The Problem

- Attackers are reusing attacks (because they work)

- Defenders are collecting and/or sharing information, but...
  - Often a manual process (copy-paste from a PDF)
  - Different sources provide different levels of context/details/terms
  - Some groups do supply tools/automation, but usually just used in that group
Solution

- **Standardized Language**
  - Structured Threat Information Expression

- **Standardized Exchange Mechanism**
  - Trusted Automated Exchange of Indicator Information

- STIX and TAXII are efforts to enable automated cyber threat information exchange across organization and product boundaries.
How We Got Here

- The US Department of Homeland Security (DHS)
  - Tasked with protecting the nation’s cyber infrastructure
  - Funded a project to develop standards for threat intelligence expression and sharing

- Homeland Security Systems Engineering and Development Institute (HS SEDI)
  - A DHS Federally Funded Research and Development Center (FFRDC) operated by the MITRE Corporation
  - DHS tasked HS SEDI with this project

- The MITRE STIX and TAXII Teams
  - Oversee initial development, operate public resources, moderate community discussion, develop tools, documentation, and utilities, and provide training and guidance to users
What are STIX and TAXII?

- **STIX** is a *framework and language* for the characterization and communication of cyber threat information

- **TAXII** is a *set of service and message definitions* for securely exchanging cyber threat information
  - NOT a sharing program, database, or tool
  - …but supports all of those uses and more
  - They are a set of specifications offered freely to the public

- **Developed with open community feedback**

- **Support**
  - Clear understandings of cyber threat information
  - Consistent expression of threat information
  - Secure, automated processing based on collected intelligence
  - Advance the state of practice in threat analytics
STIX provides a common mechanism for addressing structured cyber threat information across and among this full range of use cases improving consistency, efficiency, interoperability, and overall situational awareness.
What is “Cyber (Threat) Intelligence?”

Consider these questions:

- What activity are we seeing?
- What threats should I look for on my networks and systems and why?
- Where has this threat been seen?
- What does it do?
- What weaknesses does this threat exploit?
- What can I do about it?
- Who is responsible for this threat?
- Why does it do this?
STIX Indicator
What is a cyber observable?

- A **measurable event or stateful property** in the cyber domain
  - Some measurable events: a registry key is created, a file is deleted, an http GET is received, …
  - Some stateful properties: MD5 hash of a file, value of a registry key, existence of a mutex, …

- Cyber Observable eXpression (CybOX) is a standardized language for encoding and communicating information about cyber observables ([http://cybox.mitre.org](http://cybox.mitre.org))
# CybOX v2.1 Objects

- Account
- Address
- API
- Archive File
- ARP Cache Entry
- Artifact
- Autonomous System
- Code
- Custom
- Device
- Disk
- Disk Partition
- DNS Query
- DNS Record
- DNS Cache
- Domain Name
- Email Message
- File
- GUI
- GUI Dialog Box
- GUI Window
- Hostname
- HTTP Session
- Image
- Library
- Link
- Linux Package
- Memory
- Mutex
- Network Connection
- Network Flow
- Network Packet
- Network Route Entry
- Network Route
- Network Subnet
- PDF File
- Pipe
- Port
- Process
- Product
- Semaphore
- SMS
- Socket
- Socket Address
- System
- Unix File
- Unix NetworkRoute Entry
- Unix Pipe
- Unix Process
- Unix User Account
- Unix Volume
- URI
- URL History
- User Account
- User Session
- Volume
- Whois
- Win Computer Account
- Win Critical Section
- Win Driver
- Win Event
- Win Event Log
- Win Executable File
- Win File
- Win Filemapping
- Win Handle
- Win Hook
- Win Kernel
- Win Kernel Hook
- Win Mailslot
- Win Memory Page Region
- Win Mutex
- Win Network Route Entry
- Win Pipe
- Win Network Share
- Win Prefetch
- Win Process
- Win Registry Key
- Win Semaphore
- Win Service
- Win System
- Win System Restore
- Win Task
- Win Thread
- Win User Account
- Win Volume
- Win Waitable Timer
- X509 Certificate

(more on the way)
CybOX Object

- Memory CybOX Object
  - For generic memory region descriptions
STIX 1.1 Architecture (Possible Subset)
Expressing Relationships in STIX

Backdoor

Infrastructure

Malware

Badurl.com,
10.3.6.23,
...

Indicator-9742

Observables

Email-Subject:
“Follow-up”
Expressing More Relationships in STIX

“Bad Guy”

Backdoor

Malware

Badurl.com, 10.3.6.23, ...

Email-Subject: “Follow-up”

RelatedTo

ObservedTTP

RelatedTo

Exploit

Indicators

Observeds

MD5 hash...

“BankJob23”

CERT-2013-03...

RelatedTo

Campaign

RelatedTo

Incident

Infrastructure

Observables

RelatedTo

CERT-2013-03...

Indicator-9742

RelatedTo

CERT-2013-03...

