National Institute of Standards and Technology
U.S. Department of Commerce

Demonstration: *Sharing Actionable Threat Indicators Using SCAP*

JIM HANSON, DIRECTOR OF ENGINEERING AND DEVELOPMENT, CYBER ENGINEERING SERVICES, INC.

CYBERSECURITY INNOVATION FORUM

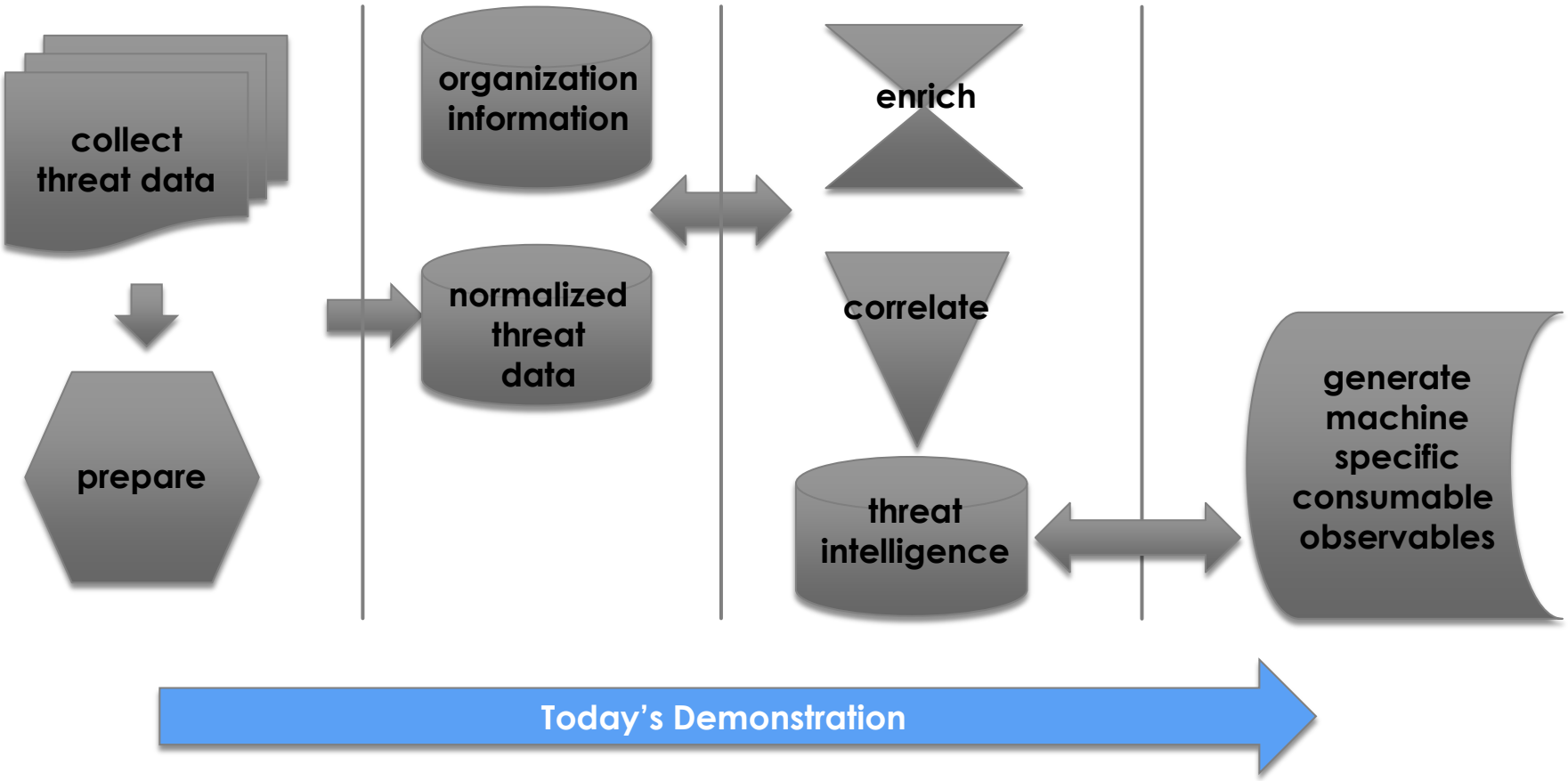
11 SEPT 2015

The Problem Space

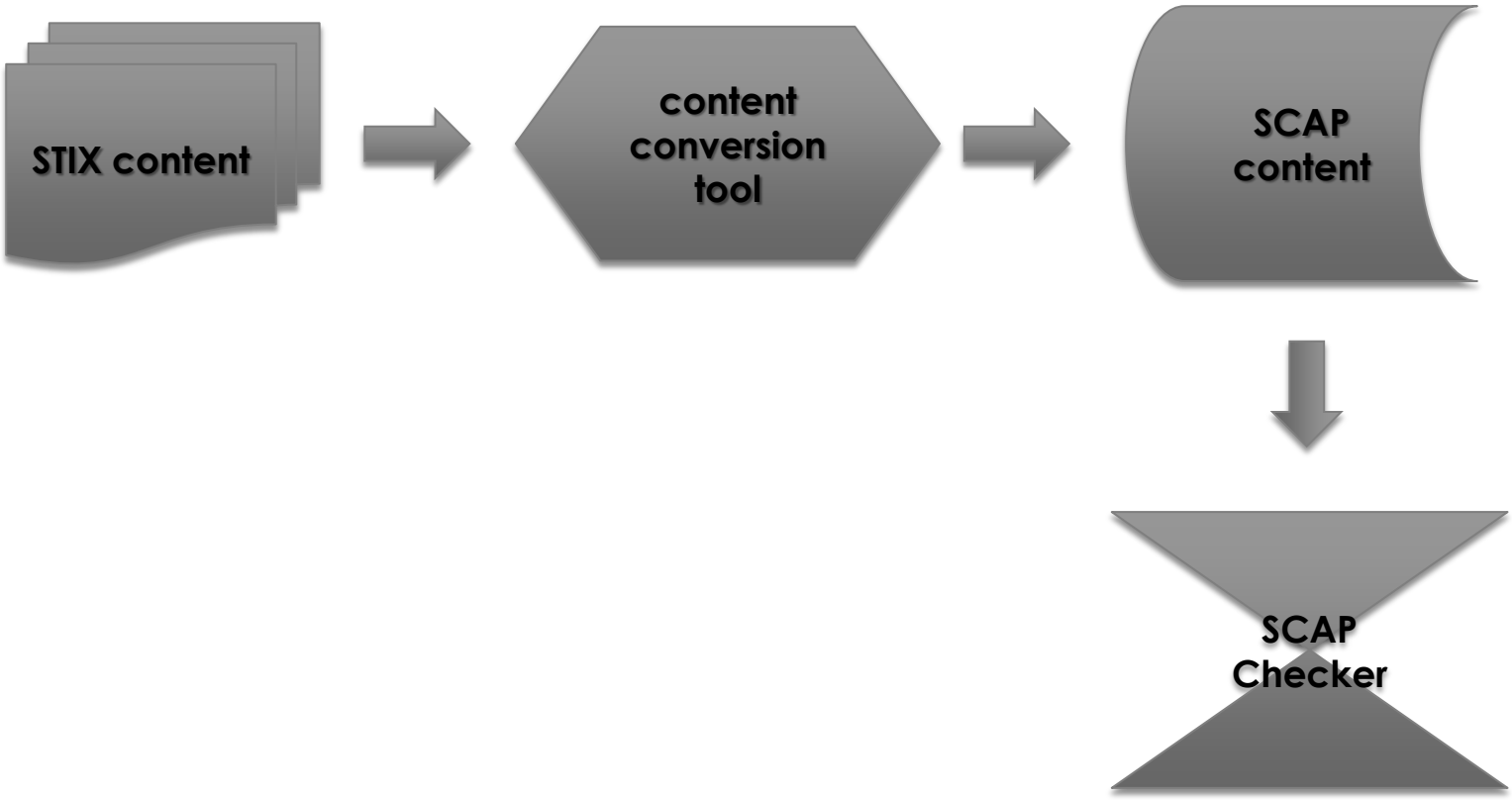
- Threat data today is largely not machine consumable or widely shared
- Takes time for analysts to translate the indicators to machine format
- Errors can be introduced in the translation process
- Cannot leverage existing deployed tools across the enterprise such as SCAP validated tools
- Other standard data feeds are years away from common deployment
- Threat Data repositories exist that, if rendered in standards-based, machine-consumable format, could benefit organizations today

NIST's Approach

input | storage | analytics | output



Specific Demonstration



Today's Demonstration

- Based on Draft NISTIR 8057, *Creating Windows Actionable Threat Indicators using Security Content Automation Protocol (SCAP) Version 1.2*
  - Presents technical approach to using SCAP 1.2 content for malware mitigation
  - Leverages existing standard and tools for detecting sophisticated malware
- Proof of Concept Tool
  - Demonstrates synergy between STIX and SCAP
  - Converts STIX-based indicators to machine-actionable content
  - Output is SCAP 1.2 content
