

# Security Information Standardization and Automation



John Banghart

National Institute of Standards  
and Technology

---

**NIST**



# The Challenge



## • Information Chaos

- Producing and consuming data in proprietary formats
- Lack of interoperability between tools and information domains

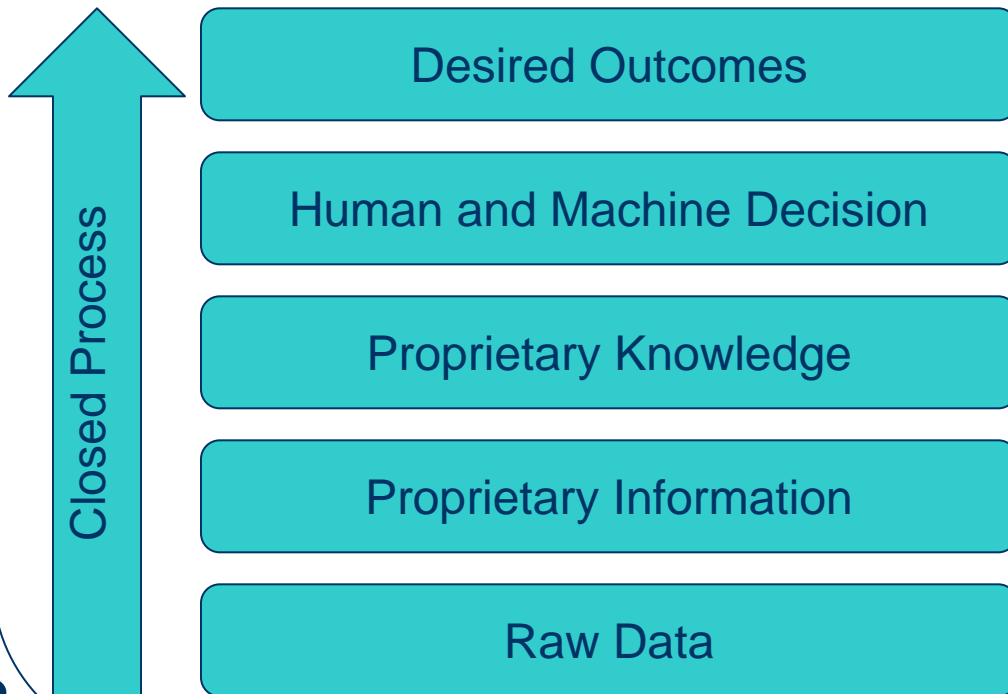
## • Inefficiency

- Resources spent on “maintenance” security
  - Patch Management
  - Configuration Management
  - Vulnerability Management
  - Compliance Management



# Traditional information sharing was bounded by the closed systems within an organization

## Closed System

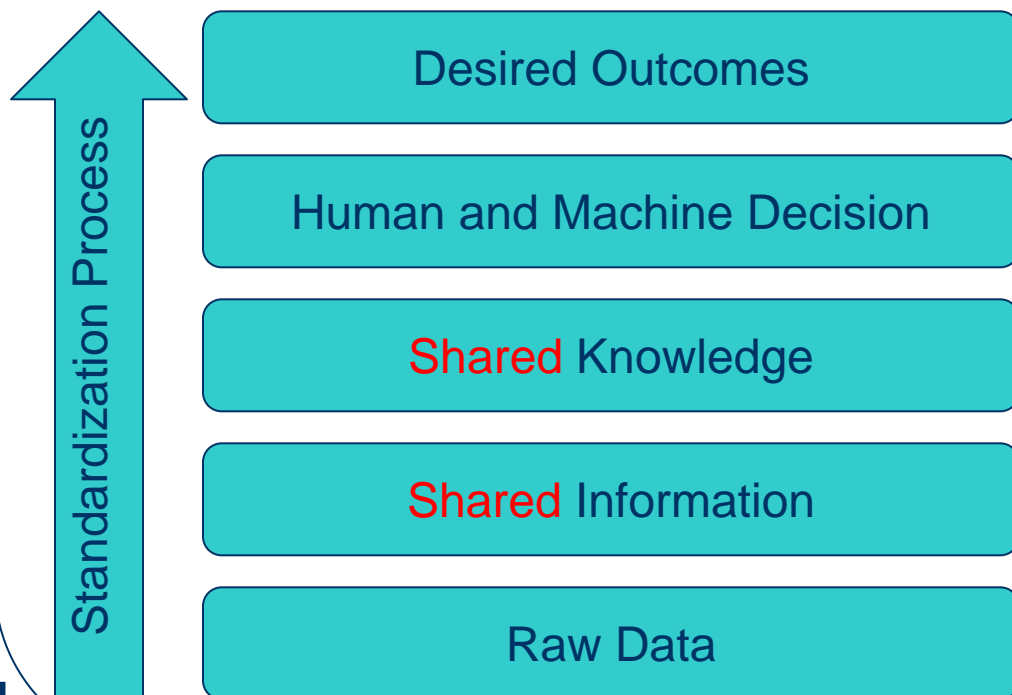


- Closed systems rely on proprietary process and information models to transmit knowledge.
- Scope of knowledge limited by boundaries within the system.
- Automation of decisions cannot occur outside the system itself.



