Security Automation Program Update

Cybersecurity Innovation Forum

September 10, 2015

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

Agenda

- What is security automation?
- What is the NIST Security Automation Program?
- Review NIST Security Automation Activities
- Conclusions
- How you can help?

What is security automation?

What is Security Automation?

“*We need a much greater focus on standardization and automation to allow humans to get out of the loop of manual defense and focus instead on human-worthy activities*” – Tony Sager

What is Security Automation?

"*We need a much greater focus on **standardization** and **automation** to allow **humans** to get out of the loop of manual defense and **focus** instead **on human-worthy activities***" – Tony Sager

Security automation is the **use** of data-driven **tools** to **manage** security controls and to **perform** well-understood **security tasks.**

Security automation includes**:**

- **Representing** human security **knowledge** as machine-readable data
- **Exchanging** machine-readable **data** to drive **automated action**
- Timely, scalable, and accurate **situational awareness** supporting **risk decision making**
  - Knowing what assets you have
  - Continuously knowing the operational state of these assets
  - Measuring the deployment and effectiveness of security controls

What is the NIST Security Automation Program?

The NIST Security Automation Program

Program Description

Supporting the creation and testing of standardized data sets and commercially available products that enable interoperable security automation solutions.

Goals

Enabling organizations to:

- Gain accurate and timely situational awareness over the state of their computing assets
- Measure security control effectiveness on an ongoing basis
- Measure compliance of endpoints to their risk-based policies
- Prevent and detect cyber-attacks

Activities

- Development of standards and guidelines
  - Data Models
  - Network Protocols
  - Implementation Guidance
- Hosting data repositories and data sets
  - Software Identification and Metadata
  - Vulnerability Information
  - Configuration Checklists
- Product Validation Program and Testing Tools
- Research
  - Measurement models
  - New methods and techniques

What is SCAP?

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

Brings existing specifications together to provide a **standardized approach for measuring** the security of enterprise systems

Provides a means to **identify, express, report,** and **measure** security data in standardized ways

Currently in 3rd revision – SCAP 1.2

- Defined by Special Publication (SP) 800-126 revision 2
- Project website: http://scap.nist.gov

What is SCAP?

Community developed specifications for:

Languages

Means of providing instructions

- Machine-readable XML
- Representing security checklists
- Detecting and reporting machine state

Metrics

Risk scoring framework

- Transparent
- Metrics
  - Base
  - Temporal
  - Environmental

Enumerations

Identification and naming

- Product names
- Vulnerability identifiers
- Configuration settings

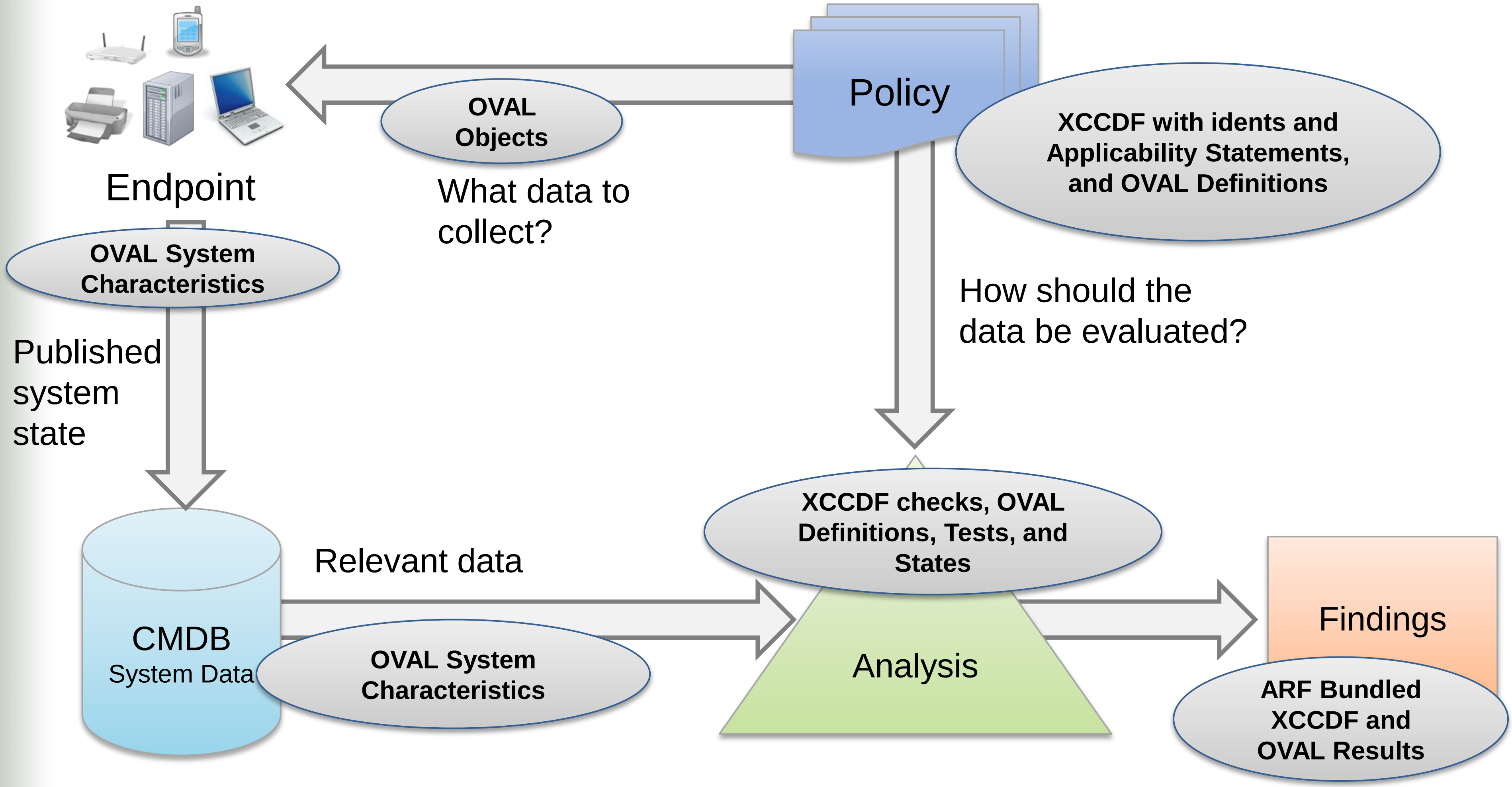
Integrity

Conventions for applying existing and emerging XML signature standards and best practices to sign and verify content

What is SCAP?

