Improving Enterprise Security:

Cyber Threat Sharing with STIX and TAXII

Presented by Chris Lenk and Michael Kouremetis

ASQ Sections 509/511 Software SIG Meeting, McLean, VA
22 August 2017

Presenters

Chris Lenk
(clenk {at} mitre {dot} org)

MITRE projects:

- Python STIX 2 API
- STIX Validator
- Malware Analysis Framework

Domains: Cyber security, Software/web development

Michael Kouremetis
(mkouremetis {at} mitre {dot} org)

MITRE projects:

- Python STIX 2 API
- MAEC standard
- (MITRE) InfoSec analyst tools

Domains: Cyber security, Software/API development

Disclaimer

The opinions expressed in this presentation are those of the speakers alone and do not represent those of any organizing entity, standards body, or the speakers' employer. MITRE does not guarantee the accuracy or reliability of the information contained herein.

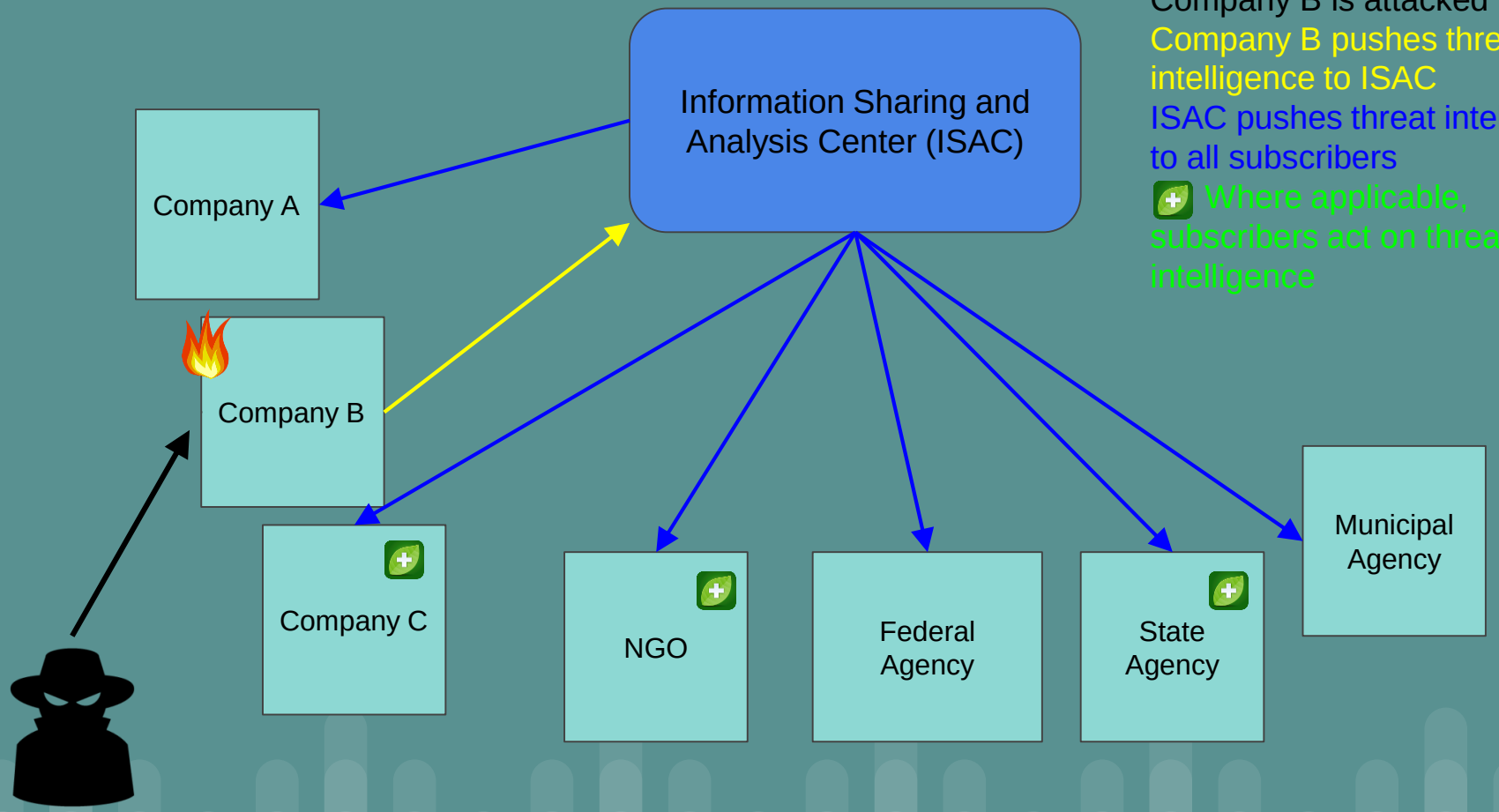
Agenda

- What is Cyber Threat Sharing?
  - Purpose of Cyber Threat Sharing
  - Example Use Cases
- How can my organization share cyber threat intelligence?
  - Sharing models
  - Sharing levels
  - Types of data
  - Sharing technologies
- STIX, an awesome way to structure threat data!
  - Overview
  - Data Markings
  - Example Use Cases
  - Resources
- TAXII, the vehicle to share STIX data
- Takeaways

Cyber Threat Sharing

- The practice of sharing cyber threat intelligence, vulnerabilities, configurations, best practices, knowledge and tips to a larger external community.
- **Goal:** To enhance the cyber security of an individual organization as well as that of the entire sharing community.
- Enterprise/Organization:
  - Obtains a vast stream of cyber security information that can be highly tailored to its infrastructure, network/host systems, software etc...
- Community:
  - The pooled intelligence, knowledge and experience allows for a much more formidable cyber defense than any single organization could produce.
  - A survey of the Advanced Cyber Security Center (ACSC) sharing partners concluded that 87% of the partners were receiving actionable threat intelligence and 50% of the partners noted demonstrable improvement to their cyber security (Bakis, 2015)