# Systems that leverage standardized data communication may communicate with larger IT ecosystem

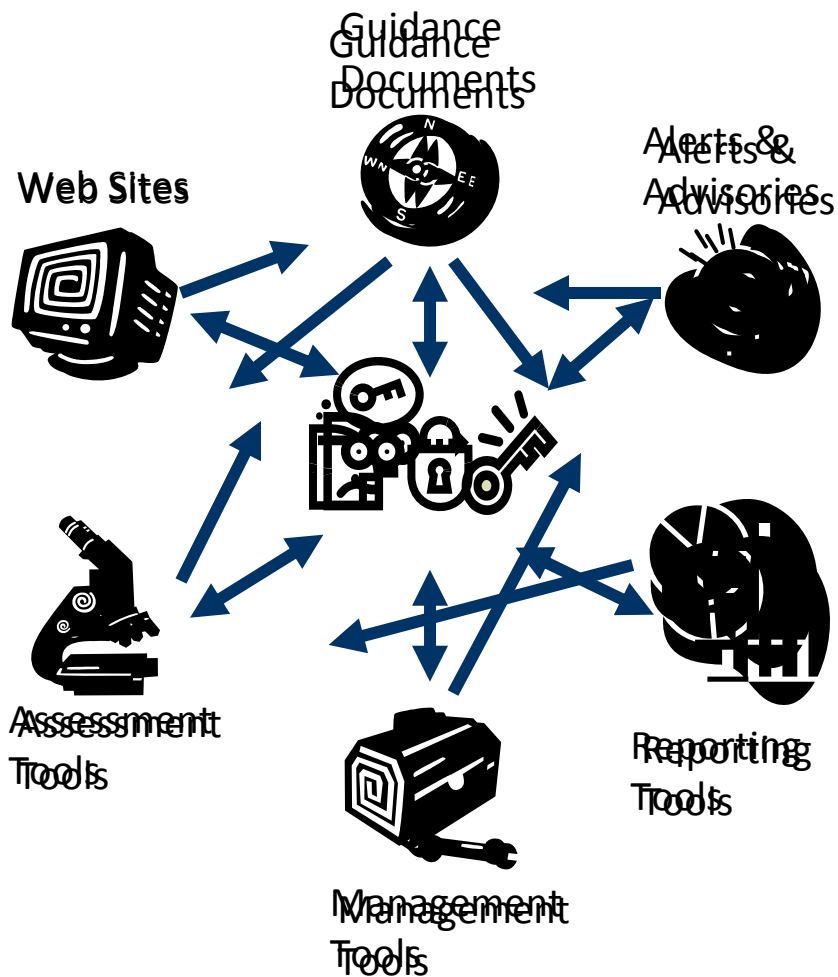
## Open System Leveraging Standards



- System leverages standards to define how information and knowledge is communicated.
- System may share knowledge across system boundaries.
- Automation of decisions can occur across a broad ecosystem of standard-driven systems.



