Automation Specifications Overview

Paul Cichonski

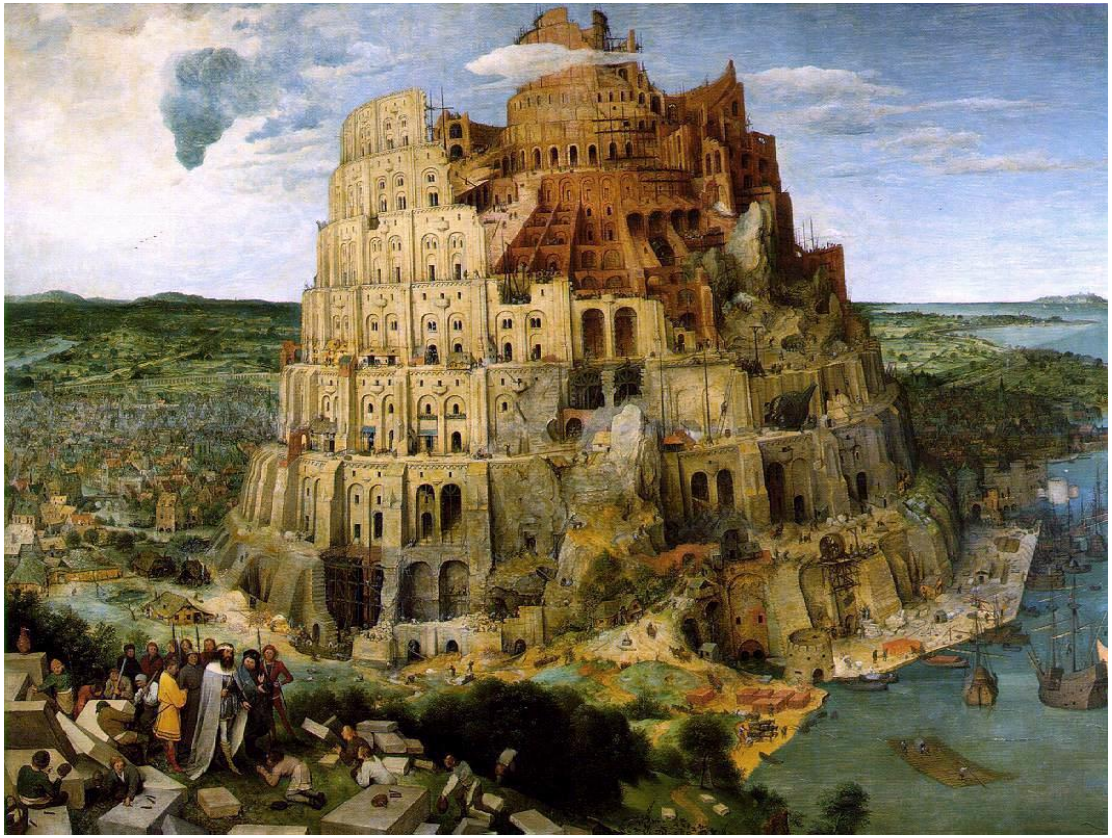
Booz Allen Hamilton

National Institute of Standards and Technology (NIST)

Security Automation: the Challenge

- Many disparate tools exist in IT security
  - Producing and consuming data in proprietary formats
  - Lack of interoperability between tools
- Many disparate domains exist in IT security
  - Each domain consists of distinct information objects
  - Lack of integration across domains

“Tower of Babel” Problem Exists



- Too much proprietary, incompatible information
  - error prone
  - difficult to scale
- Creates Inefficiencies
  - costly
  - resources spent on creating “glue code”

Security Automation: the Solution

- Standardization:
  - Provided through automation specifications
  - Same Object, Same Name
  - Reporting
- Automation:
  - Efficiency
  - Accuracy
  - Resources re-tasked to harder problems:
    - Incident response
    - Infrastructure enhancement

Agenda

- What is the goal of standardization?
- What domains has Security Automation standardized so far?
- What new domains are being standardized now?
- What domains do we need to standardize in the future?
- What are the individual specification efforts for the domains covered in this track?

Standards provide the infrastructure for sharing knowledge

- Standards are meant to serve as the infrastructure *within a single* community of practice.
  - Common naming of things and relationships (i.e. the nouns and verbs of the community).
  - Common naming applies to all levels of the community from very specific to very general.
- Standards are meant to serve as the communication infrastructure *across multiple* disparate communities of practice.
  - Common naming is usually limited to the general things shared across the disparate communities (e.g. boundary objects)
  - Allows knowledge to be shared across heterogeneous domains
- Infrastructure should be hidden!

Standardization provides the foundation for data interoperability

- Communication across domain, or organizational boundaries can only occur if there is common naming.
  - This is true for both machine-oriented and human-oriented activities.
  - Machines only benefit if common naming is unique and unambiguous.
- Use case specific functionality may be built on the foundation standardization provides.
  - Communication of information across organizational boundaries (e.g. compliance reporting).
  - Communication of information across domain boundaries (e.g. horizontal interoperability).