Cyber Threat Sharing



Company B is attacked
Company B pushes threat intelligence to ISAC
ISAC pushes threat intelligence to all subscribers
Where applicable, subscribers act on threat intelligence

How to share: Sharing Models

Decision Factors

Information goals

Sharing model and mechanisms

Availability

Centralized/Hub & Spoke/Subscriber

Advantages:

- Data enhancement, added analysis
- Macro trend analysis
- Rule/agreement enforcement, organization
- Anonymization/data cleansing
- Low technical costs for new consumers

Requirements: Wide-scale trust, capitalization

Direct/Peer-to-Peer

Advantages:

- Tailored for efficiency and speed
- Lower trust requirements

Requirements: Often requires participants to have more sophisticated and matured cyber threat sharing operations

How to share: Sharing Models

Centralized/Hub & Spoke/Subscriber (examples)

- Department of Homeland Security's (DHS) Automated Indicator Sharing (AIS), Cyber Information Sharing and Collaboration Program (CISCP)
- Advanced Cyber Security Center (ACSC)
- National Council of ISAC's
  - Automotive ISAC
  - Aviation ISAC
  - Defense Industrial Base (DIB) ISAC
  - .
  - .
  - .
  - Water ISAC
- Indiana-ISAC, Michigan-ISAC

Direct/Peer-to-Peer (examples)

- Exist between all size organizations
- From handshake agreements to formal contracts
- May be for highly esoteric information or for the entire cyber threat production capabilities of the participants

(Mature cyber threat sharing organizations are highly inclined to personalized, private partnerships; especially when in the same industrial domains)

How to share: Sharing Levels

- Consuming vs. Producing
- Implement cyber threat sharing capability incrementally
  - Basic consumption -> advanced consumption -> basic production -> advanced production
- Human relationships still play pivotal role regardless of technological sophistication and capability
- Section 4, NIST Special Publication 800-150: Guide to Cyber Threat Information Sharing (Johnson et al., 2014)