# The Solution



## •Standardization:

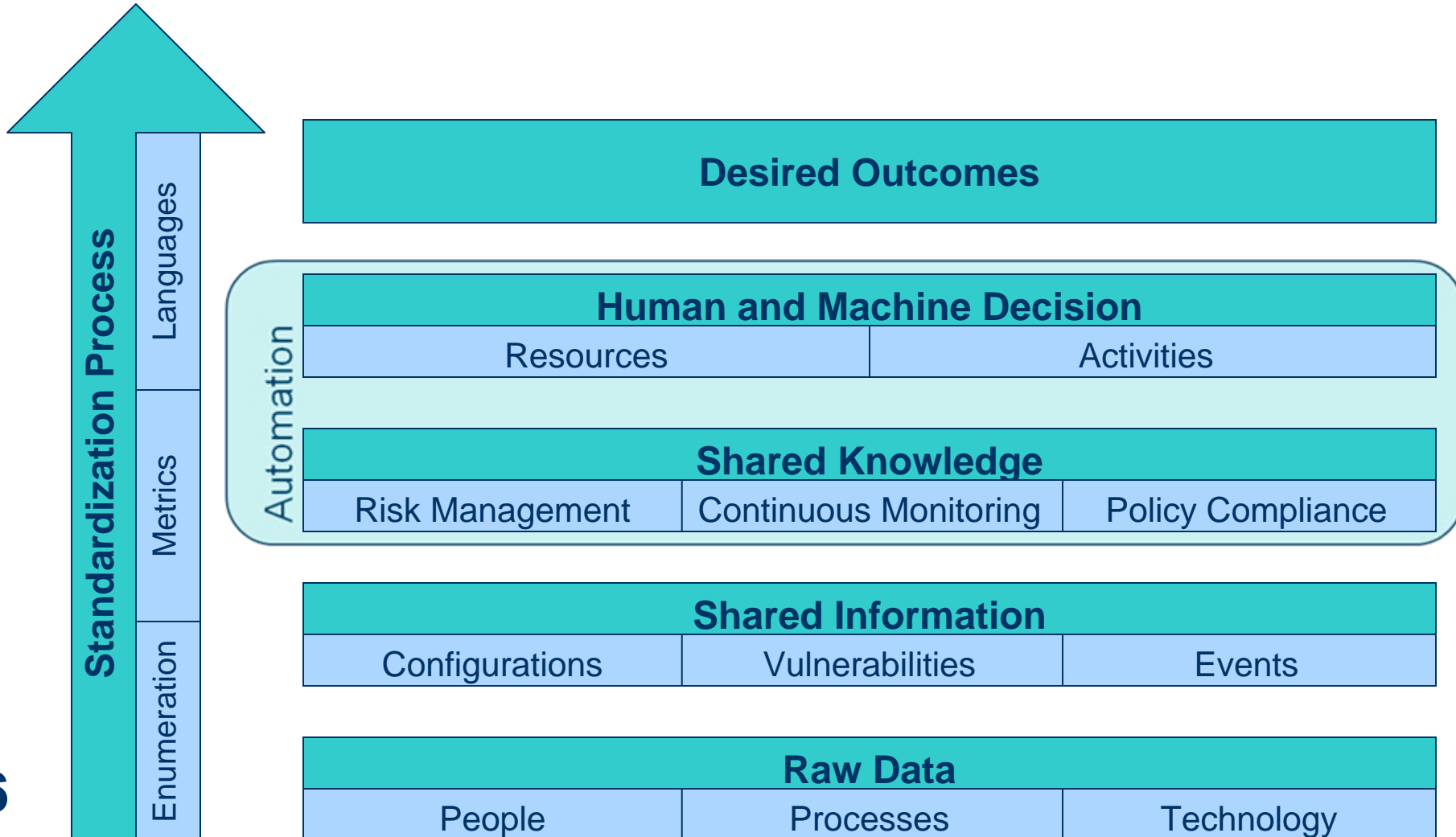
- Provided through technical specifications
- Common reference data
- Common reporting

## •Automation:

- Efficiency
- Accuracy
- Resources re-tasked to harder problems:
  - Incident response
  - Infrastructure enhancement