Important Definitions

- **Security Automation Domain**: *any common grouping of objects / entities that describe a particular topic in the IT security industry.*

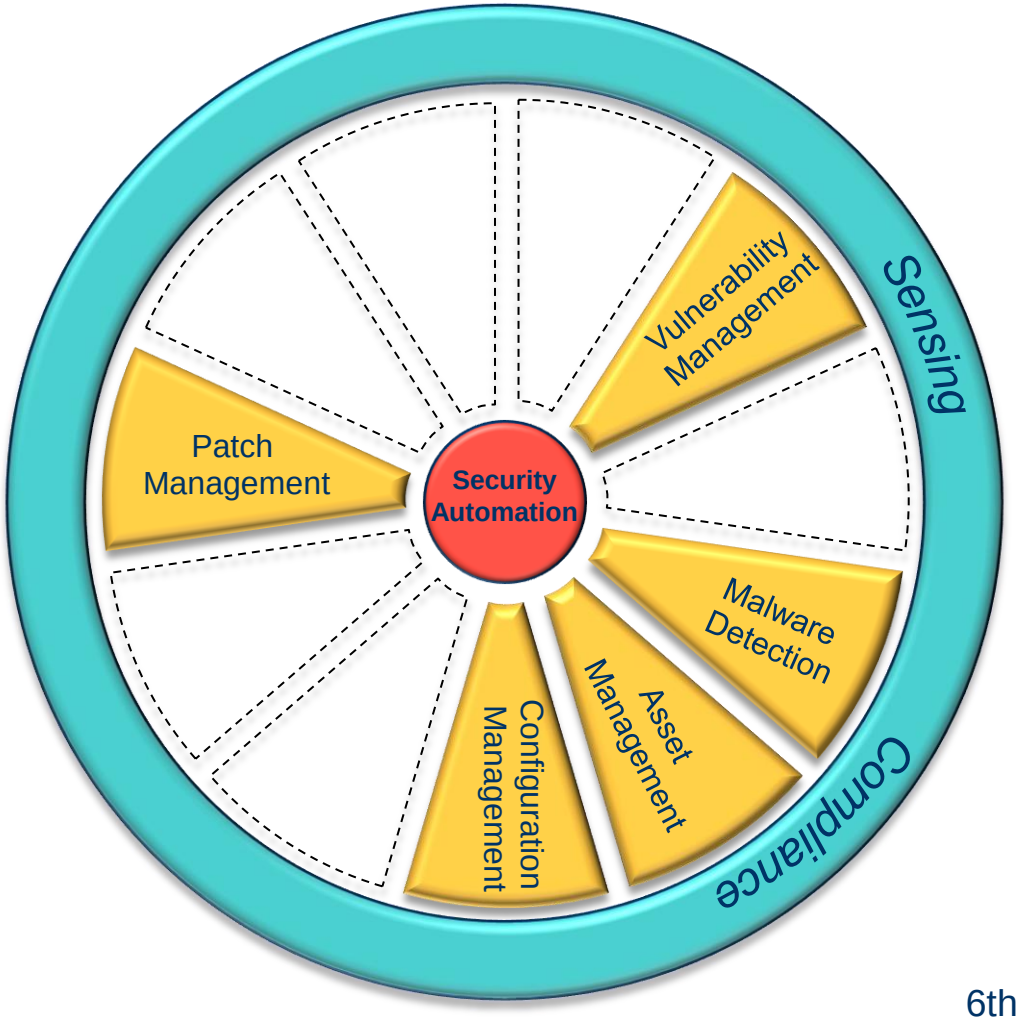
- **Security Automation Activity**: any cross-cutting *operation relating to the tasking, manipulation, or communication of Security Automation Domain data between tools.*

Examples of Domains and Activities

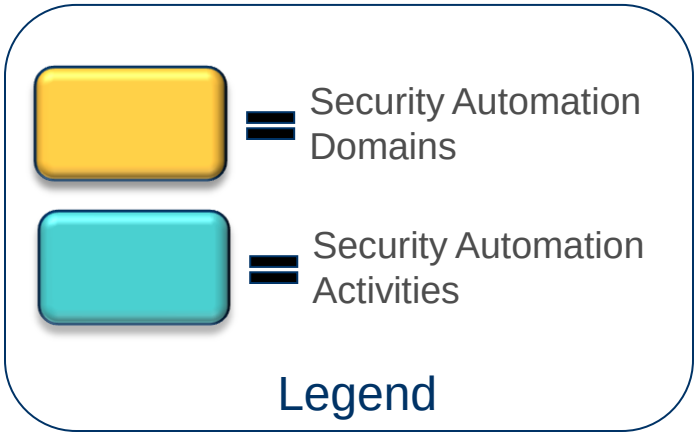
Security Automation Domains	Security Automation Activities
• Vulnerability Management • Configuration Management • Malware Detection • Software Assurance • Event Management • Asset Management • Network Management • Incident Management • Patch Management • License Management • Information Management	• Sensing • Compliance • Remedy • Reporting • Orchestration

* *Activities function on the information captured within, or across, the various domains.*