How to share: Types of Data

- Internal factors
  - Capability
  - Restrictions
  - Useful

- NIST SP 800-50 - Indicators should be:
  - Timely
  - Relevant
  - Accurate
  - Specific
  - Actionable

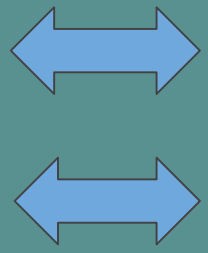
How to share: Types of Data

- Cyber Threat Information sources
  - Logs, flagged events, emails, network packets
  - Incidents, attack attempt descriptions
  - Vulnerabilities, secure configurations, firewall/IDS/IPS rules and policies
  - Malware signatures: host (files, registry keys, strings, processes), network (IP, domains, protocol, content), hashes
  - Analysis of: malware, attack pattern, exploit, network activity, host activity

How to share: Sharing Technologies

Cyber Threat Information Languages
(how data is stored)

- Structured Threat Information Expression (STIX)
- Incident Object Description Exchange Format (IODEF)
- OpenIOC



Cyber Threat Sharing Protocols
(how data is transmitted)

- Trusted Automated eXchange of Indicator Information (TAXII)
- Real-time Inter-network Defense (RID)

→ A language standard and a sharing protocol are the primary technical requirements for cyber threat sharing but they are not the *only* requirements. In practice, additional tools such as format converters, tool plugins, and APIs are essential to efficient use and adoption of cyber threat sharing.

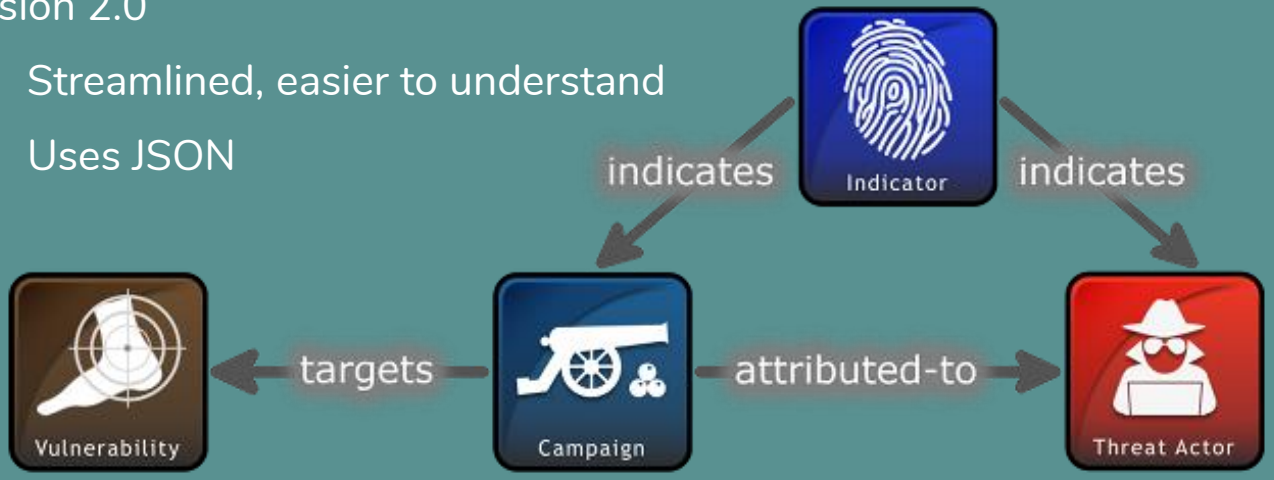
STIX: Overview

- Example of a language for sharing Cyber Threat Intelligence
  - Easy to use
  - Commonly-used
  - Well-known
  - Machine-readable (supports automation)

- Community-driven: OASIS
  - Vendors, Users
  - Government, Private Sector, Academia
  - Open Source

STIX: Overview

- Graph-based model: STIX domain objects, and relationship objects between them
  - Easier to add information
- Tool-agnostic
- Version 2.0
  - Streamlined, easier to understand
  - Uses JSON