  - Tool output can be interpreted by some validated SCAP products

Benefits

- Leverages existing standards:
  - STIX 1.2 & SCAP 1.2
- Output is immediately actionable with existing tools
  - No waiting for vendor adoption & agency deployment of new tools
- Process can be fully automated
  - From *indicators* to *action* at network speed
  - Amenable to automated indicator sharing
- Not just limited to Threat Data…
  - what about other system state information repositories?

NIST

Next Steps

This research is a good beginning, but other work remains:

- Tools to rapidly convert *insight* into sharable, actionable content. Examples include:
  - Tools to convert output of existing malware analysis tools to STIX indicators.
  - Tools to convert common malware indicators to appropriate STIX content.
- Techniques for sharing *machine-actionable* content. Examples:
  - STIX Indicator Sharing Profile
  - Forum for sharing content both internally and among specific communities of interest.

NIST

For more information…

- Review Draft NISTIR 8057, *Creating Windows Actionable Threat Indicators using Security Content Automation Protocol (SCAP) Version 1.2*
- Contacts:
  - Murugiah Souppaya, Computer Scientist, NIST, http://www.nist.gov/itl/csd/souppaya-murugiah.cfm
  - Jim Hanson, Director of Engineering & Development, Cyber Engineering Services, Inc., jhanson@cyberesi.com
  - Brad Wood, Senior Scientist, G2, Inc., brad.wood@g2-inc.com