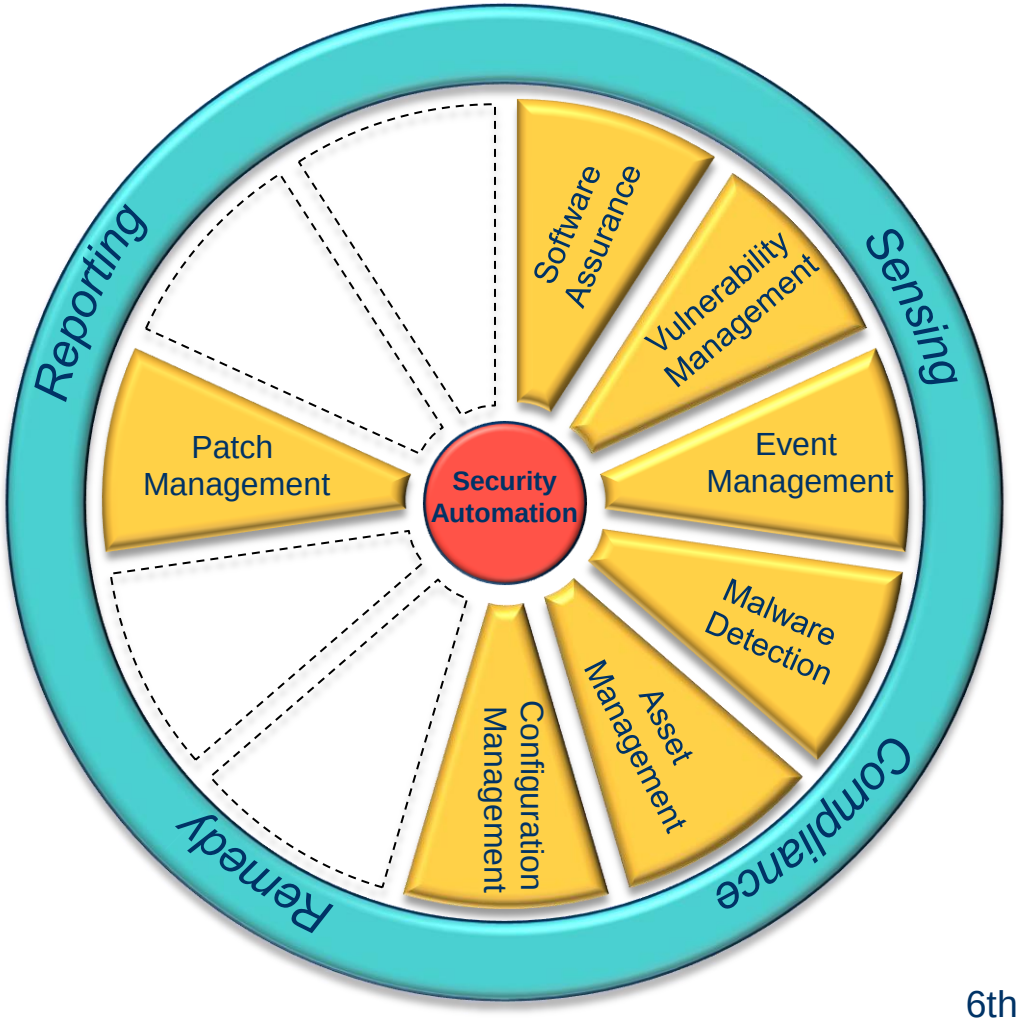
Past Scope of Security Automation Program



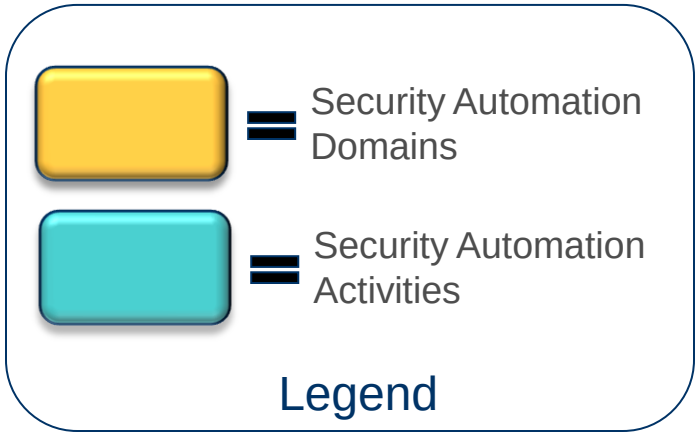
- Past work has been largely focused on domains relating to network endpoints.
- While this work is maturing, a lot of work still remains within these domains / activities.



Current Scope of Security Automation Program

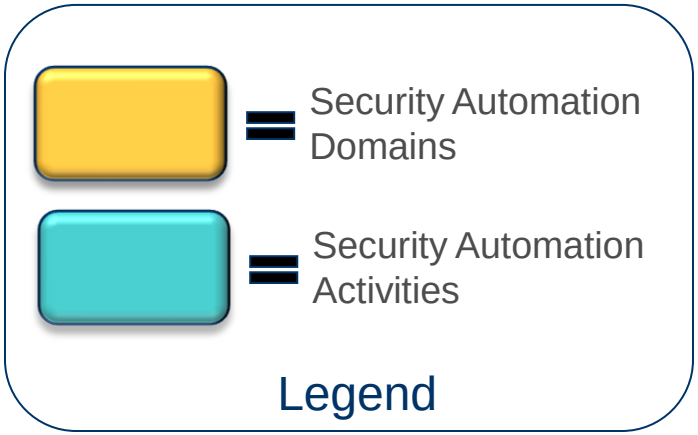


- Current work is expanding into Software Assurance, Asset and Event Management space.
- Efforts are also underway to standardize the way Reporting and Remediation data is communicated.

