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

Sharing Actionable Threat Indicators Using SCAP

STEPHEN QUINN, SR. COMPUTER SCIENTIST, NIST

CYBERSECURITY INNOVATION FORUM

11 SEPT 2015

Setting the Stage

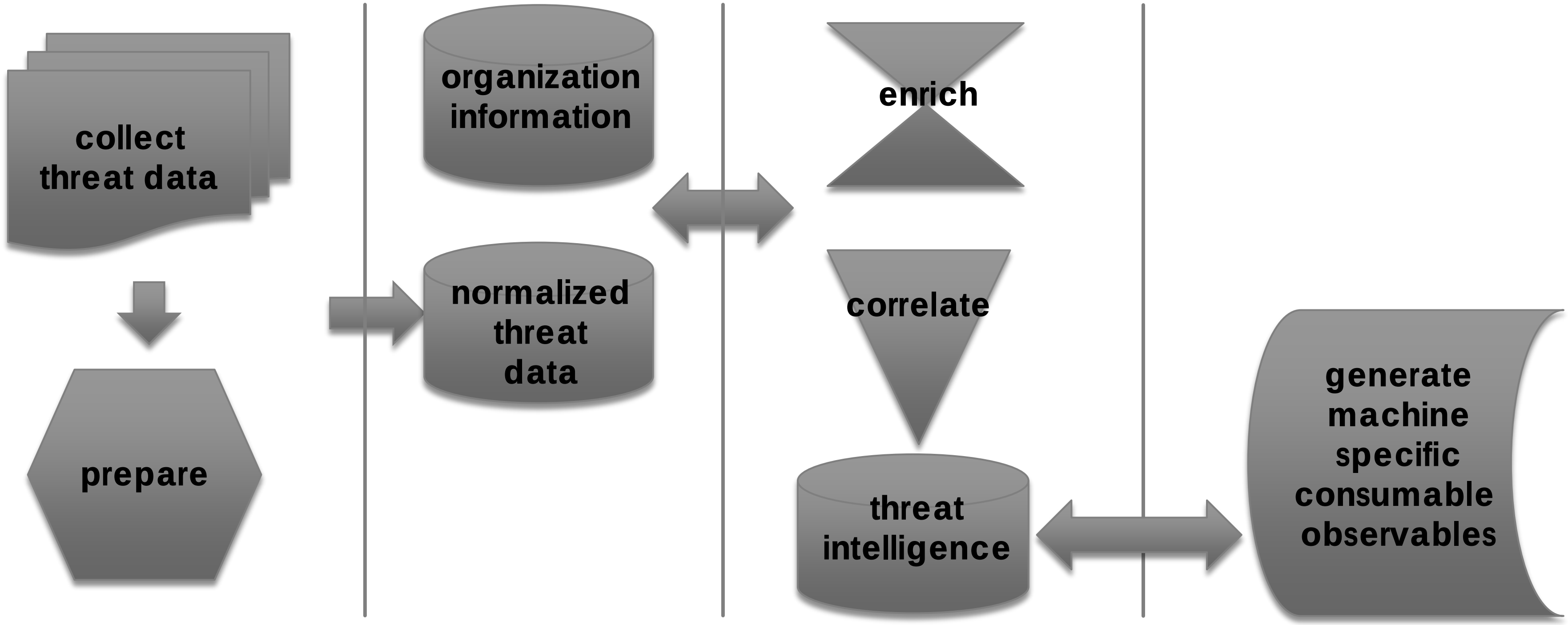
- “Foster the development and adoption of automated mechanisms for the sharing of information” – Executive Order – Promoting Private Sector Cybersecurity Information Sharing
- “Standardize data formats and transport protocols to help facilitate the interoperability needed for secure, automated exchange of incident data” – NIST Special Publication 800-150 (Draft), Guide to Cyber Threat Information Sharing (Draft)
- “Organization…actively shares information with partners to ensure that accurate, current information is being distributed and consumed to improve cybersecurity before a cybersecurity event” – Framework for Improving Critical Infrastructure Cybersecurity
- “SCAP was created to provide an automated approach to…examining systems for signs of compromise, and having situational awareness—being able to determine the security posture of systems and an organization at any given time” – NIST Special Publication 800-117, Revision 1 (Draft), Guide to Adopting and Using the Security Content Automation Protocol (SCAP) Version 1.2 (Draft)

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



Recent Contributions

- Draft NISTIR 8057, *Creating Windows Actionable Threat Indicators using Security Content Automation Protocol (SCAP) Version 1.2h*
  - 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
  - Dispels the myth that STIX and SCAP are competitors
  - Converts STIX-based indicators to machine-actionable content
  - Output is SCAP 1.2 content
  - Demonstrate that 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?

Demonstration next session!

Potential Issues

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

- Indicator Availability
  - Who would generate? Who would share? Who would publish? What to share?
- Automation Impacts
  - To what extent are users willing and able to automate their processes?
- Industry Impacts
  - User costs? Vendor incentives? Practical impacts? Business model impacts?
- Unintended Consequences
  - New vulnerabilities? Self-imposed denial-of-service?

Panelists

- **Ron Nielson**, Technical Director / SHARKSEER Program Manager, Department of Defense,
- **Tom Millar**, Communications Chief - US-CERT, US Department of Homeland Security
- **Jim Hanson**, Director of Engineering and Development, Cyber Engineering Services, Inc.
- **Paul Green**, CEO/President, G2, Inc.