Automated Indicator Sharing

W. Preston Werntz

Homeland Security

Background

The Automated Indicator Sharing (AIS) initiative was driven by proposed White House cybersecurity legislation designating the National Cybersecurity and Communications Integration Center (NCCIC) as the single civilian cybersecurity center for the private sector to share cyber threat indicators.

- Even in absence of legislation, DHS is committed to this effort.
- When legislation is passed, it may impact some parts of the initiative.

Homeland Security

Goal

To maximize, to the fullest extent possible, the near-real-time dissemination of all relevant and actionable cyber threat indicators among the private sector and Federal Departments and Agencies for the purposes of network defense, and, within any statutory limitations, law enforcement purposes, while ensuring appropriate privacy and civil liberties protections.

Homeland Security

What does that really mean?

Through AIS, we are expecting to generate lots of commodity indicators for the purpose of network defense …

- This represents change in approach for some organizations.
- The predictive analytical value of a single indicator alone is likely low. The predictive analytical value of single indicator, either specifically enriched with other information or assessed generally as part of larger big data pattern analysis of indicators, could be quite high.

Homeland Security

Let's talk indicators

- An **indicator** is not an incident, malware, or detailed analysis regarding a campaign or TTP, though it may relate to those things.
- Specifically, an **indicator** means: an observable plus a hypothesis about a threat. An observable is an identified fact.
  - "A file with the MD5 hash 8743b52063cd84097a65d1633f5c74f5 is seen." - **observable**
  - "A file with the MD5 hash 8743b52063cd84097a65d1633f5c74f5 indicates the Poison Ivy Malware." – **indicator**, where Poison Ivy Malware is the remote access threat.

Homeland Security

Approach

- Continue supporting existing paths for receipt and dissemination of cyber threat indicators.
- Leverage and build upon work already accomplished and adopted to the fullest extent possible, including:
  - STIX and TAXII as core enabling technologies.
  - Enhance Shared Situational Awareness (ESSA) Access Control Specification (handling and dissemination controls for sharing with Federal Departments and Agencies).
  - Cyber Information Sharing and Collaboration Program (CISCP) information sharing program.

Homeland Security

What have we done so far?

- Deployed an accredited TAXII server into Amazon's GovCloud to push out existing indicators.
- Completed a Privacy Threshold Analysis.
- Completed a high-level System Description Document.
- Created an AIS STIX profile and data dictionary of cyber threat indicator fields and which ones have privacy concerns (e.g., free text).
- Identified six initial policy items and recommendations.
- Uploaded ~1,100 existing CISCP indicators and ~150 AIS indicators to the TAXII server.

Homeland Security

Policy Items and Recommendations

Six policy items were identified for adjudication via inter-agency input:

- Cutting room floor
- Sanitization speed
- Ingress risk
- Requirements for Sector Specific Agencies to receive
- International coordination and considerations
- Moving indicator sharing beyond CISCP

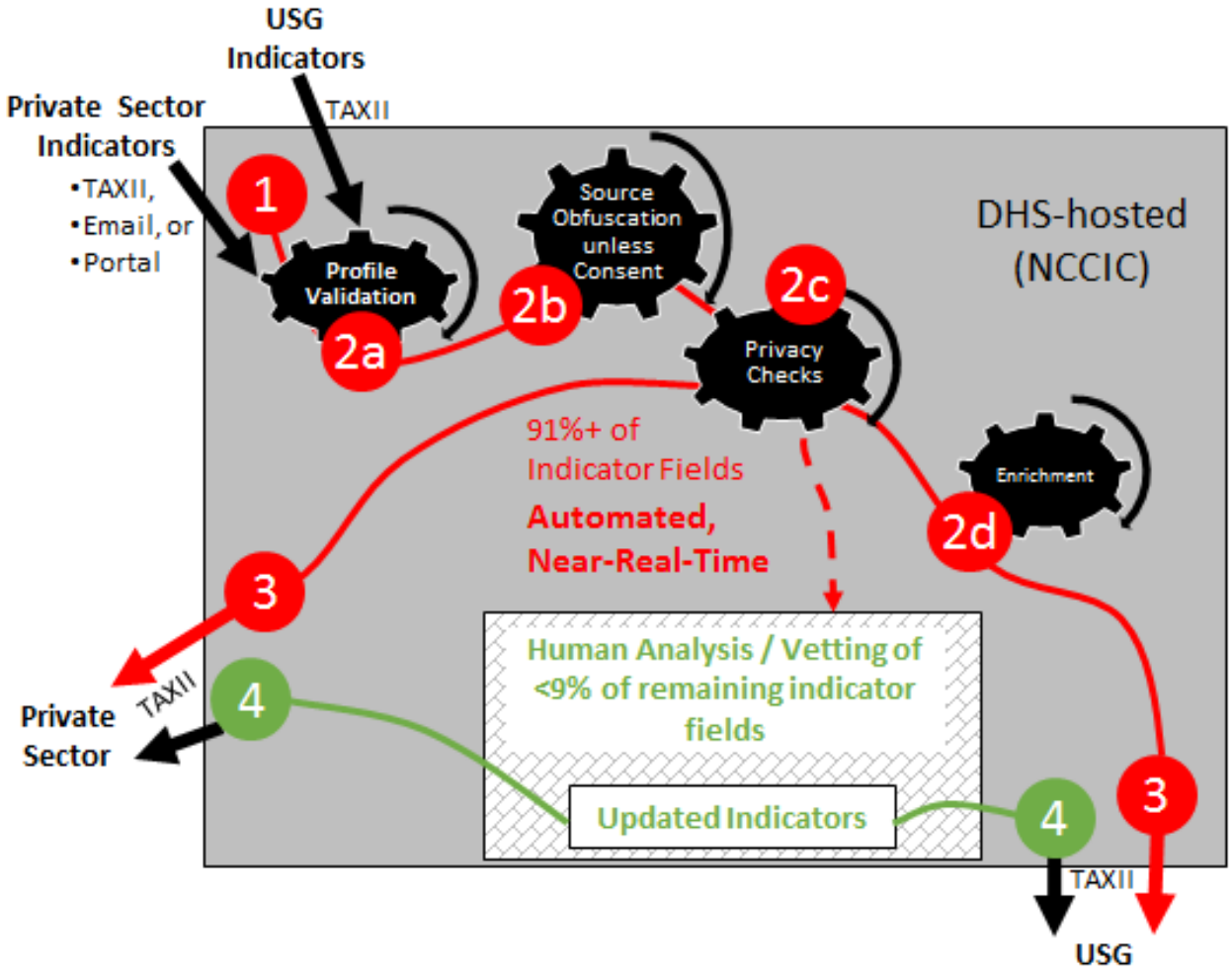
Homeland Security

What are we doing next?

- Adding additional infrastructure and capabilities to allow the private sector to submit indicators to DHS via the TAXII server that can be processed automatically.
- Finalizing a Terms of Use agreement and submission guidance.
- Finalizing a Privacy Impact Assessment.
- Expanding the number of other TAXII implementations we can connect with.

Homeland Security

Notional indicator ingest workflow



Homeland Security

Technical and manual mitigations

- Replacing ID with NCCIC
- Defining vocabulary and schema restrictions
- Regular expression (pattern matching)
- Matching against list of known good values
- Replacing with auto generated text
- Conducting human review

Homeland Security

Where are we going in the future?

- Increasing automation allowing for more fields to be processed without human analysis being required.
- Introduction of a “shared services capability” to help agencies participate in automated cyber threat indicator sharing regardless of cybersecurity sophistication or resources.

Homeland Security

Questions?

Homeland Security