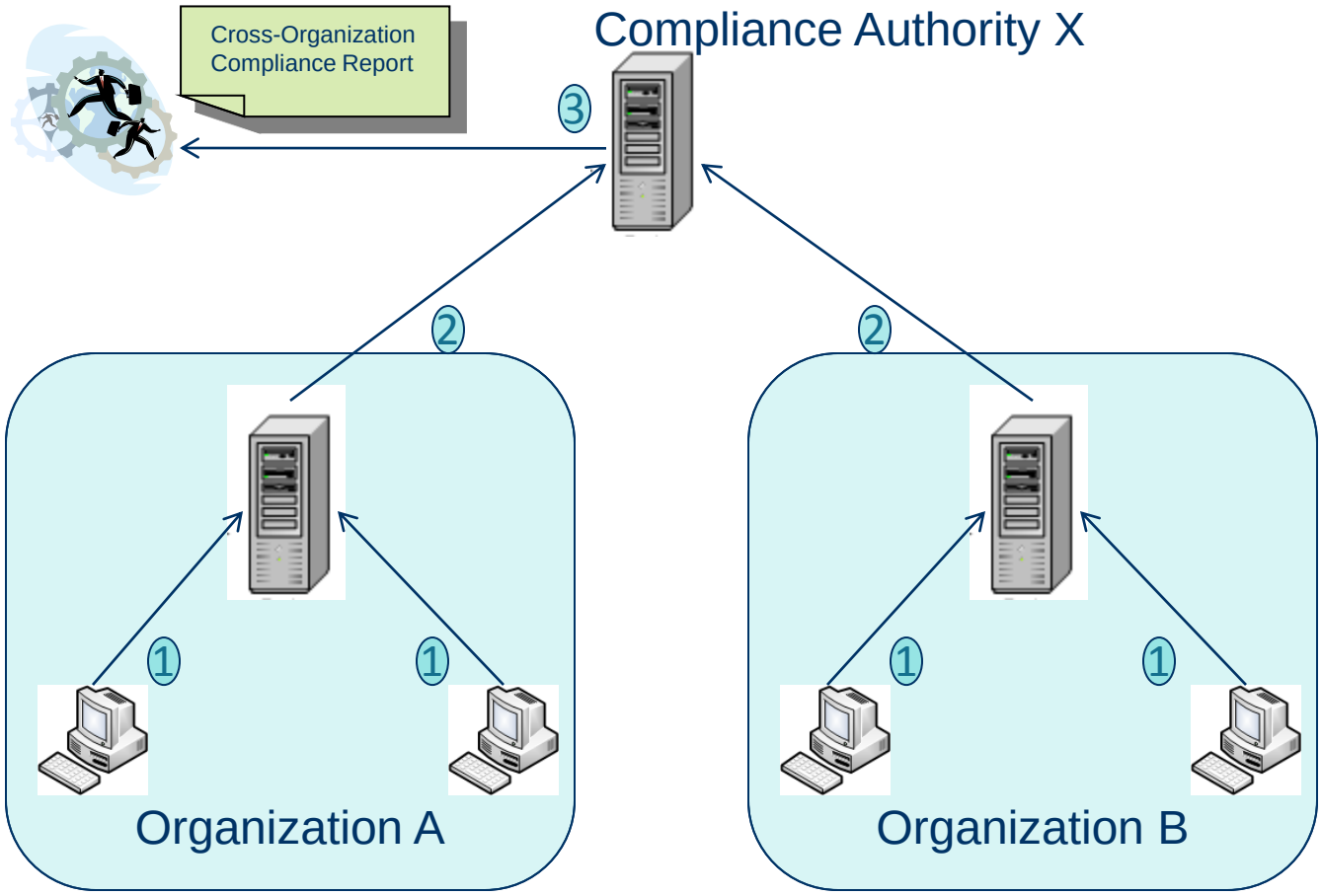


Future Scope of Security Automation Program

- Future work may expand into even more domains / activities than those listed here.
- Security Automation specifications are required in each domain/activity area to ensure true interoperability across the IT security landscape.