Naming	CVE	**Common Vulnerability Enumeration**	Standard nomenclature and dictionary of security related software flaws
	CCE	**Common Configuration Enumeration**	Standard nomenclature and dictionary of software misconfigurations
	CPE	**Common Platform Enumeration**	Standard nomenclature and dictionary for product naming
Expressing	XCCDF	**eXtensible Checklist Configuration Description Format**	Standard XML for specifying checklists and for reporting results of checklist evaluation
Assessing	OVAL	**Open Vulnerability and Assessment Language**	Standard XML for test procedures
	OCIL	**Open Checklist Interactive Language**	Standard XML for human interaction
Scoring	CVSS	**Common Vulnerability Scoring System**	Standard for measuring the characteristics and impacts of vulnerabilities
	CCSS	**Common Configuration Scoring System**	Metrics for software security configuration vulnerabilities
Reporting		**Asset Identification**	Method to identify assets based on known identifiers and/or other information
	ARF	**Asset Reporting Format**	Data format to relate assets to reports containing asset details
Signing	TMSAD	**Trust Model for Security Automation Data**	Guidance for using XML signatures with security automation data

The SCAP Assessment Model


Endpoint
OVAL Objects
What data to collect?
Policy
XCCDF with idents and Applicability Statements, and OVAL Definitions
OVAL System Characteristics
Published system state
How should the data be evaluated?
CMDB
System Data
Relevant data
OVAL System Characteristics
XCCDF checks, OVAL Definitions, Tests, and States
Analysis
Findings
ARF Bundled XCCDF and OVAL Results

NIST Security Automation Activities

NIST Security Automation Program Activities by Area

Standards, Specifications, and Guidelines

- Security Content Automation Protocol Version 1.3
- Software Identification (SWID) Tagging Guidance
- Security Automation and Continuous Monitoring Standards

Data Repositories and Reference Data Sets

- National Vulnerability Database (NVD)
- NVD and National Software Reference Library Integration
- National Checklist Program
- United States Government Configuration Baselines

Product Conformance Testing and Testing Tools

- SCAP 1.2 Product Test Suite Content
- SCAP Content Validation Tool (SCAPVal)
- SCAP 1.2 Validation Program

Research

- Multidimensional Cybersecurity Analytics
- Automated Generation of Indicators Using OVAL

Standards, Specifications, and Guidelines

NIST Security Automation Activities

Security Content Automation Protocol (SCAP) Version 1.3

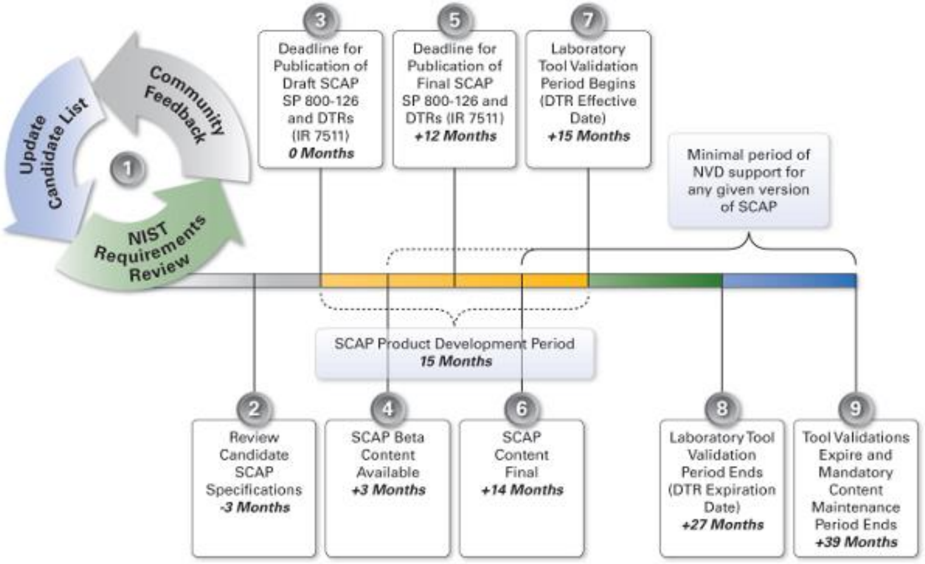
Project Description

Updating the SCAP specification, guidance, and validation program to address public feedback and changes to the underlying component specifications.

Goals

- Address updates to the underlying SCAP component specifications.
- Provide agility to address future changes to OVAL platform schema.
- Modify requirements for backwards compatibility to reduce product development effort.

Specifications, Standards, and Guidelines



Update Candidate List
Community Feedback
NIST Requirements Review
1
3 Deadline for Publication of Draft SCAP SP 800-126 and DTRs (IR 7511) 0 Months
5 Deadline for Publication of Final SCAP SP 800-126 and DTRs (IR 7511) +12 Months
7 Laboratory Tool Validation Period Begins (DTR Effective Date) +15 Months
Minimal period of NVD support for any given version of SCAP
SCAP Product Development Period 15 Months
2 Review Candidate SCAP Specifications -3 Months
4 SCAP Beta Content Available +3 Months
6 SCAP Content Final +14 Months
8 Laboratory Tool Validation Period Ends (DTR Expiration Date) +27 Months
9 Tool Validations Expire and Mandatory Content Maintenance Period Ends +39 Months

Requesting public comments as we move towards step 3.

Security Content Automation Protocol (SCAP) Version 1.3

Accomplishments

- Participated in the FIRST CVSS-SIG to produce CVSSv3
- Contributed to the OVAL 5.11 revisions
- Posted announcement requesting comments on the SCAP 1.3 revision (8/21/2015)

Current Work

- Waiting for public comments based on the announcement

Next Steps

- Produce drafts of NIST SP 800-126 revision 3 and NISTIR 7511
- Update SCAP content validation tool (SCAPVal) and product test suite

Project Contact

Harold Booth

harold.booth@nist.gov

Learn More

Call for comments on SCAP 1.3:

http://csrc.nist.gov/publications/drafts/800-126/sp800-126r3_call-for-comments.html

Send comments to:

800-126comments@nist.gov

Questions?

