DC3 DCISE Information Sharing Efforts

Sam Perl,

CSIRT Development and Training Team,

CERT, SEI, Carnegie Mellon University

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

DM22-0786

DC3 DCISE Information Sharing - Agenda

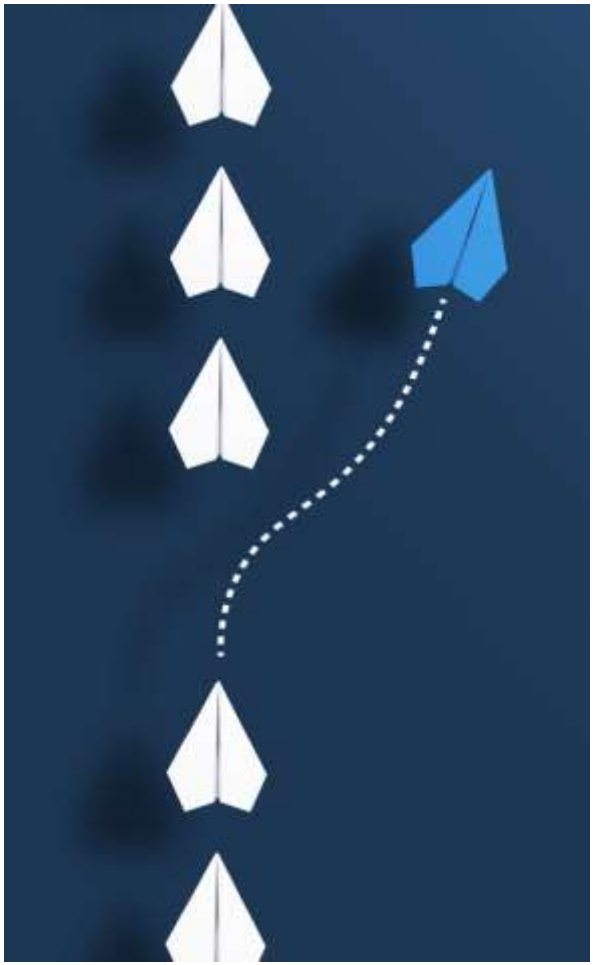
1. What is Machine-to-Machine (M2M) and Information Sharing?
2. DCISE M2M Goals
3. Current Activity
4. Future Plans

Information Sharing Assumptions

- Can help enable private and public IT-communities to share a wide range of information.
- Sharing indicators of compromise, artifacts, context, TTP, and more within a community can have direct impact on reaction capability.
- Can help with prevention, detection, and response

Shifting Cybersecurity Information Sharing Practices

- Traditional sharing of Cybersecurity related information
  - Human Analyst to Human Analyst
  - Often uses natural language to describe events, situations, and actions
- A Government, Industry, and International teams cybersecurity information sharing shift to “Machine to Machine”
  - Goal is to improve cyber defense performance at lower cost
  - Targeted for most benefit



Machine to Machine M2M – Benefits

M2M Benefits

- Faster circulation of information to those who need it most
- Potential for more personalization of data
- Reduced manual effort may lower cost per unit
- Collective understanding and cyber defenses improve quickly

Machine to Machine M2M – Challenges

M2M Challenges

- Too much data that is not relevant may inundate analysts and increase costs
- M2M systems can be complex and may be costly to establish and maintain
- Mistakes in configuration, sharing, data categorization, etc. are frequent
- Machine standards may not always express what analysts need to communicate easily
- Integration with existing systems may be difficult

DCISE M2M Information Sharing Goals

1. Reduce effort for partners to access data and increase available channels
2. DCISE Products in **machine consumable formats** to Industry and Government constituents
3. Act as a relay for relevant data from others using M2M processes
4. Use M2M where reasonably possible

Path to Sharing

DCISE is exploring options to improve M2M sharing to address the challenges and meet sharing goals

- Options for partners new to M2M
  - Option to download data via an API
  - Other Interfaces (evaluations in progress)
- Support common formats MISP, STIX, others (CSV)
- Support common protocols (ex. TLP)
- Expand Offerings to additional sources, formats, protocols
- Plans to offer relevant supplemental data obtained through connections with other sources

Current Activity

- Operational Pilot MISP server
- Successfully connected to other MISP servers
- Making initial decisions on scope, format mappings, and data types
- Testing integration with other DCISE service environments (SSO)
- Establishing processes and procedures for data loading, analysis, usage
- Negotiating agreements for receipt of additional datasets
- Investigating data interchange formats and system interoperability

What will M2M mean for the audience(s)?