Use Case: Compliance Reporting

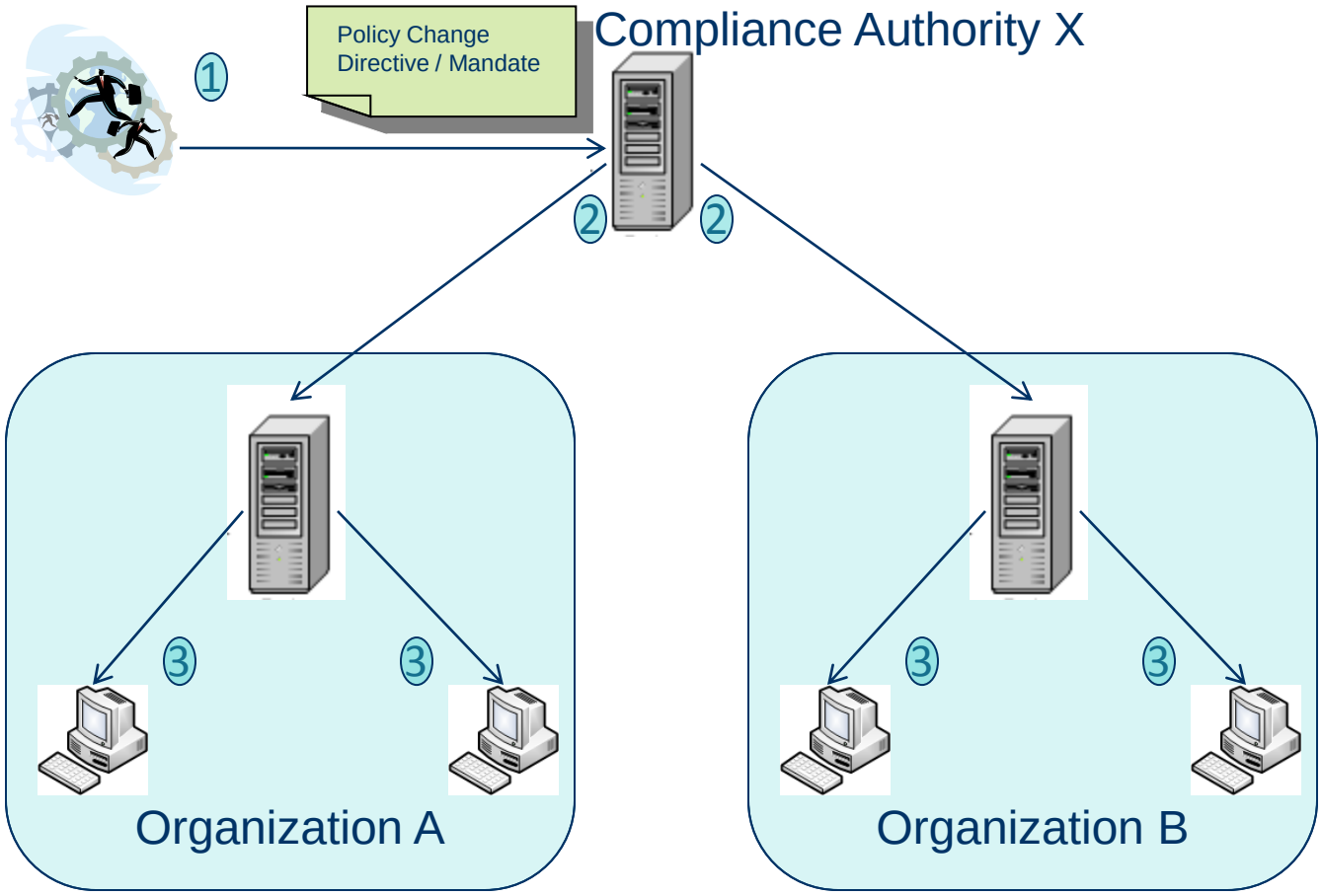


1. Endpoints within an organization periodically report their compliance to a policy mandated by Compliance Authority X. This is done automatically.

2. Multiple organizations periodically report their compliance to Compliance Authority X's Policy in an automated fashion.

3. Compliance Authority X's systems deliver compliance report detailing current compliance state for all organizations that must adhere to it's policy.