Email scap@nist.gov

Software Identification (SWID) Tagging Guidance

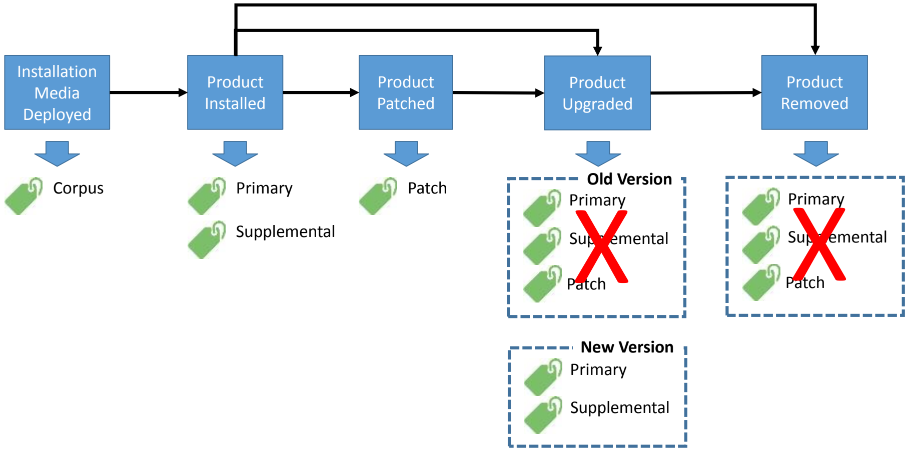
Specifications, Standards, and Guidelines

Project Description

Developing standards and guidelines for software metadata to support cybersecurity, license management, and other operational use cases across the software deployment lifecycle.

Goals

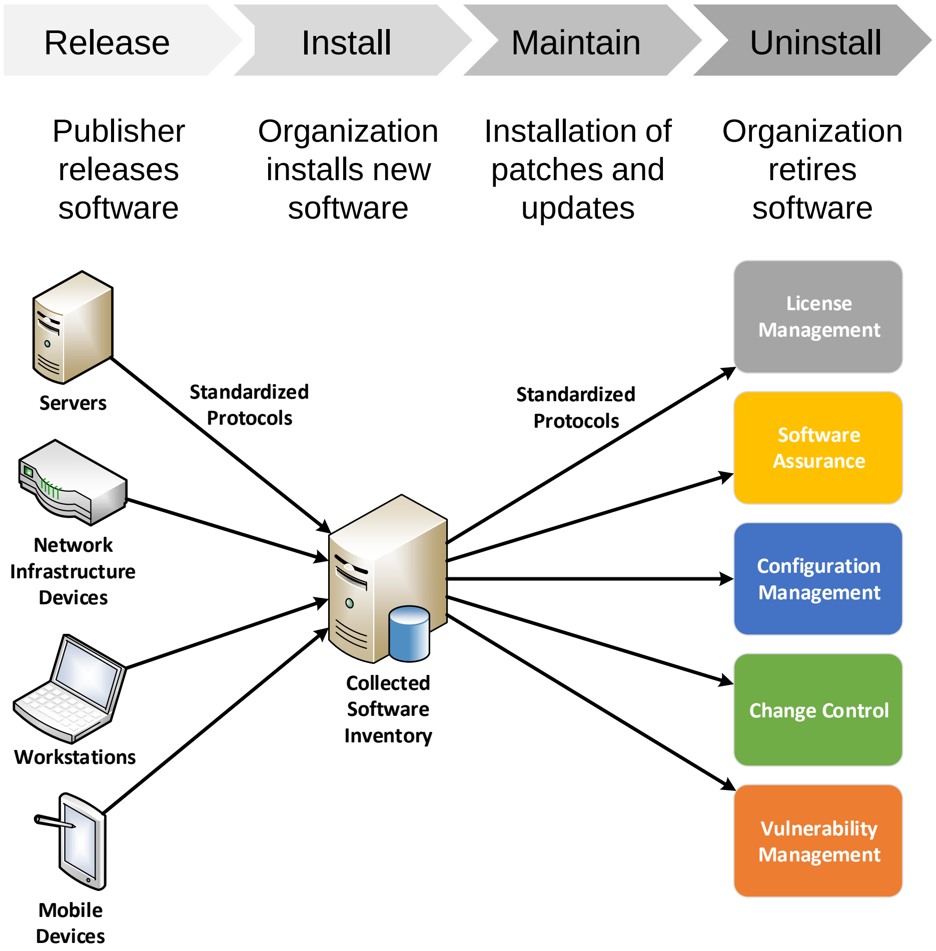
- Platform-neutral continuous monitoring of installed software and patch inventory
- Ensure software is updated to minimize vulnerability exposure
- Enforcing software policies based on software identity and other characteristics



The Concept of SWID Tags

SWID tags enable:

- High-fidelity software metadata provided by vendors
- Platform-neutral, standardized software inventory
- Integration of data and process verticals
- Automation and innovation supporting risk-based management of software



Release — Publisher releases software

Install — Organization installs new software

Maintain — Installation of patches and updates

Uninstall — Organization retires software

SWID Tagging Guidance

Accomplishments

- Active participation in ISO/IEC JTC1 SC7 WG21
- Collaborated in the development of a 2015 revision of ISO/IEC 19770-2: *Information technology — Software asset management — Part 2: Software identification tag*

Current Work

- Developing NISTIR 8060: *Guidelines for the Creation of Interoperable Software Identification Tags*
  - Contains guidelines for creating SWID tags that support cybersecurity use cases
  - Includes rules for generating Common Platform Enumeration (CPE) version 2.3 names from SWID tags
  - Released 3 public drafts
  - Draft #3 currently open for public comment

SWID Tagging Guidance

Next Steps

- Complete final draft of NISTIR 8060
- Development of a SWID tag validation tool based on:
  - ISO/IEC 19770-2
  - NISTIR 8060 guidelines
- Development of reference implementations for:
  - CPE generation from SWID tags
  - Applying XML Digital Signatures to SWID tags

Project Contact

David Waltermire

david.Waltermire@nist.gov

Learn More

- NISTIR 8060
- The ISO/IEC 19770 Family of Standards

Questions or Comments?