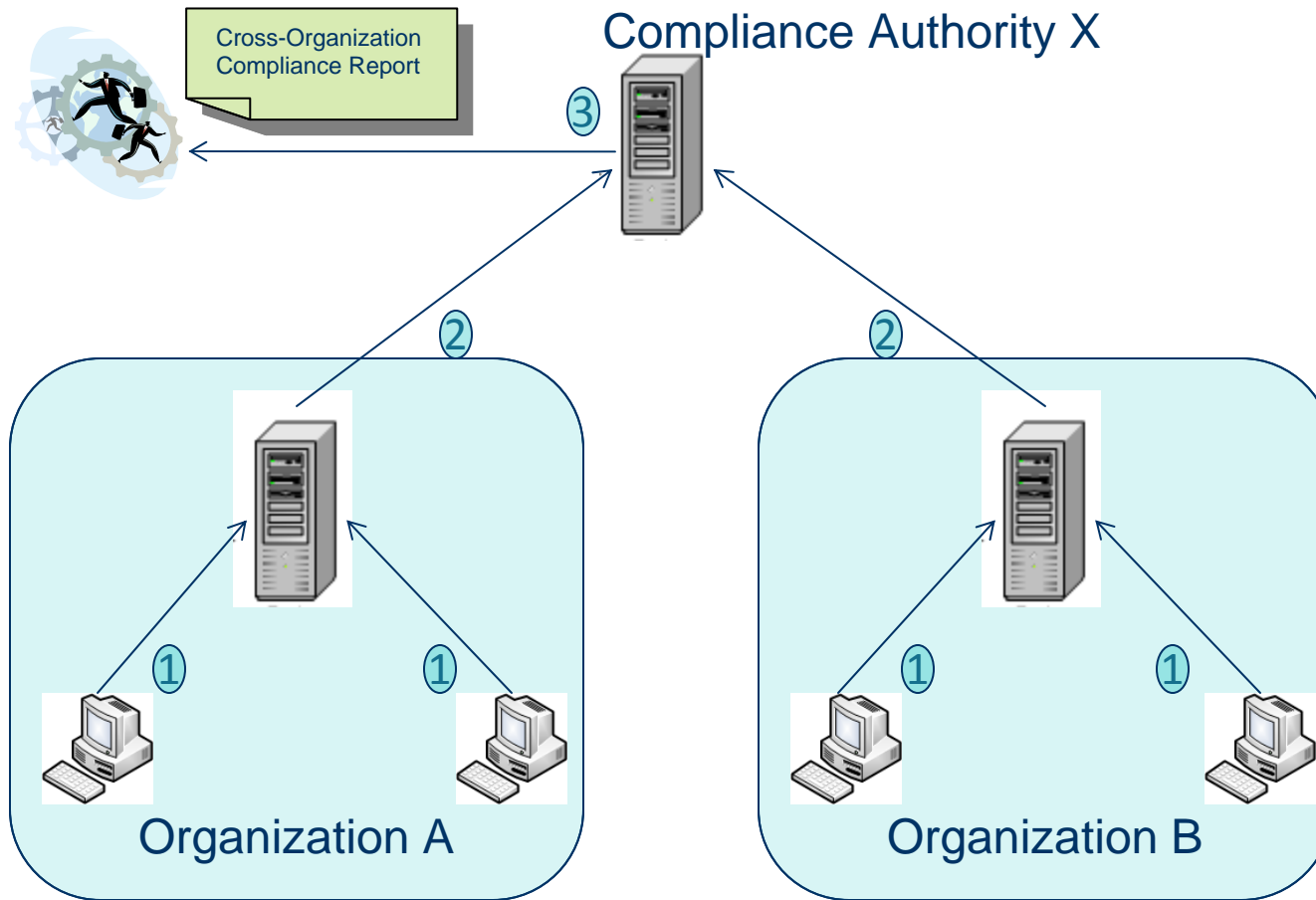


# Desired Outcomes from standardized systems





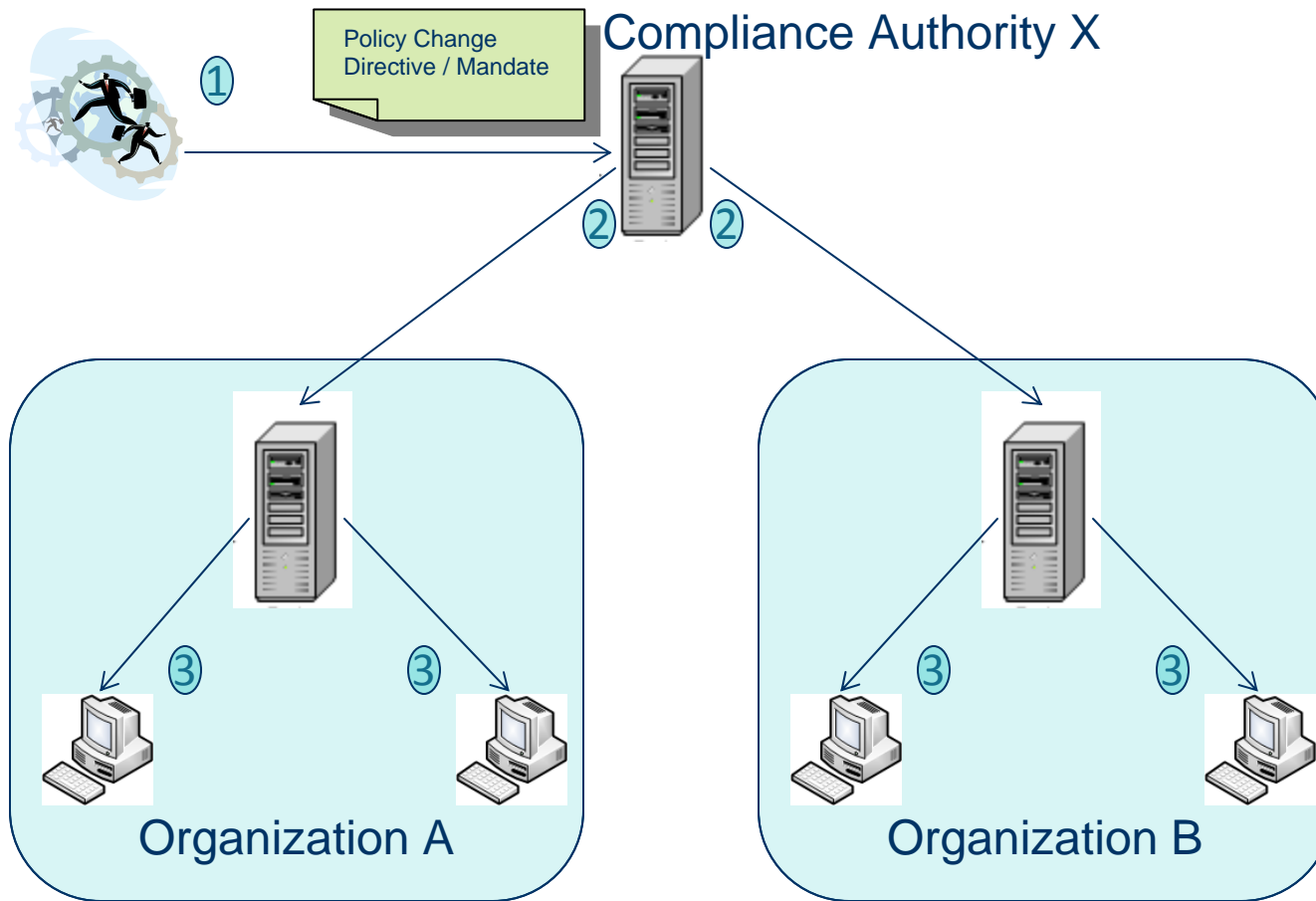
# Use Case: Compliance Reporting



- 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 its 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.