Use Case: Policy Enforcement

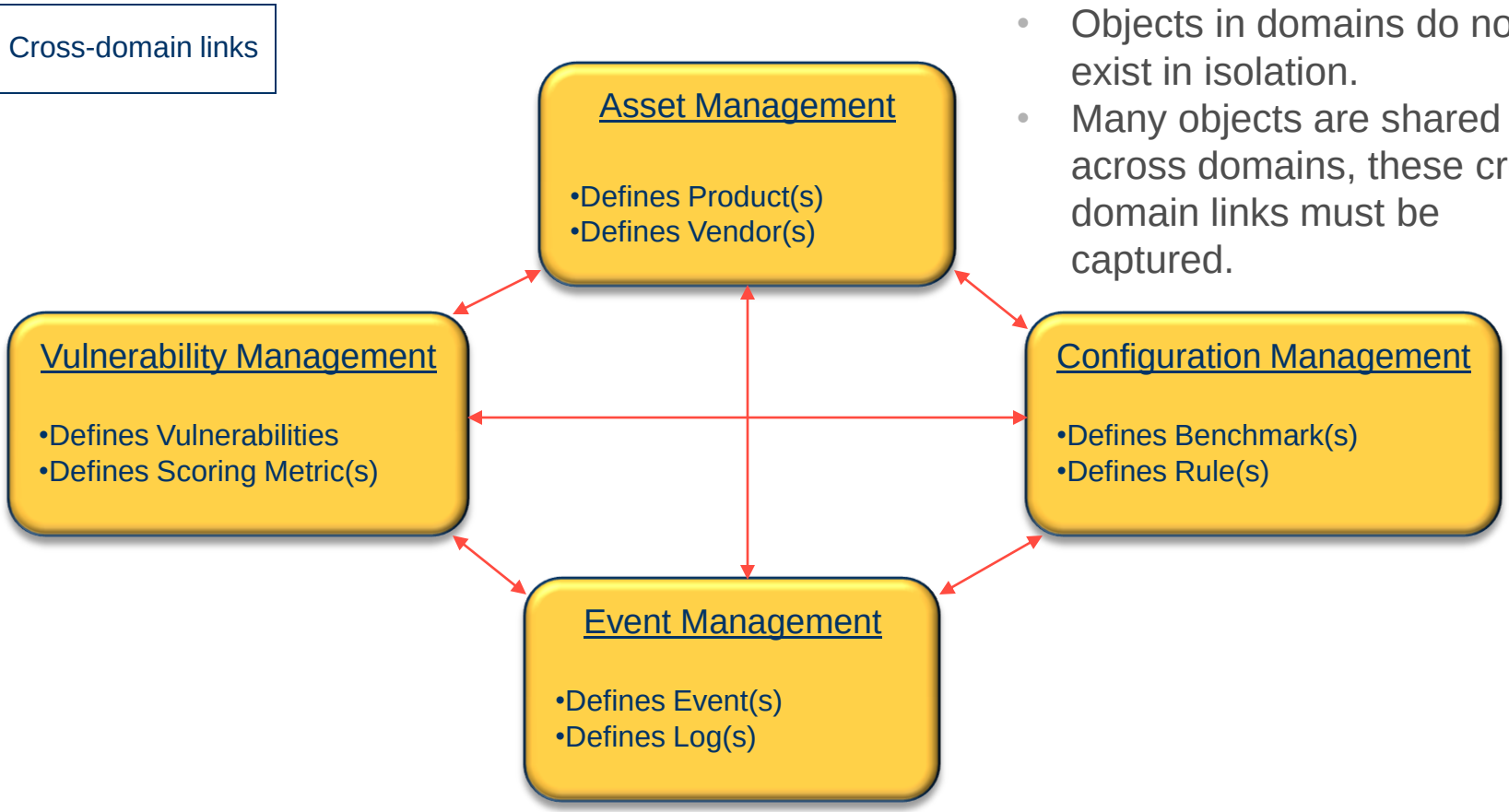


1. Policy Creator at Authority X issues a policy change effecting organizations under the authority's purview .

2. Systems from Compliance Authority X send the machine-readable policy change to all affected organizations.

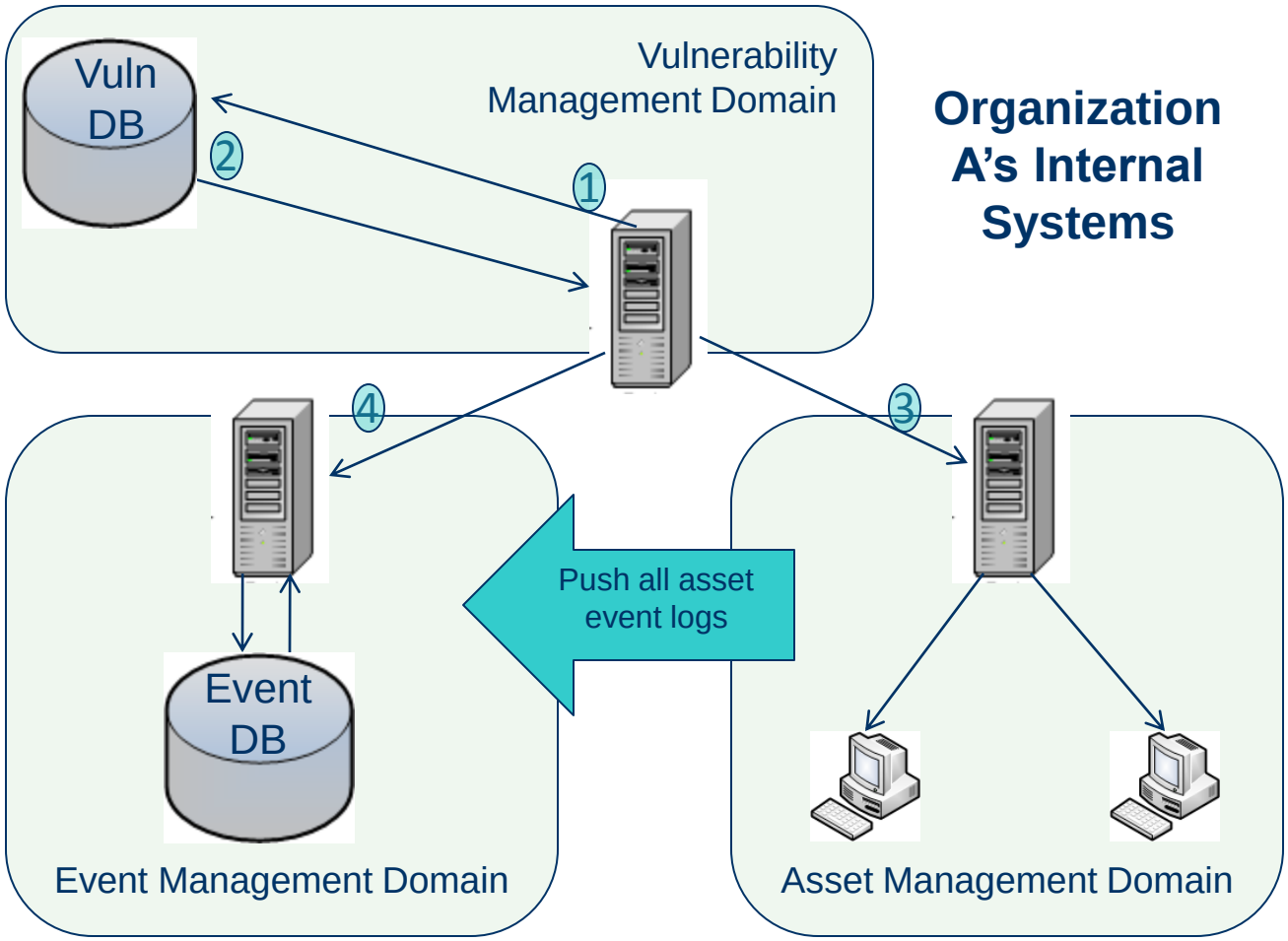
3. Individual organizations process policy change and use remediation tools to automatically implement policy on affected endpoints.