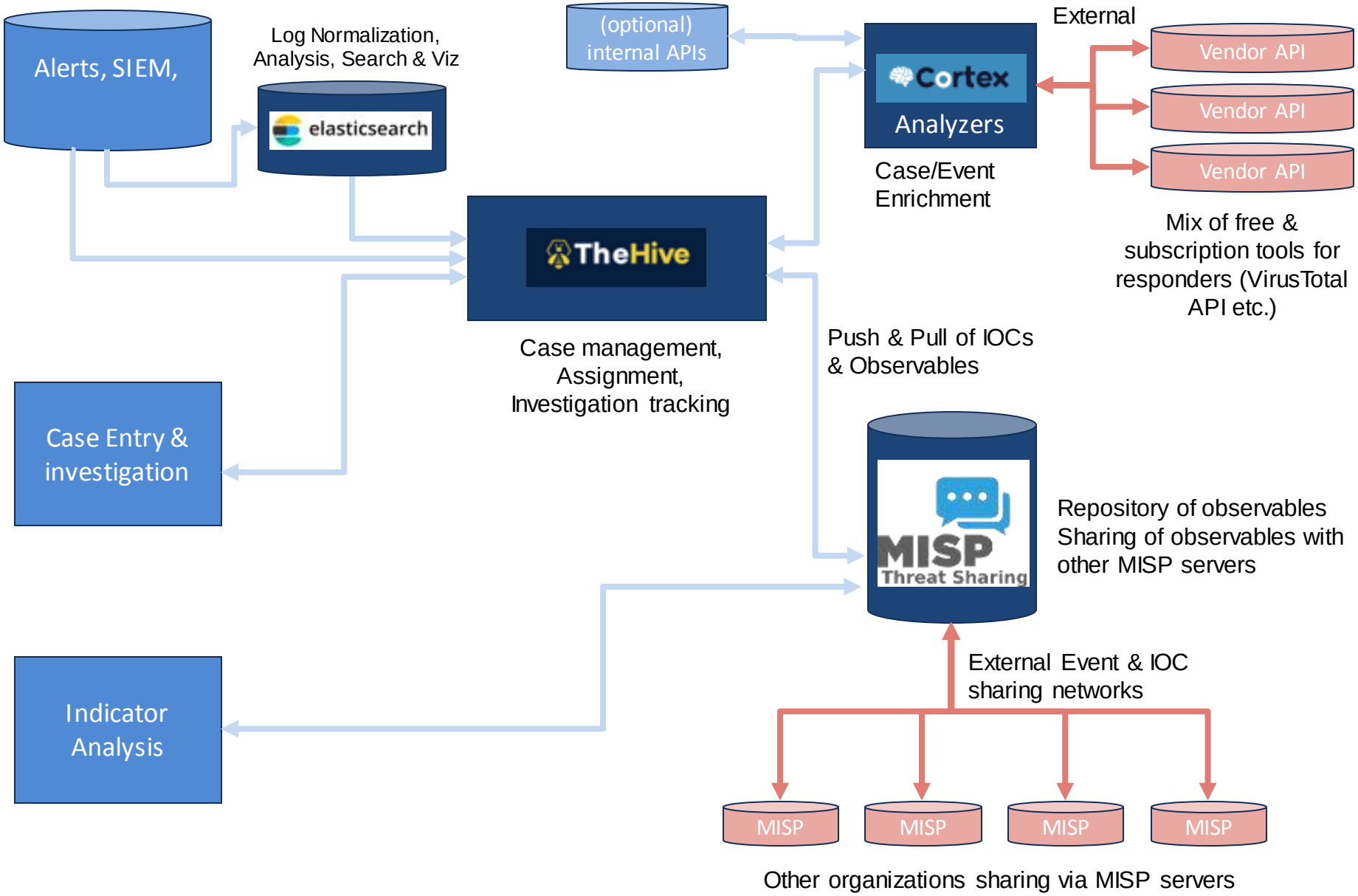
MISP has an API, and a python library (PyMISP). A GUI is available for manual access. Data in MISP format, exportable to other formats.