# What is SCAP? (1 of 3)

---

## 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 3)

---

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



# What is SCAP? (3 of 3)



## Languages

Means of providing instructions

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



## Metrics

Risk scoring framework

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



## Enumerations

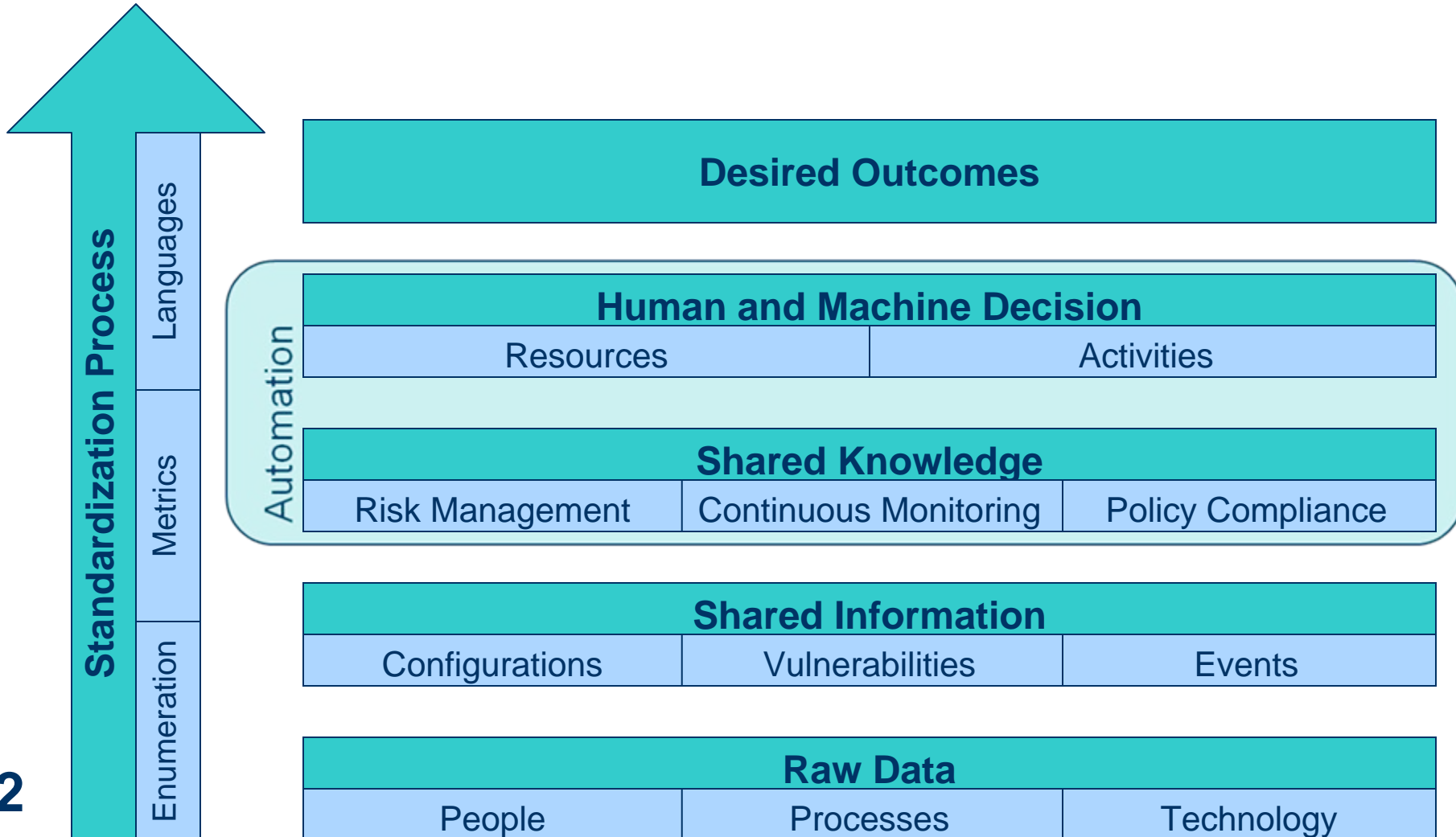
Convention for identifying and naming

- Community developed
- Product names
- Vulnerabilities
- Configuration settings



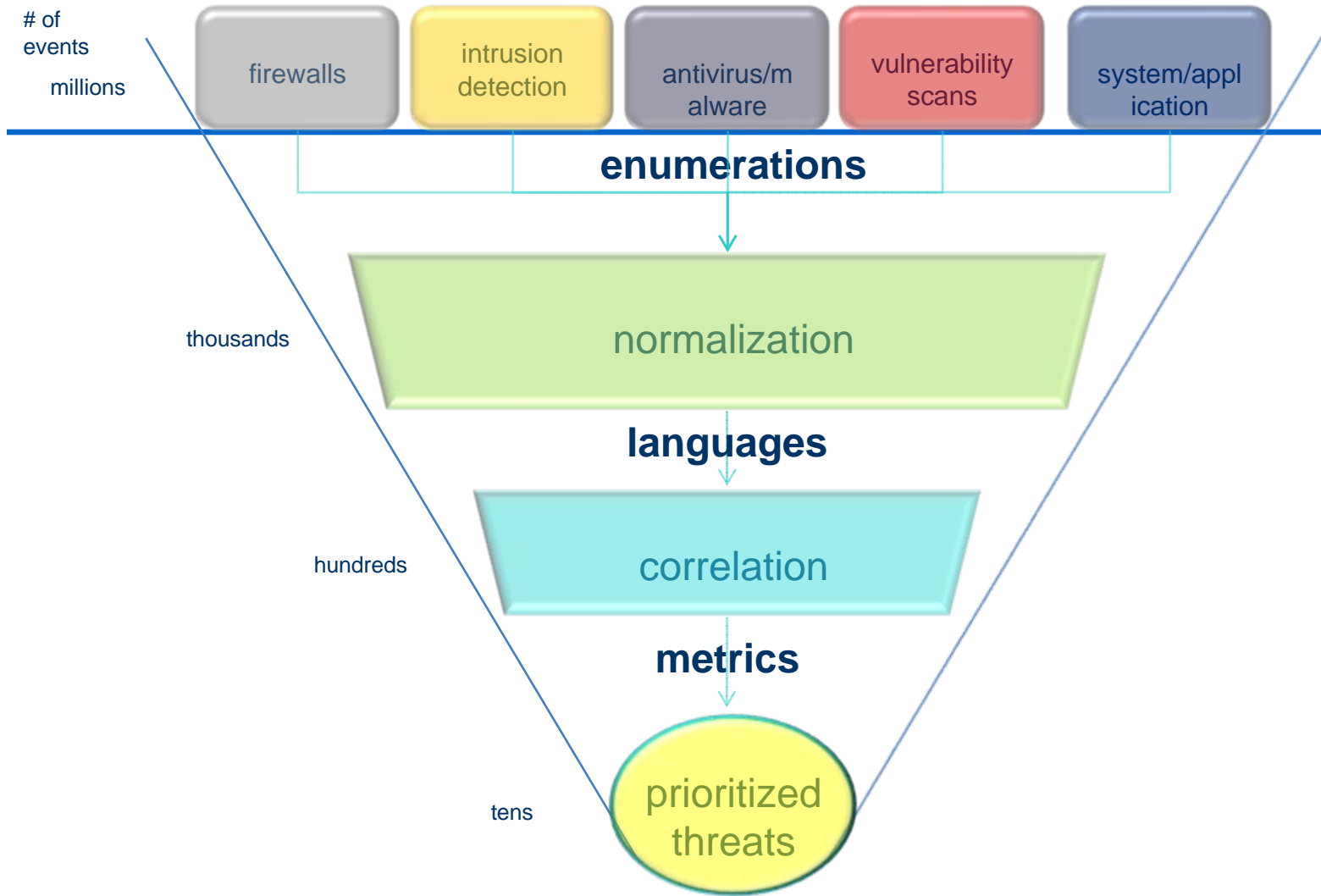


# Desired Outcomes from standardized systems



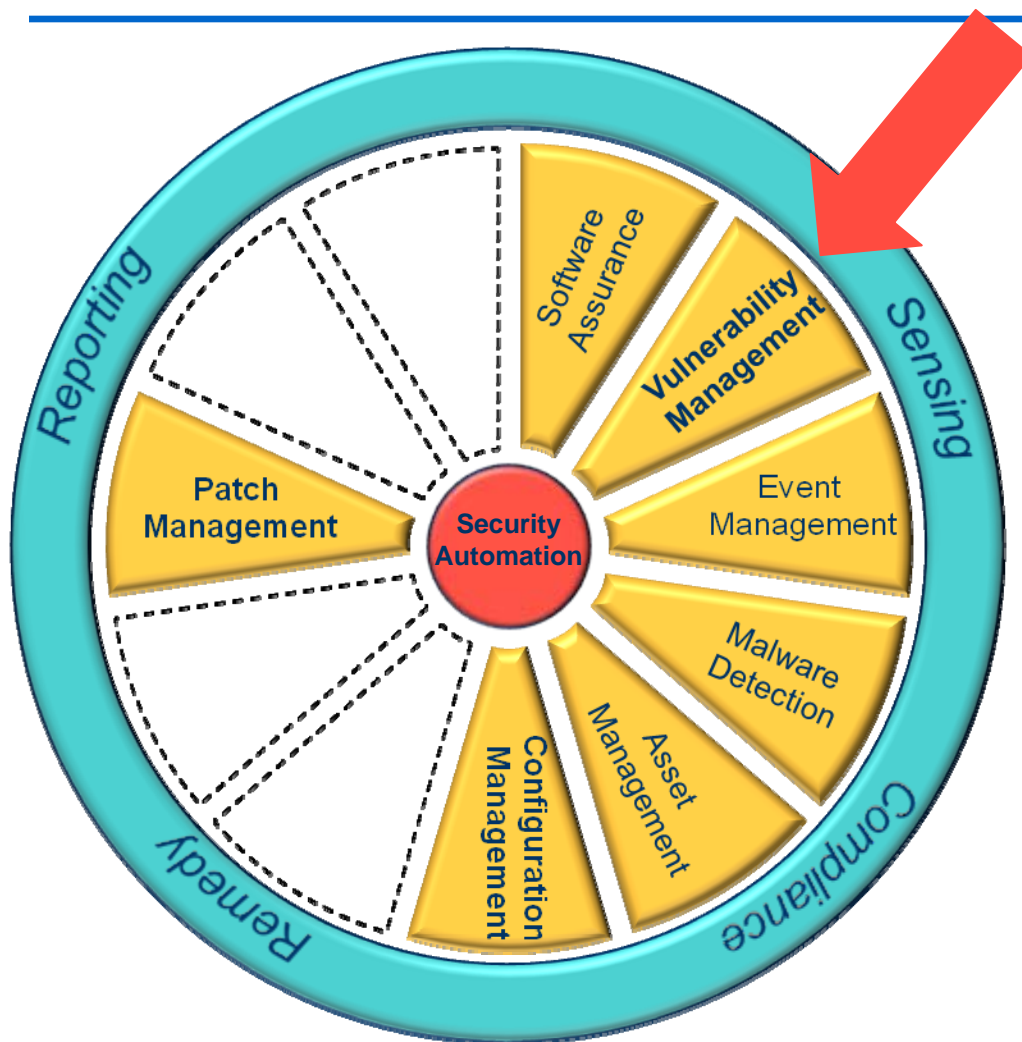


# Event Standardization







# 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.

 = Information Domains