Connections between domains are necessary to share knowledge across domain boundaries



- Objects in domains do not exist in isolation.
- Many objects are shared across domains, these cross-domain links must be captured.

Use Case: Horizontal Interoperability



1. Vulnerability management system in Organization A polls public vulnerability database for information on new vulnerability.
2. Vulnerability database returns data asserting what products the vulnerability is found on, and what events the exploitation of that vulnerability produce.
3. Vulnerability management system asks asset management system if applicable products exist on the network
4. Vulnerability management system asks event management system if events exist to prove vulnerability was exploited on network

What is SCAP? (1 of 4)

The **S**ecurity **C**ontent **A**utomation **P**rotocol:

- Security Automation Program's first specification suite – focused on standardizing communication of endpoint related data – **Still Evolving!**
- Created to bring together existing specifications and to provide a standardized approach to maintaining the security of enterprise systems.
- SCAP ...
  - provides a means to identify, express and measure security data in standardized ways.
  - is a suite of individually maintained, open specifications
  - defines how these specifications are used in concert

What is SCAP? (2 of 4)

- Domains SCAP is focused on standardizing include:
  - Configuration Management
  - Vulnerability Management
  - Asset Inventory (subset of Asset Management)
  - Malware Detection
  - Patch Management
- Activities SCAP is focused on standardizing include:
  - Sensing
  - Compliance

What is SCAP? (2 of 4)

SCAP™

Languages
Means of providing instructions

- Community developed
- Machine readable XML
- Reporting
- Representing security checklists
- Detecting machine state

XCCDF security benchmark automation

OVAL Open Vulnerability and Assessment Language

Metrics
Risk scoring framework

- Community developed
- Transparent
- Metrics
  - Base
  - Temporal
  - Environmental

CVSS

Enumerations
Convention for identifying and naming

- Community developed
- Product names
- Vulnerabilities
- Configuration settings

CVE cve.mitre.org

CCE™

CPE™ common platform enumeration

What is SCAP? (3 of 4)

MITRE	cve.mitre.org	CVE	Common Vulnerability and Exposures	Standard nomenclature and dictionary of security related software flaws
MITRE		CCE	Common Configuration Enumeration	Standard nomenclature and dictionary of software misconfigurations
MITRE	common platform enumeration	CPE	Common Platform Enumeration	Standard nomenclature and dictionary for product naming
NSA	XCCDF security benchmark automation	XCCDF	eXtensible Configuration Checklist Description Format	Standard XML for specifying checklists and for reporting results of checklist evaluation
MITRE	OVAL	OVAL	Open Vulnerability and Assessment Language	Standard XML for test procedures
MITRE		OCIL	Open Checklist Interactive Language	Standard XML for human interaction
FIRST	CVSS	CVSS	Common Vulnerability Scoring System	Standard for measuring the impact of vulnerabilities

The Core SCAP Publications

The NIST has publications on SCAP available on its Computer Security Resource Center (CSRC) website:

- **SP800-117**: Guide to Adopting and Using SCAP, May 5, 2009.
- **SP800-126**: The Technical Specification for the SCAP 1.0, November 2009.
- **SP800-126 Rev 1**: The Technical Specification for the SCAP 1.1 (Draft), May 27, 2010.
- **IR-7511 Rev 1**: DRAFT SCAP Validation Program Test Requirements, Apr. 21, 2009.

SCAP Specification Timeline

	SCAP 1.0	SCAP 1.1	SCAP 1.2
Scheduled Release Date	Currently Final	Q4, 2010 – Final Version	Q1, 2011 – Initial Draft
Included Specifications	• CVE • CCE 5.0 • CPE 2.2 • XCCDF 1.1.4 • OVAL 5.3, 5.4 • CVSS 2.0	• CVE • CCE 5.0 • CPE 2.2 • XCCDF 1.1.4 • OVAL 5.3, 5.4, 5.5, 5.6, 5.7, 5.8 • CVSS 2.0 • OCIL 2.0	• CVE • CCE 5.0 • CPE 2.3 • XCCDF 1.2 • OVAL 5.3, 5.4, 5.5, 5.6, 5.7, 5.8 • CVSS 2.0 • OCIL 2.0 • ARF 1.0 • AI 1.0

** The release dates of future SCAP revisions and the inclusion of specific component specifications is tentative and subject to change.*

Automation Specifications Track - XCCDF

e**X**tensible **C**onfiguration **C**hecklist **D**escription **F**ormat

Time: Tuesday, 10:45AM

Speaker: Charles Schmidt (MITRE), XCCDF Lead

Highlights:

- High level description of XCCDF.
- An overview of the new features in the XCCDF 1.2 specification and how they will benefit the community
- Upcoming changes in the XCCDF Specification (beyond XCCDF 1.2).

