
We've built the plumbing …
STIX™
TAXII™

Homeland Security

Plumbing's Done! Now What Do We Do With All This Water?

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

Chair,
OASIS Cyber Threat Intelligence Technical Committee

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 *before or as they occur*

Is the Plumbing Really “Done”?

Sort of.

Significant progress towards creating a global ecosystem of automated cyber threat intelligence sharing

Existing versions of STIX/TAXII on their way to becoming true international standards

Implementations are out there but we are probably more at the “crawl” or “walk” stages than we are at “run”

Transition to OASIS

- Transition of STIX/TAXII/CybOX to OASIS Cyber Threat Intelligence (CTI) Technical Committee (TC) is complete
- OASIS CTI TC is the largest TC in OASIS history with over 200 members
- The CTI TC has begun the process of codifying the existing STIX/TAXII specifications as formal international standards
- CTI TC members are now hard at work on the future – STIX 2.0 and TAXII 2.0
- For more information: https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=cti

OASIS CTI Members

aetna

AIRBUS

AIT AUSTRIAN INSTITUTE OF TECHNOLOGY

ANZ

Bank of America

BlueCoat

BOEING

CENTER FOR INTERNET SECURITY

CenturyLink

CERT-UK

Check Point

CISCO

CITRIX

Cyber THREAT Intelligence Network

DELL

DTCC

eclectic iq

EMC²

esentire

FORTINET

FINANCIAL SERVICES ISAC

FUJITSU

GEORGETOWN UNIVERSITY

hp

IBM

iboss

IID

intel

iSIGHTPARTNERS

APL JOHNS HOPKINS APPLIED PHYSICS LABORATORY

JPMorganChase

KAISER PERMANENTE

Lumeta

MITRE

NCC

NEC

NEW CONTEXT

NAESB

paloalto NETWORKS

QUERALT

Raytheon

resilient SYSTEMS

R-CISC Retail Cyber Intelligence Sharing Center

SECURONIX

SIEMENS

SOLTRA

splunk>

Symantec

TELUS

THREAT INTELLIGENCE

THREATCONNECT

THREATQUOTIENT

THREATSTREAM

TRUSTAR TECHNOLOGY

usbancorp

VeriSign

ViaSat

YAANA

Making the plumbing better…

- CTI TC is incorporating lessons-learned from 3+ years of implementation to inform the evolution of STIX 2.0, TAXII 2.0 and CybOX 2.0
- Key takeaways:
  - STIX and CybOX complexity often an issue – refactoring to reduce complexity
  - XML is a barrier for many developers – JSON is the new mandatory to implement (MTI) representation
  - TAXII specification will be expanded to better define services to promote interoperability

STIX/TAXII in Practice

- Foundation for DHS Automated Indicator Sharing (AIS) initiative enabling bi-directional indicator exchange between the USG and the private sector
- Used by over 350 financial organizations to exchange threat indicators with the FS-ISAC
- Powers CTI exchange at ISAC's/ISAO's including:
  - FS-ISAC, NH-ISAC, HITRUST, DSIE, R-CISC, MS-ISAC and ICS-ISAC
- Global reach – used by CSIRTS internationally including CERT-EU, CERT-UK, CERT-AU, and CERT-CA.

About the “water”…

As more CTI is represented using standardized and structured languages, opportunities emerge. Some examples:

- Automated CTI exchange with policy-based filtering (e.g. CISA)
- Indicator Sightings at scale
- Platform/Repository-Independent Analytics
- Structured Courses of Action shared at scale

CISA and STIX/TAXII

Cybersecurity Information Sharing Act of 2015

Provides limited liability protection for private sector entities that share cyber threat indicators with the Federal Government via DHS

DHS NCCIC is the focal point for this sharing

Our implementation of CISA for automated submission is based on STIX/TAXII

Privacy/PII Filtering

Structured representation of cyber threat indicators allows much of the privacy and Personally Identifiable Information (PII) scrubbing to be automated

Planning on using natural language processing technology to automated PII detection in free-text fields in STIX