 = Information Security Activities

Legend



# National Vulnerability Database (NVD)

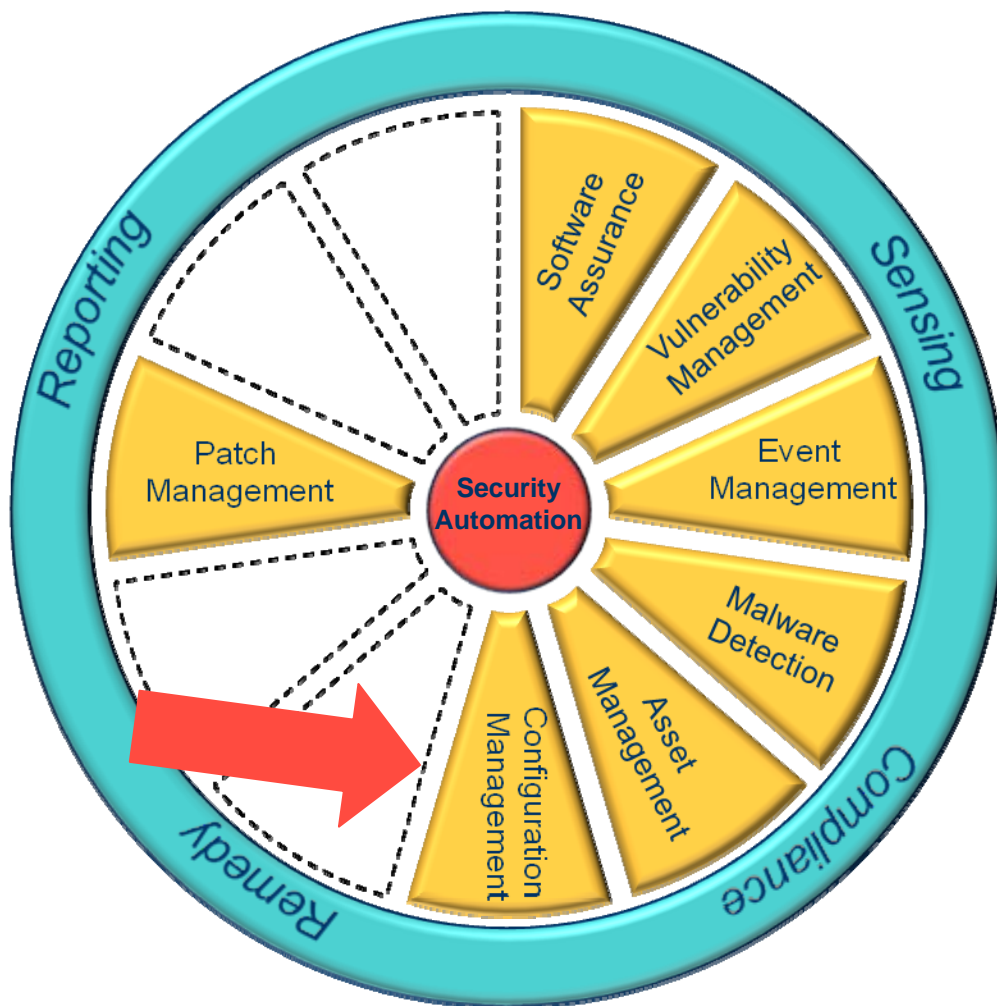
---

U.S. Government sponsored repository of public software vulnerability management information.

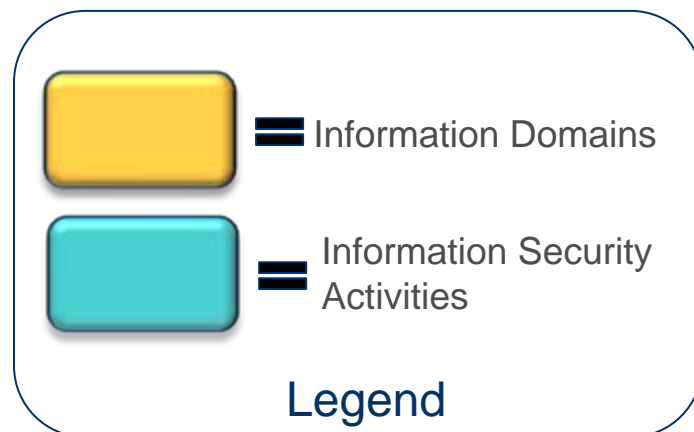
- Used by government, industry and academia worldwide
- Provides standardized reference for software vulnerabilities.
  - All tools refer to the same vulnerability when scanning, analyzing, and reporting
- Over 40,000 CVE entries with the NVD Analysis Team evaluating over 6,000 vulnerabilities a year
- <http://nvd.nist.gov>



# 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.







# National Checklist Program (NCP)

---

U.S. Government sponsored repository of publicly available security checklists

- Resources to support compliance management