Email nistir8060-comments@nist.gov

Security Automation and Continuous Monitoring Standards

Project Description

Participating in a number of standards organizations to develop requirements, architectures, network protocols, and data formats to support continuous monitoring of endpoints and security automation.

Goals

- Management of security controls through automated data collection and analysis
- Timely measurement of the effectiveness of technical security controls
- Broad commercial adoption of international consensus standards for continuous monitoring

Specifications, Standards, and Guidelines

Accomplishments

- Editor for RFC7632: *Endpoint Security Posture Assessment: Enterprise Use Cases*

Current Work

- Participating in the Internet Engineering Task Force (IETF) Security Automation and Continuous Monitoring (SACM) working group

Project Contact

David Waltermire

david.waltermire@nist.gov

Learn More and Participate

https://datatracker.ietf.org/wg/sacm/

Data Repositories and Reference Data Sets

NIST Security Automation Activities

National Vulnerability Database (NVD)

Project Description

The NVD provides standards-based vulnerability management data represented using SCAP. It includes security checklists, security-related software flaws, misconfigurations, impact metrics, and software product names.

Goals

- Automation of vulnerability management using standardized vulnerability information
- Provide reference data to enable security and compliance measurement
- Participate in activities to improve the automation of vulnerability standards

Data Repositories and Reference Data Sets

Vulnerabilities
Over 72,000 CVE entries

Product Names
Product dictionary with over 105,000 CPE product names

Checklists
Over 290 Checklists posted

Vulnerability Analysis
The NVD team evaluates over 6,000 vulnerabilities a year

SCAP Checklists
80+ checklists in SCAP Format (Tier III or Tier IV)

National Vulnerability Database (NVD)

Accomplishments

- Participated in the development of CVSS v3 in the FIRST CVSS-SIG
- Completed major architectural changes to the NVD, supporting future enhancements
- Providing vulnerability entry change histories
- Published NISTIR 7946 documenting the NVD analysis process
- Implemented process to assign CCE identifiers – Ongoing work on CCE data feed

Current Work

- Developing a vulnerability taxonomy to produce CVSS v2 and v3 base scores
- Removing uncompressed vulnerability feeds
- Improving documentation for expected use of data feeds

Next Steps

- Publish vulnerability taxonomy documentation
- Integrate taxonomy information into data feeds
- Website redesign
- Provide REST-based services

Project Contacts

Harold Booth
harold.booth@nist.gov
Robert Byers
robert.byers@nist.gov

Learn More

https://nvd.nist.gov

Questions?

Email nvd@nist.gov

National Software Reference Library (NSRL) and NVD Integration

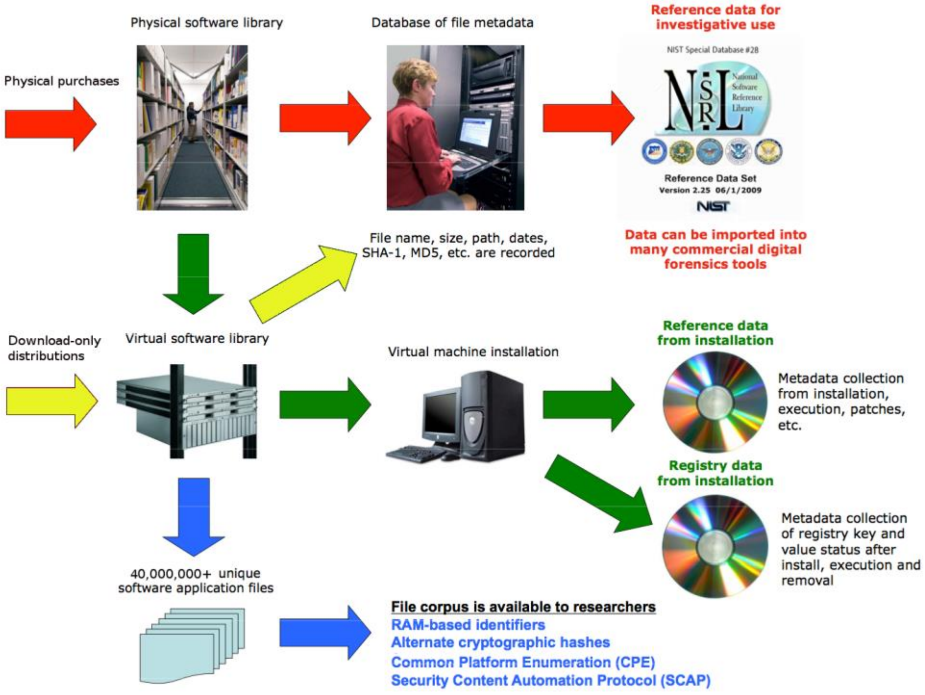
Data Repositories and Reference Data Sets

Project Description

Employing NSRL data to improve software identification and metadata within the National Vulnerability Database (NVD).

Goals

- Improving signatures of software deployment
- Cataloging and recognizing vulnerable software versions
- Researching and evaluating software signature generation mechanisms



Physical purchases
Physical software library
Database of file metadata
Reference data for investigative use
NIST Special Database #28
NSRL
National Software Reference Library
Reference Data Set
Version 2.25 06/1/2009
NIST
File name, size, path, dates, SHA-1, MD5, etc. are recorded
Data can be imported into many commercial digital forensics tools
Download-only distributions
Virtual software library
Virtual machine installation
Reference data from installation
Metadata collection from installation, execution, patches, etc.
Registry data from installation
Metadata collection of registry key and value status after install, execution and removal
40,000,000+ unique software application files
File corpus is available to researchers
RAM-based identifiers
Alternate cryptographic hashes
Common Platform Enumeration (CPE)
Security Content Automation Protocol (SCAP)

NSRL and NVD Integration

Accomplishments

- Use of a document search based technique to identify forensic artifacts relevant to software.