Automation Specifications Track - CPE

Common **P**latform **E**numeration

Time: Tuesday, 11:45AM

Speaker: Brant Cheikes (MITRE), CPE 2.3 Lead

Highlights:

- High level description of CPE.
- Upcoming changes in the CPE Specifications (specifically relating to CPE 2.3).
- An overview of CPE 2.3 and the benefits it will provide to the community.

Automation Specifications Track - OVAL

Open **V**ulnerability and **A**ssessment **L**anguage

Time: Tuesday, 1:30PM

Speaker: Jon Baker (MITRE), OVAL Lead

Highlights:

- High level description of OVAL.
- Overview of new features in OVAL 5.6, which will be included in SCAP 1.1.
- Upcoming changes to the OVAL language (including OVAL 5.8 and beyond).

Automation Specifications Track - OCIL

Open **C**hecklist **I**nteractive **L**anguage

Time: Tuesday, 2:30PM

Speaker: Maria Casipe (MITRE), OCIL Lead

Highlights:

- High level description of OCIL.
- An overview of the use cases OCIL is designed to support, and what additional functionality it adds to SCAP 1.1.
- A brief discussion of future plans for OCIL.

Automation Specifications Track - ARF / AI

Asset **R**eporting **F**ormat / **A**sset **I**dentification

Time: Monday, 3:45PM

Speakers: John Wunder (MITRE) and Adam Halbardier (Booz Allen Hamilton)

Highlights:

- An overview of the purpose, scope, use cases and data models for ARF and AI.
- How ARF and AI are helping to standardize reporting within Security Automation.

Beyond SCAP

Security Automation efforts are also focused on standardizing IT security domains / activities beyond the endpoint-centric scope of SCAP.

Domain: Event Management*

- Standardizing the communication of network events and logs.
- Standardizing the processes around analyzing network events and logs.

Activity: Remediation*

- Standardizing the representation of remediation events.
- Standardizing the tasking of remediation actions on a network.

**Additional work is also in progress, but is out of scope for this track.*

Automation Specifications Track – EMAP / CEE

Event **M**anagement **A**utomation **P**rotocol **/**
Common **E**vent **E**xpression

Time: Monday, 1:30PM

Speaker: William Heinbockel (MITRE)

Highlights:

- High level overview of EMAP specifications, with focus on CEE.
- Overview of ongoing development of a language for events.

Automation Specifications Track – The Use of Rules in EMAP

Event **M**anagement **A**utomation **P**rotocol

Time: Monday, 2:30PM

Speaker: George Saylor (G2)

Highlights:

- A description of ongoing research relating to the use of standardized rule expressions within EMAP.
- An overview of the relationship between the use of rules and the goals of EMAP relating to correlating, filtering, and searching logs.

Automation Specifications Track – Enterprise Remediation Automation

Time: Monday, 11:45AM

Speaker: Chris Johnson (NIST)

Highlights:

- An overview of the current work being done to create a suite of specifications to standardize the communication of remediation activity data.
- An overview of the use cases this new suite of specifications is aimed towards fulfilling.
- An overview of the component specifications within this remediation suite.

Automation Specifications Track – Vendor Interoperability Panel

Time: Monday, 4:45PM

Moderator: Tim Keanini (nCircle)

Panelists: Luis Nuñez (Cisco), Kent Landfield (McAfee), John Bordwine (Symantec), Jeff Spitulnik (IBM), Todd Dolinsky (HP)

Highlights:

- Hear thoughts from vendors in the Security Automation community relating to their perspective and experience relating to using the specifications within the Security Automation Community.
- An overview of what it is really like to be a vendor supporting Security Automation specifications.

Automation Specifications Track – NCP

National Checklist Program

Time: Tuesday, 3:45PM

Speaker: Chuck Wergin (Booz Allen Hamilton), Harold Owen (G2)

Highlights:

- An overview of NCP and how it has evolved into the a repository of SCAP expressed security configuration checklists.
- New NCP features designed to categorize and filter SCAP content.
- An overview of a new web-based and web-service based system to allow external parties to manage their checklists within NCP.

Additional Resources

NIST Websites:

- SCAP Homepage: http://scap.nist.gov
- SCAP Validated Tools: http://nvd.nist.gov/scapproducts.cfm
- SCAP Validation Homepage: http://nvd.nist.gov/validation.cfm
- National Checklist Program: http://checklists.nist.gov
- National Vulnerability Database: http://nvd.nist.gov
- NIST Computer Security Resource Center (CRSC) http://csrc.nist.gov/publications/PubsSPs.html

Questions & Answers / Feedback

Paul Cichonski

Associate

Booz Allen Hamilton

Supporting National Institute of Standards and Technology (NIST)

paul.cichonski@nist.gov

(301) 975-6587