Indicator-985
Part of Mandient’s APT 1 in STIX
STIX and CybOX Today

- Currently defined by a set of XML Schemas and controlled vocabularies
  - Just the way we chose to define the structure
  - Not intended to represent permanent alignment with XML

- Current releases:
  - STIX 1.1.1
  - CybOX 2.1

- Where possible, use existing structures
  - CIQ for identity and addresses
  - Snort, YARA, etc. for test mechanisms
  - CVRF for vulnerability descriptions
  - Extension points allow inclusion of other structures
TAXII Use Cases

- UC1 – Allow existing sharing communities to add automation and interoperability without forcing large scale architecture changes
- UC2 – Provide an easy way for new communities to begin sharing

Design Philosophy
- Keep it simple
  - Use existing transport protocols when possible
- Do not tell people how to arrange their sharing architecture
Flexible Sharing Models

- TAXII supports a wide variety of sharing models
  - Push or pull delivery
  - On-demand or subscription

Peer to Peer

Hub and Spoke

Source/Subscriber
Key TAXII Features

- Content agnostic
  - Allow anything; depend on nothing in the payload
- “Data Collections” used for content organization
  - Collections can be ordered or unordered
  - Data provider decides what constitutes a collection
- Support establishing and fulfilling subscriptions
- Support data pushing and pulling
- Support network and content-level security
  - Encrypt transport and/or encrypt payloads
- Extensible bindings to network protocols and message formats
  - Currently define XML messages over HTTP(S)
  - Layered design allows for other options
TAXII Services

- TAXII defines four services
  - Discovery – A way to learn what services an entity supports and how to interact with them
  - Collection Management – A way to learn about and request subscriptions to Data Collections
  - Inbox – A way to receive pushed content (push messaging)
  - Poll – A way to request content (pull messaging)
- Each service is optional – implement only the ones you wish
- Services can be combined in different ways for different sharing models
Hub & Spoke Example

Discovery  Collect. Manage.  Poll  Inbox  Client

Spoke 1
- Get connection info
- Subscribe to data collections

Hub
- Push new data to the hub
- Pull recent data from the hub

Spoke 2
- Push recent data to a spoke

Spoke 3

Spoke 4
- Subscribe to data collections

Client
Hub & Spoke Example (2)

- **Discovery**
- **Collect. Manage.**
- **Poll**
- **Inbox**
- **Client**

### Hub & Spoke Example

- **Spoke 1**: Subscribe to data collections, Get connection info
- **Spoke 2**: Push new data to the hub
- **Spoke 4**: Pull recent data from the hub

**Clients do not host services.**
Hub & Spoke Example (3)

- Discovery
- Collect. Manage.
- Poll
- Inbox
- Client

Spoke 1: Get connection info
Spoke 1: Subscribe to data collections
Hub: Push recent data to a spoke
Spoke 3: Push new data to the hub
Hub: Retains no records.

Client

Push new data to the hub

Get connection info

Subscribe to data collections

Push recent data to a spoke

Hub retains no records.
Hub & Spoke Example (4)

Subscribe by purchasing contract

Hub

Spoke 2

Spoke 4

Spoke 3

Push new data to the hub

Push recent data from the hub

Pull recent data from the hub

Push recent data to a spoke
(Not a) Hub & Spoke (anymore) Example

No Hub (Peer-to-peer network)

Spoke 1
Spoke 2
Spoke 3
Spoke 4

Push new data to peers
Operational

- FS-ISAC is currently sharing operational data using STIX/TAXII
  - http://avalanche.fsisac.com/

- HP Threat Central (HPTC) uses STIX and TAXII

- Microsoft Active Protection Program (MAPP) is developing STIX & TAXII support

- US-CERT is integrating support for STIX and TAXII for its alerts

- Lockheed Martin is helping the Open Information Security Foundation (OISF) add STIX & TAXII support to Suricata
Some of the organizations contributing to the STIX conversation:
Available Resources

- STIX, TAXII, and CybOX are actively supported
  - Documentation and tutorials
  - Training sessions
    - Next is May 19-20 at FIRST in Redmond, WA
  - Active mailing list communities
Enabling Utilities

- Python Language bindings for STIX, CybOX, etc.
  - Also includes high-level programmatic APIs for common needs/activities
- Conversion utilities from commonly used formats & tools
  - E.g., OpenIOC-to-STIX; others under development
- STIX Validator – Includes validation against STIX Profiles and suggested practices
- STIX-to-HTML – Turn STIX into human-readable documents
- Stixviz – Simple graphical visualization tool
- Utilities supporting common use cases
  - Email_to_CybOX utility supporting phishing analysis & management
  - X.509-to-CybOX utility supports generation of CybOX from an X.509 certificate
- Libtaxii – Python binding for TAXII supports TAXII client development
- YETI – Python/Django web app; Simple implementation of TAXII services
Summary

- **Standardized Language**
  - Structured Threat Information Expression

- **Standardized Exchange Mechanism**
  - Trusted Automated Exchange of Indicator Information

- **Make it easier to express, exchange, consume, and correlate cyber threat intelligence**

- **Large group of contributing parties**
- **Used by real products/communities**
- **Supported by an active community and running code**
Next Steps

- If you are creating or consuming threat intelligence, talk to your vendors about STIX

- If you are sharing threat intelligence, talk with your community about TAXII

- If you build tools that create, consume, or exchange cyber threat intelligence, talk to us – we can help
For more information

- **Websites** – Contains official releases and other info
  - [https://stix.mitre.org/](https://stix.mitre.org/)
  - [https://taxii.mitre.org/](https://taxii.mitre.org/)
  - [https://cybox.mitre.org/](https://cybox.mitre.org/)

- **Sign up for the Discussion and Announcement mailing lists**
  - [https://[stix/taxii/cybox].mitre.org/community/registration.html](https://[stix/taxii/cybox].mitre.org/community/registration.html)

- **Open issues can be discussed on GitHub**
  - [https://github.com/STIXProject](https://github.com/STIXProject)
  - [https://github.com/TAXIIProject](https://github.com/TAXIIProject)
  - [https://github.com/CybOXPProject](https://github.com/CybOXPProject)

- **Related sites**
  - [https://maec.mitre.org/](https://maec.mitre.org/)
  - [https://capec.mitre.org/](https://capec.mitre.org/)
Questions?

- Charles Schmidt – cmschmidt@mitre.org
- STIX team – STIX@mitre.org
- TAXII team – TAXII@mitre.org