Current Work

- Enhancement of product version information based on executable and shared library metadata
- Working on replication of NSRL data to the NVD
- SWID generation based on replicated NSRL data

Next Steps

- Establish a testing framework to compare NSRL-derived data and publisher-provided SWID tags
- Publish analysis of information retrieval forensic technique
- Publish SWID tags based on the NSRL reference data

Project Contacts

Harold Booth

harold.booth@nist.gov

Alex Nelson

alexander.nelson@nist.gov

Learn More

- http://www.nsrl.nist.gov
- http://nvd.nist.gov

National Checklist Program (NCP)

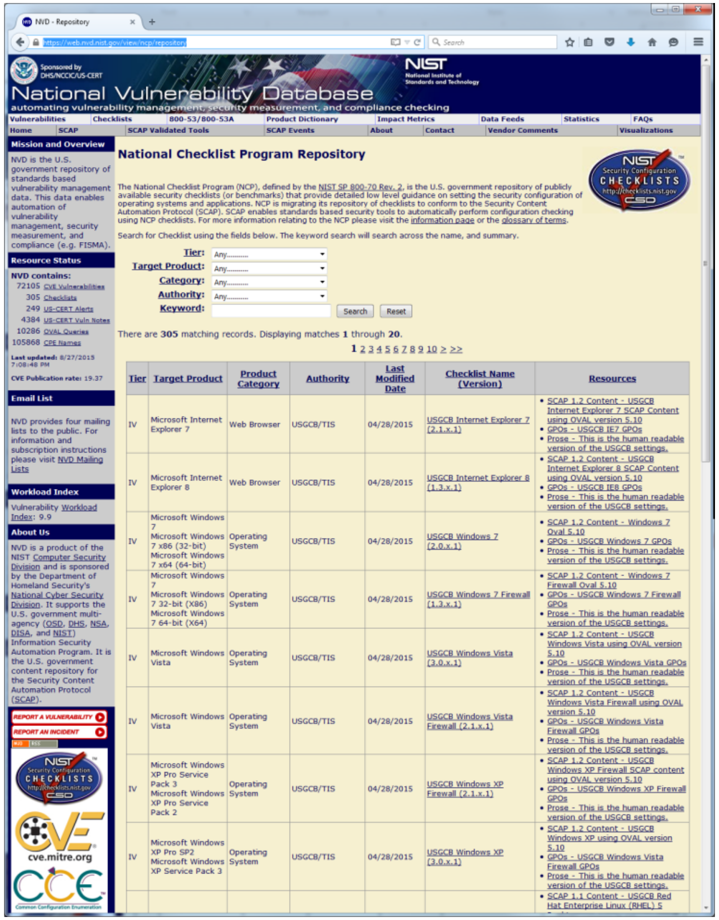
Project Description

The NCP hosts a searchable database of configuration checklists provided by government agencies, IT product vendors, and 3rd-party organizations. The NCP provides guidance on the creation, selection, and use of configuration baselines for federal agencies.

Goals

- Guide agencies on what should be done to improve and maintain effective IT product configuration settings
- Provide practical, security configuration and patch content to the Federal Government
- Enable users to quickly search for, identify, and retrieve appropriate checklists for their IT products

Data Repositories and Reference Data Sets


NVD - Repository
https://web.nvd.nist.gov/view/ncp/repository
Search
Sponsored by DHS/NCCIC/US-CERT
NIST National Institute of Standards and Technology
National Vulnerability Database
automating vulnerability management, security measurement, and compliance checking
Vulnerabilities
Checklists
800-53/800-53A
Product Dictionary
Impact Metrics
Data Feeds
Statistics
FAQs
Home
SCAP
SCAP Validated Tools
SCAP Events
About
Contact
Vendor Comments
Visualizations
NIST Security Configuration CHECKLISTS http://checklists.nist.gov CSD
REPORT A VULNERABILITY
REPORT AN INCIDENT
CVE cve.mitre.org
CCE Common Configuration Enumeration

Mission and Overview

NVD is the U.S. government repository of standards based vulnerability management data. This data enables automation of vulnerability management, security measurement, and compliance (e.g. FISMA).

Resource Status

NVD contains:

72105	CVE Vulnerabilities
305	Checklists
249	US-CERT Alerts
4384	US-CERT Vuln Notes
10286	OVAL Queries
105868	CPE Names

Last updated: 8/27/2015 7:08:48 PM

CVE Publication rate: 19.37

Email List

NVD provides four mailing lists to the public. For information and subscription instructions please visit NVD Mailing Lists

Workload Index

Vulnerability Workload Index: 9.9

About Us

NVD is a product of the NIST Computer Security Division and is sponsored by the Department of Homeland Security's National Cyber Security Division. It supports the U.S. government multi-agency (OSD, DHS, NSA, DISA, and NIST) Information Security Automation Program. It is the U.S. government content repository for the Security Content Automation Protocol (SCAP).

National Checklist Program Repository

The National Checklist Program (NCP), defined by the NIST SP 800-70 Rev. 2, is the U.S. government repository of publicly available security checklists (or benchmarks) that provide detailed low level guidance on setting the security configuration of operating systems and applications. NCP is migrating its repository of checklists to conform to the Security Content Automation Protocol (SCAP). SCAP enables standards based security tools to automatically perform configuration checking using NCP checklists. For more information relating to the NCP please visit the information page or the glossary of terms.

Search for Checklist using the fields below. The keyword search will search across the name, and summary.

Tier: Any..........
Target Product: Any..........
Category: Any..........
Authority: Any..........
Keyword:
Search Reset

There are **305** matching records. Displaying matches **1** through **20**.