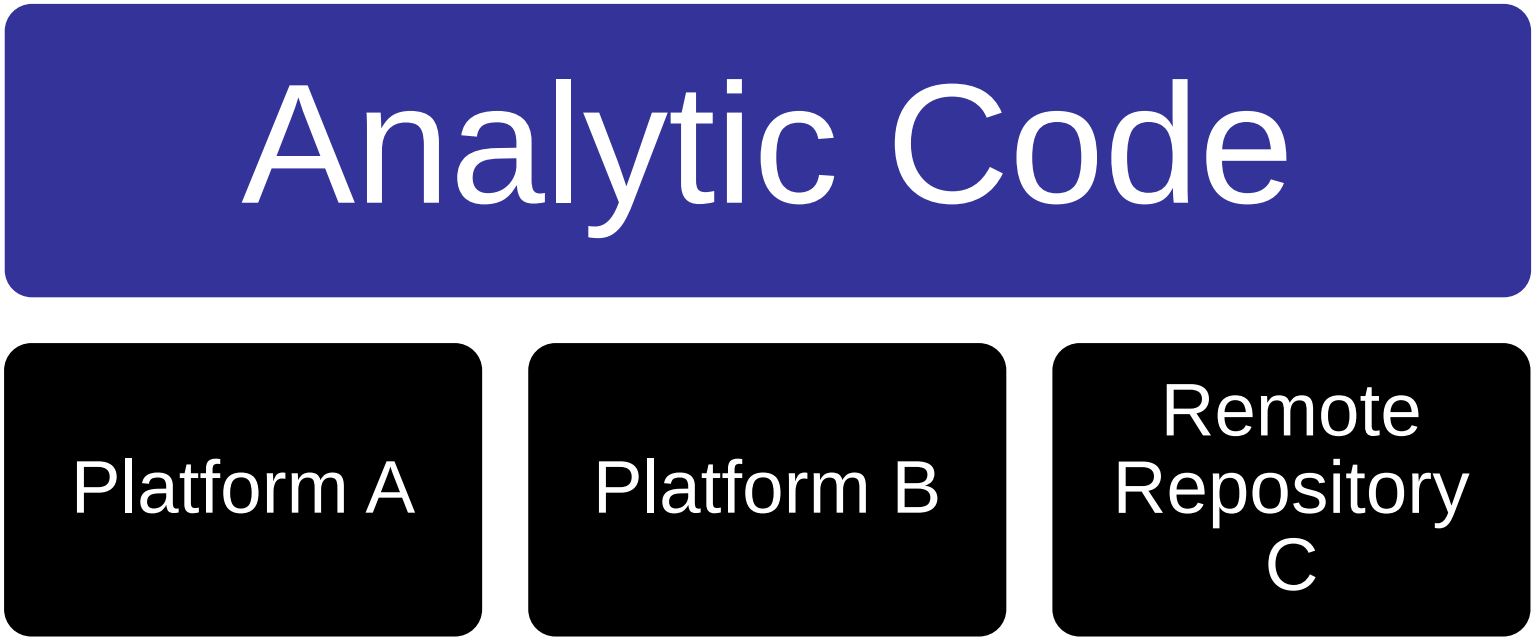
Indicator Sightings At Scale

Sighting: Report that a previously-published/shared indicator has “fired” in an organization

Sightings allow adversary activity to be tracked across organizations and sectors

Sightings also support a quality-control feedback loop that can help users gauge the quality of information sources

Platform/Repository Independent Analytics



Structured Courses of Action at Scale

Courses of Action answer the “now what?” question when indicators “fire”

Structured Courses of Action enable organizations to share COAs that can be machine-interpreted (e.g. blocking/sink-holeing)

Requires a high degree of trust/confidence in information source

Can help eliminate the noise allowing analysts to focus on what is important

Improving the “water”…

Some areas where additional work is needed to improve our ability to leverage standardized CTI at scale:

- Data markings – going beyond TLP
- More uniform confidence/reputation scoring of content & sources
- Content deduplication/correlation

The Future

Join us and help us shape the future of CTI!

For more information contact:
richard.struse@hq.dhs.gov

Homeland Security