Can use a TAXII client to interface with TAXII server (DCISE TAXII server in discussion) and receive STIX format data

Automated receipt of data and loading into defensive tools.

- Via MISP, TAXII client, or other analysis platforms that support MISP or STIX formats
- For example; export of **network related** attributes in **Snort or Suricata** rule formats

Notional design plan for MISP integration and data flow

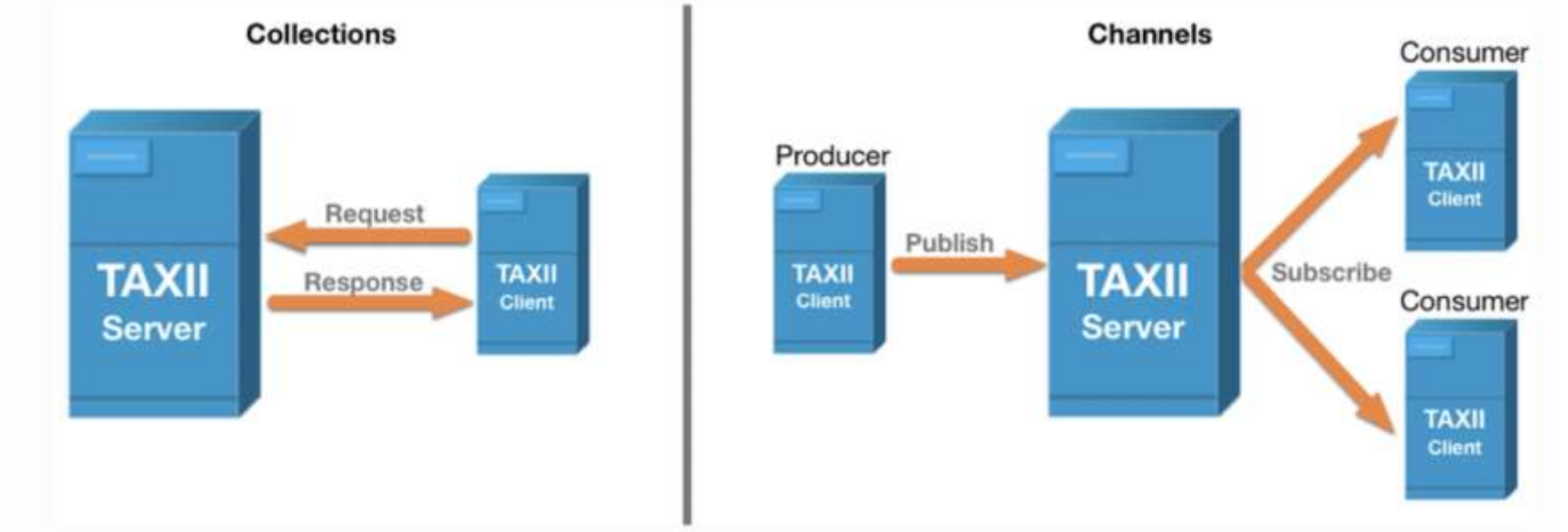


Next Steps

- Integration with future DCISE analysis systems
- ‘System’ Architecture
- Analysis processes and procedures
- Legacy data: load, test, operate
- Incorporate more datasets
- **Improvements to Interfaces, APIs, GUIs based on audience**

STIX / TAXII middleware solution to data exchange

- Add improvements for M2M in common Government exchange formats



https://oasis-open.github.io/cti-documentation/taxii/intro.html

Future Plans

- Provide MISP server access to Partners
- Establish STIX / TAXII server with relevant DCISE data for Government constituents
- Improve automated receipt and processing of relevant cybersecurity data

Seeking feedback as we move forward

Questions

- Are you using MISP?
- Do you have experiences with M2M?
- What are your obstacles and challenges?
- Would M2M allow you to automate processes you are performing manually now?
- If Cybersecurity data is available, how will you use it?

Contact Information

Sam Perl – sjperl@cert.org

Don Ranta – donald.ranta.ctr@us.af.mil and dmranta@sei.cmu.edu

Aaron Reffett – akreffett@cert.org

Michael J. Weiskopff – michael.weiskopff.1@us.af.mil

Discussions & Questions?