1 2 3 4 5 6 7 8 9 10 > >>

Tier	Target Product	Product Category	Authority	Last Modified Date	Checklist Name (Version)	Resources
IV	Microsoft Internet Explorer 7	Web Browser	USGCB/TIS	04/28/2015	USGCB Internet Explorer 7 (2.1.x.1)	• SCAP 1.2 Content - USGCB Internet Explorer 7 SCAP Content using OVAL version 5.10 • GPOs - USGCB IE7 GPOs • Prose - This is the human readable version of the USGCB settings.
IV	Microsoft Internet Explorer 8	Web Browser	USGCB/TIS	04/28/2015	USGCB Internet Explorer 8 (1.3.x.1)	• SCAP 1.2 Content - USGCB Internet Explorer 8 SCAP Content using OVAL version 5.10 • GPOs - USGCB IE8 GPOs • Prose - This is the human readable version of the USGCB settings.
IV	Microsoft Windows 7 Microsoft Windows 7 x86 (32-bit) Microsoft Windows 7 x64 (64-bit)	Operating System	USGCB/TIS	04/28/2015	USGCB Windows 7 (2.0.x.1)	• SCAP 1.2 Content - Windows 7 Oval 5.10 • GPOs - USGCB Windows 7 GPOs • Prose - This is the human readable version of the USGCB settings.
IV	Microsoft Windows 7 Microsoft Windows 7 32-bit (X86) Microsoft Windows 7 64-bit (X64)	Operating System	USGCB/TIS	04/28/2015	USGCB Windows 7 Firewall (1.3.x.1)	• SCAP 1.2 Content - Windows 7 Firewall Oval 5.10 • GPOs - USGCB Windows 7 Firewall GPOs • Prose - This is the human readable version of the USGCB settings.
IV	Microsoft Windows Vista	Operating System	USGCB/TIS	04/28/2015	USGCB Windows Vista (3.0.x.1)	• SCAP 1.2 Content - USGCB Windows Vista using OVAL version 5.10 • GPOs - USGCB Windows Vista GPOs • Prose - This is the human readable version of the USGCB settings.
IV	Microsoft Windows Vista	Operating System	USGCB/TIS	04/28/2015	USGCB Windows Vista Firewall (2.1.x.1)	• SCAP 1.2 Content - USGCB Windows Vista Firewall using OVAL version 5.10 • GPOs - USGCB Windows Vista Firewall GPOs • Prose - This is the human readable version of the USGCB settings.
IV	Microsoft Windows XP Pro Service Pack 3 Microsoft Windows XP Pro Service Pack 2	Operating System	USGCB/TIS	04/28/2015	USGCB Windows XP Firewall (2.1.x.1)	• SCAP 1.2 Content - USGCB Windows XP Firewall SCAP content using OVAL version 5.10 • GPOs - USGCB Windows XP Firewall GPOs • Prose - This is the human readable version of the USGCB settings.
IV	Microsoft Windows XP Pro SP2 Microsoft Windows XP Service Pack 3	Operating System	USGCB/TIS	04/28/2015	USGCB Windows XP (3.0.x.1)	• SCAP 1.2 Content - USGCB Windows XP using OVAL version 5.10 • GPOs - USGCB Windows Vista Firewall GPOs • Prose - This is the human readable version of the USGCB settings.
						• SCAP 1.1 Content - USGCB Red Hat Enterprise Linux (RHEL) 5

National Checklist Program (NCP) and Next Steps

Overview

- Participating organizations from government and industry.
- Currently hosts 305 separate guidance documents for over 400 IT products and product versions
- Updated Draft NIST SP 800-70 Rev 3 continues to encourage vendor development and maintenance of security guidance
- Organizations are translating this backlog of checklists into the Security Content Automation Protocol (SCAP)

Accomplishments

SP 800-70 Revision 3 was posted April 2015 as public draft.

Next Steps

- Release of final NIST SP 800-70 revision 3
- Updates to the NCP website and database based on the SP 800-70 revision

Project Contact

Stephen Quinn
stephen.quinn@nist.gov

Learn More

http://checklists.nist.gov

Questions?

Email checklists@nist.gov

The United States Government Configuration Baseline (USGCB)

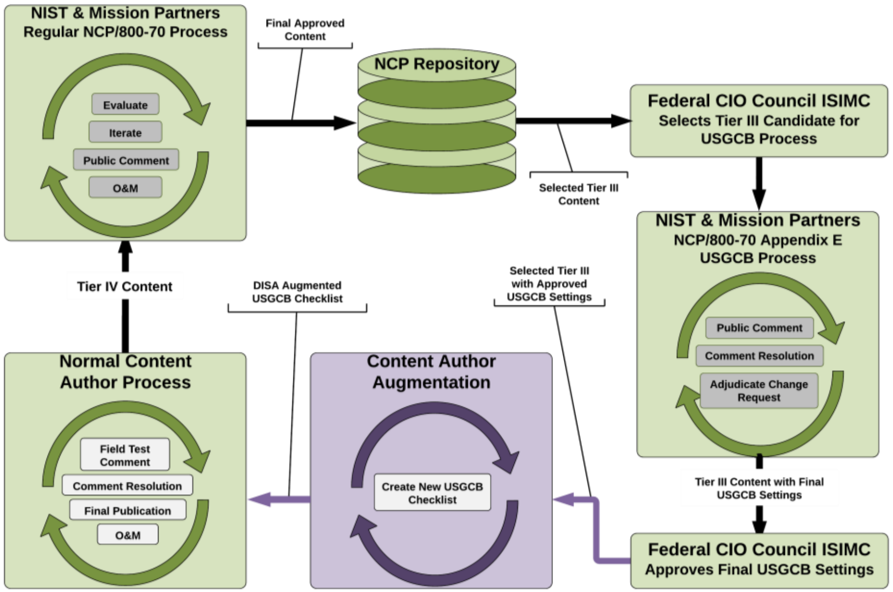
Data Repositories and Reference Data Sets

Project Description

A Federal government-wide initiative to define automatable security configuration baselines for IT products, with a focus on configuration settings, to enhance product security. The USGCB baseline initiative evolved from the Federal Desktop Core Configuration mandate.

Goals

- Provide a formal process for adoption of new and revised configuration baselines by the US Government
- Promote wide adoption of secure configuration baselines within Federal agencies
- Express baselines in SCAP to maximize automation


NIST & Mission Partners Regular NCP/800-70 Process
Evaluate
Iterate
Public Comment
O&M
Final Approved Content
NCP Repository
Federal CIO Council ISIMC Selects Tier III Candidate for USGCB Process
Selected Tier III Content
NIST & Mission Partners NCP/800-70 Appendix E USGCB Process
Public Comment
Comment Resolution
Adjudicate Change Request
Tier IV Content
DISA Augmented USGCB Checklist
Selected Tier III with Approved USGCB Settings
Normal Content Author Process
Field Test Comment
Comment Resolution
Final Publication
O&M
Content Author Augmentation
Create New USGCB Checklist
Tier III Content with Final USGCB Settings
Federal CIO Council ISIMC Approves Final USGCB Settings

NIST SP800-70 Appendix E describes the USGCB process. Agencies should concentrate reviews within the two formal review cycles.

