standards covering all fields of telecommunications.

- Study Groups meet in person according to a calendar to develop Recommendations
- X.509 Public Key Encryption, H.323 family of VoIP standards

ISO/IEC

ISO develops IT standards for the global marketplace.

- Participation of 163 national standards bodies
- ISO 27001, Information Security Management Systems Requirements

W3C

W3C is the main standards organization for the Web.

- Members include universities, governments, companies and individuals
- HTML, CSS, XML, SVG, OWL, WSDL, SOAP, XQuery

IETF

IETF, part of the Internet Society, develops Internet standards, particularly those that comprise the Internet protocol suite.

- No formal voting; members can come from anywhere
- ICMP, UDP, TCP, IPv4, IPv6, DNS, SMTP

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:

Security, Privacy, Cloud, M2M, IoT, Content Technologies, Energy, eGov, Legal, Emergency Management, Finance, Big Data, Healthcare, & more

Open, democratic, transparent

OASIS in the international community

The EU classifies OASIS as “one of the top three ICT consortia.”

- EU Regulation 1025/2012 allows OASIS specifications to be referenced in public procurement.
- OASIS is a permanent member of EC’s European Multi-Stakeholder Platform on ICT Standardization.
- See www.oasis-open.org/liaisons for more.

ISO IEC ITU UN/CEFACT WORLD BANK European Union

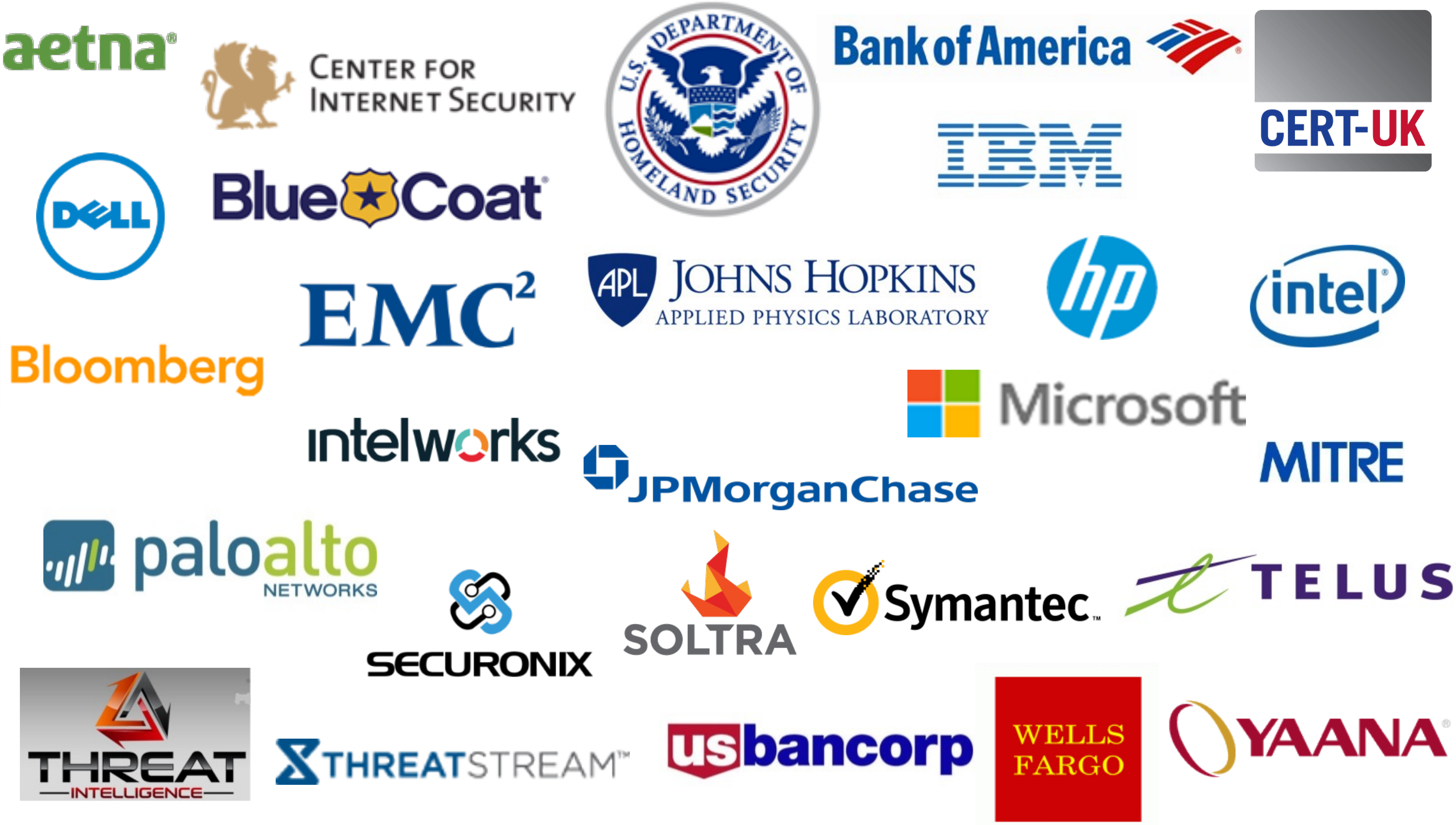
Why OASIS?

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. 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.

Breaking The Record: 27 Supporters



Questions?

Learn more about STIX and TAXII:

www.us-cert.gov/taxii

U.S. DEPARTMENT OF HOMELAND SECURITY

Homeland
Security