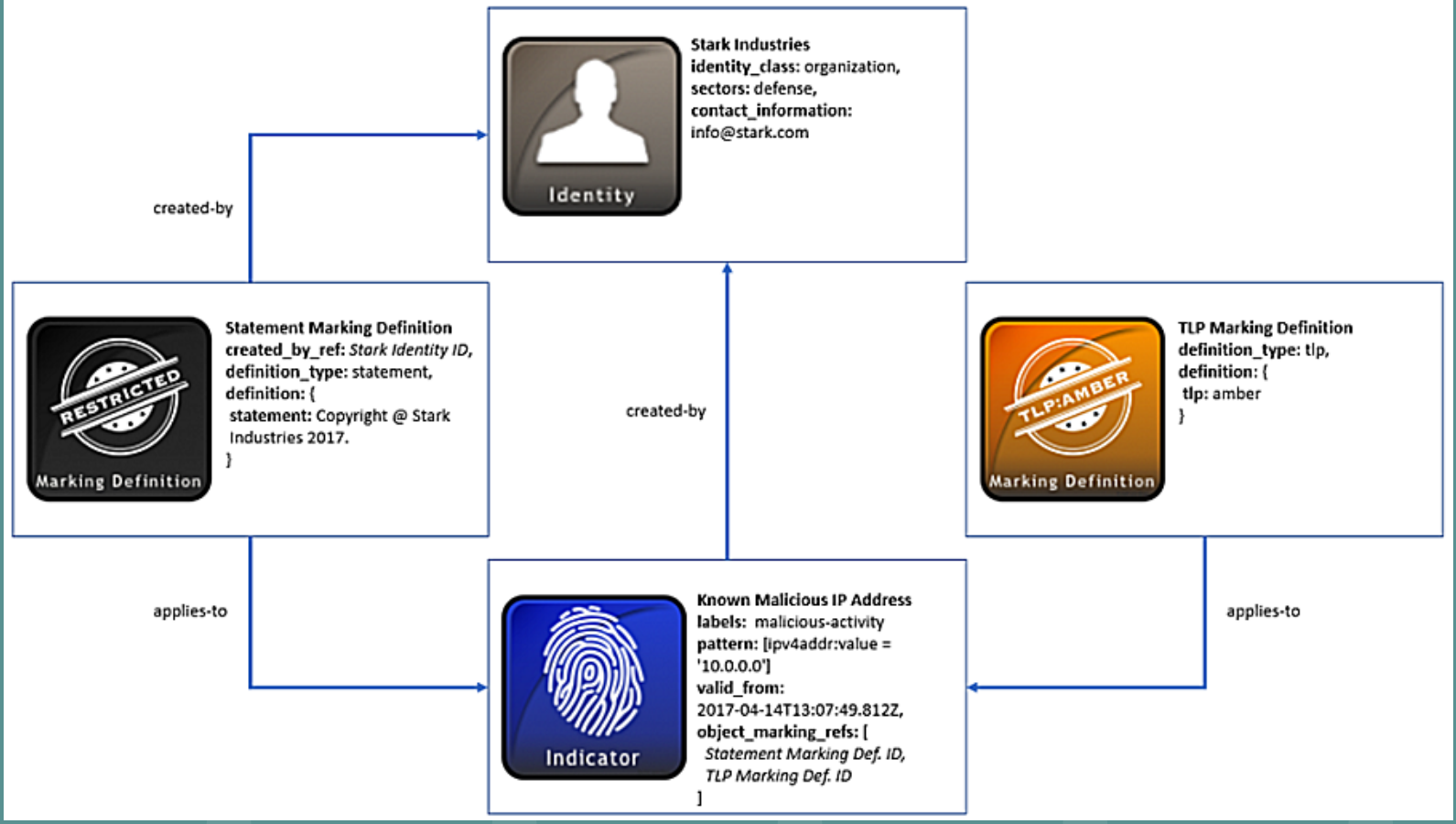
STIX: Overview

- What types of objects are included in model?
  - Threat Actors
  - Indicators of suspicious activity
  - Vulnerabilities
  - Malware
  - Reports
  - Courses of action
  - And more...