United States Government Configuration Baseline (USGCB)

Accomplishments

- Released updated baselines for Windows 7 and IE 8 based on agency feedback

Next Steps

- Working on updated baselines for Windows 8/8.1, IE 10, Windows 2012 Server, and RedHat 6
- Additional baselines will be considered based on the evolving technology window

Project Contact

Adam Hughes

adam.hughes@cio.gov

Stephen Quinn

stephen.quinn@nist.gov

Learn More

- http://usgcb.nist.gov/
- https://cio.gov/cio-council-streamlines-configuration-baseline-process/

Questions or Feedback?

Email usgcb@nist.gov

Product Conformance Testing and Testing Tools

NIST Security Automation Activities

SCAP 1.2 Product Validation

Product Conformance Testing and Testing Tools

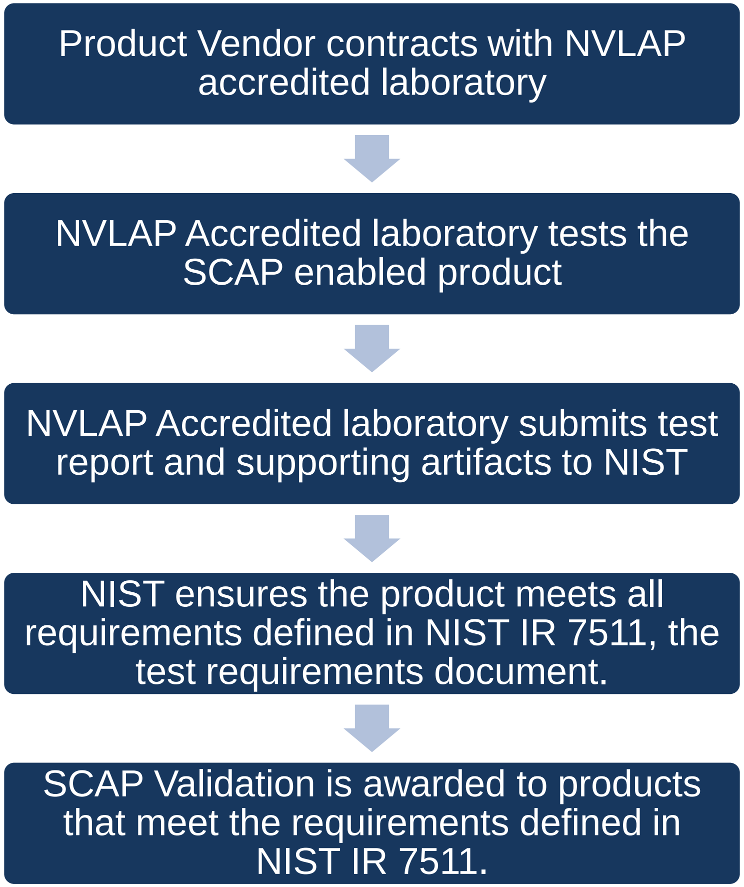
Project Description

Testing products' ability to use the features and functionality of SCAP and its component specifications. Providing SCAP reference materials for use during product development and testing.

Goals

- Interoperability of SCAP products and content
- Predictable product performance
- Publicly available validation resources for use during product development and vendor quality assurance testing

The SCAP Validation process



Product Vendor contracts with NVLAP accredited laboratory

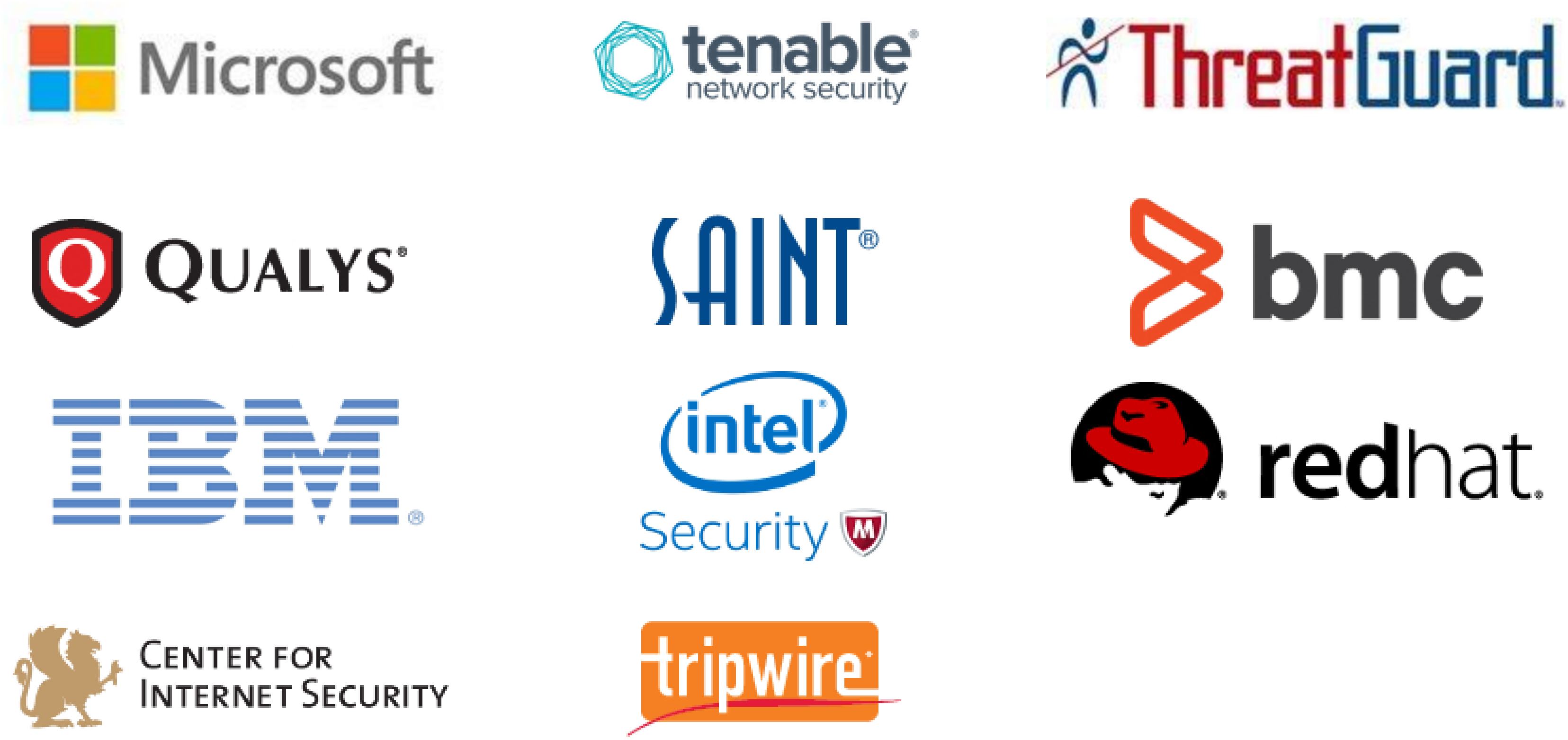
NVLAP Accredited laboratory tests the SCAP enabled product