- Security checklists cover over 175 products
  - Security automation content enables faster deployment in operational environments
- Checklist contributors include
  - Government organizations
  - Vendors
  - Non-profit organizations
- Part 39 of the Federal Acquisition Regulation (FAR)
- <http://checklists.nist.gov>



# US Government Configuration Baseline (USGCB) Use Case

---

- Evolution from FDCC for Windows XP and Vista
- CIO Council Technology Infrastructure Subcommittee (TIS)
  - TIS membership includes CISOs from every Federal Agency
- Windows 7 and Internet Explorer 8
  - Enterprise baseline configuration for all USG systems
  - Security Automation Content Protocol (SCAP): Enables SCAP-validated products to quickly assess and report system configuration and patch state compliance using open standards
  - Windows XP, Windows Vista, Internet Explorer 7 releases in April
- Baselines for other platforms planned
  - Red Hat Enterprise Linux (February)
  - Others in the future based on TIS requirements
  - Industry and various agency produced



# SCAP Validated Products

<http://nvd.nist.gov/scaproducts.cfm>

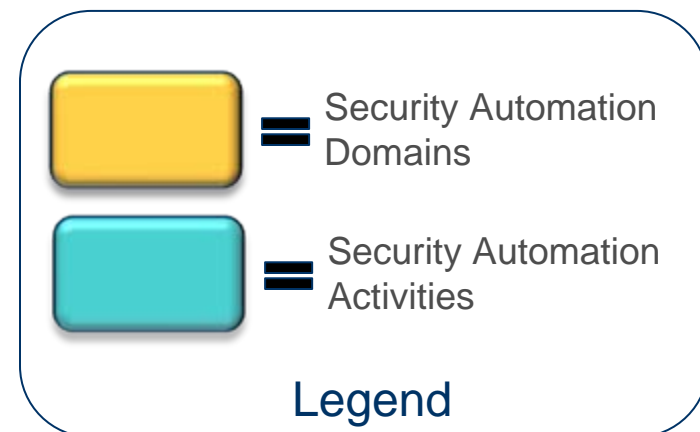




# Future Scope of Security Automation Program



- 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.





# Additional Resources

---

## NIST Websites:

- SCAP Homepage: <http://scap.nist.gov>
- SCAP Validated Tools: <http://nvd.nist.gov/scaproducts.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

---



**John Banghart**

National Institute of Standards and  
Technology (NIST)

[John.banghart@nist.gov](mailto:John.banghart@nist.gov)

(301) 975-8514