STIX: Data Markings

- Supports marking data with different restrictions
- Examples
  - Classified data
  - Data that cannot be re-shared
- Can apply to an entire object or just certain properties of the object

STIX: Data Markings



STIX: Data Markings


```
{
   "type": "marking-definition",
   "id": "marking-definition--d771aceb-3148-4315-b4b4-130b888533d0",
   "created": "2017-04-14T13:07:49.812Z",
   "created_by_ref": "identity--611d9d41-dba5-4e13-9b29-e22488058ffc",
   "definition_type": "statement",
   "definition": {
     "statement": "Copyright © Stark Industries 2017."
   }
 },
 {
   "type": "indicator",
   "id": "indicator--33fe3b22-0201-47cf-85d0-97c02164528d",
   "created": "2017-04-14T13:07:49.812Z",
   "modified": "2017-04-14T13:07:49.812Z",
   "created_by_ref": "identity--611d9d41-dba5-4e13-9b29-e22488058ffc",
   "name": "Known malicious IP Address",
   "labels": [
     "malicious-activity"
   ],
   "pattern": "[ipv4addr:value = '10.0.0.0']",
   "valid_from": "2017-04-14T13:07:49.812Z",
   "object_marking_refs": [
     "marking-definition--f88d31f6-486f-44da-b317-01333bde0b82",
     "marking-definition--d771aceb-3148-4315-b4b4-130b888533d0"
   ]
 }
```

STIX: Use Cases

- Use case examples
  - Share information about a threat actor
    - Aliases
    - Goals
    - Motivations
    - Attack patterns
  - Share indicators of compromise
    - Malicious file hashes
    - Malicious url
    - C2 IP addresses
- These are simple examples, but work is being done to include more sophisticated forms of intelligence in future versions

STIX: Use Cases


```
   {
      "type": "indicator",
      "id": "indicator--a932fcc6-e032-176c-126f-cb970a5a1ade",
      "created": "2014-02-20T09:16:08.989000Z",
      "modified": "2014-02-20T09:16:08.989000Z",
      "name": "File hash for Poison Ivy variant",
      "description": "This file hash indicates that a sample of
Poison Ivy is present.",
      "labels": [
        "malicious-activity"
      ],
      "pattern": "[file:hashes.'SHA-256' =
'ef537f25c895bfa782526529a9b63d97aa631564d5d789c2b765448c8635fb6c']
",
      "valid_from": "2014-02-20T09:00:00.000000Z"
    }
```

STIX: Resources

- STIX website: http://cti-tc.github.io
- STIX JSON schemas: https://github.com/oasis-open/cti-stix2-json-schemas
- Tools:
  - Python API https://github.com/oasis-open/cti-python-stix2
  - Validator https://github.com/oasis-open/cti-stix-validator
  - Converter/Elevator https://github.com/oasis-open/cti-stix-elevator

TAXII

- Protocol for sharing Cyber Threat Intelligence
- Defines a standard REST API
- Easy to deploy
- Specifically designed for sharing STIX
  - (can work with other standards too)
- Version 2.0
  - Uses HTTPS for security
  - Uses JSON for interoperability and ease of use

Takeaways

- Cyber Threat Sharing strengthens the security of your organization as well as the whole community.
  - No one organization knows everything!
- Key Considerations:
  - Centralized or Peer-to-Peer? Hybrid?
  - Implement sharing gradually, moving from consuming to also producing
  - What types of data to share?
- STIX and TAXII are easy-to-use examples of standards and technologies for sharing Cyber Threat Intelligence.

References

NIST Special Publication 800-150 Guide to Cyber Threat Information Sharing (Johnson et al., 2016)

Bakis, B. (2015). Cyber Threat Information Sharing - Lessons Learned and Challenges. MITRE Corporation. Retrieved from http://www.mitre.org/capabilities/cybersecurity/overview/cybersecurity-blog/blueprint-for-cyber-threat-sharing-lessons

Cyber Threat Intelligence Technical Committee. https://oasis-open.github.io/cti-documentation/