NVLAP Accredited laboratory submits test report and supporting artifacts to NIST

NIST ensures the product meets all requirements defined in NIST IR 7511, the test requirements document.

SCAP Validation is awarded to products that meet the requirements defined in NIST IR 7511.

SCAP 1.2 Product Validation



Vendors of validated products as of 9/8/2015 from:
https://nvd.nist.gov/SCAP-Validated-Tools/

SCAP 1.2 Product Validation

Next Steps

- Continue the shift from checklist test content toward comprehensive unit testing
- Add platforms
  - Windows 8.1
  - Microsoft Server 2012
  - Red Hat Linux 6
- Support SCAP module testing
- Establish *SCAP Inside* labeling program

Project Contact

Melanie Cook

melanie.cook@nist.gov

Learn More

http://scap.nist.gov/validation/

SCAP Test Content (and more):

http://scap.nist.gov/validation/resources.html

SCAP Validated Products List:

https://nvd.nist.gov/scapproducts.cfm

Questions?

scap@nist.gov

SCAP 1.2 Test Suite and SCAP Content Validation Tool

Product Conformance Testing and Testing Tools

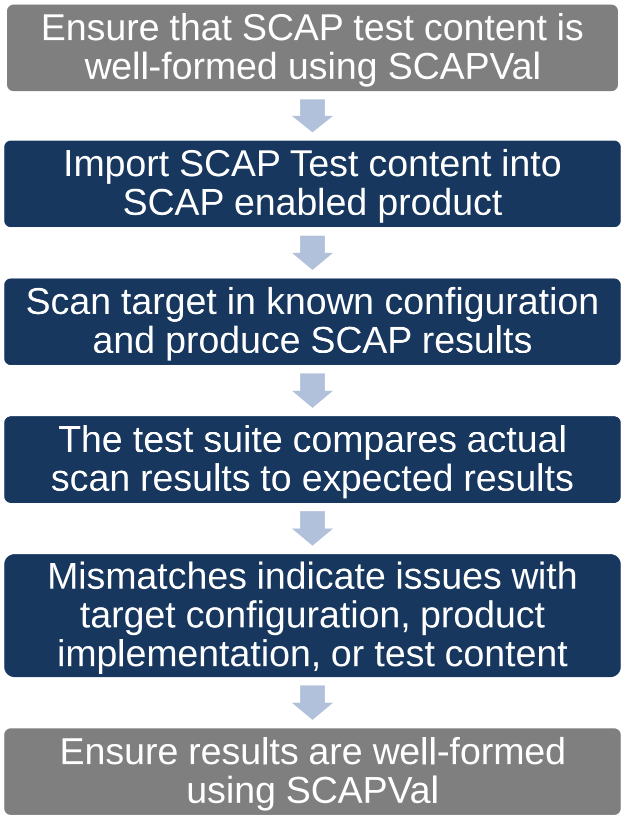
Project Description

Developing and maintaining publicly available SCAP test content and content testing tools for use during product development and testing

Goals

- Publicly available resources that can assist vendors to prepare SCAP enabled products for formal validation testing
- Utilities for ensuring SCAP content is well-formed and adheres to the specifications

Use of the SCAP Test Suite and the SCAP Content Validation Tool (SCAPVal)



Ensure that SCAP test content is well-formed using SCAPVal

Import SCAP Test content into SCAP enabled product

Scan target in known configuration and produce SCAP results

The test suite compares actual scan results to expected results

Mismatches indicate issues with target configuration, product implementation, or test content

Ensure results are well-formed using SCAPVal

SCAP 1.2 Test Suite and SCAP Content Validation Tool

Next Steps

- Expand the SCAP test suite adding support for new platforms in the validation program
- Continue the expand testing for SCAP component specifications
- Update the SCAP test suite and content validation tool for SCAP 1.3

Project Contacts

Melanie Cook

melanie.cook@nist.gov

Harold Booth

harold.booth@nist.gov

Learn More

http://scap.nist.gov/revision/1.2/#tools

http://scap.nist.gov/validation/resources.html

Research

NIST Security Automation Activities

Multidimensional Cybersecurity Analytics

Research

Project Description

Researching statistical models and the application of big data techniques to analyze software runtime behavior to detect attacks.

Goals

- Support the timely detection of zero-day attacks using anomaly detection techniques
- Develop an enterprise, scale event-based monitoring and detection system
- Generalize the approach to different event abstractions

Recent Accomplishments

- Built a Big Data storage system based on Hadoop and HBase
- Implemented a system call event collection system

Next Steps

- Publish a paper analyzing a number of statistical models for bit stream-based anomaly detection
- Development of a Big Data analytical engine based on new models

Project Contacts

Byunggu Yu

Learn More

http://csrc.nist.gov/projects/cybersec-analytics/

Applied SCAP Research
Automated Indicator Sharing

Research

Project Description

Research the use of SCAP to express, identify, and detect system artifacts of interest. Identify and translate existing data repositories and maintained data streams into SCAP for immediate use by already-deployed products.

Goals

- Automate and streamline system-level Information Sharing
- Leverage existing investments in SCAP-validated products that are already deployed
- Enable rapid creation and distribution of SCAP-based content to detect system artifacts of interest

Learn More

- Come to panel session ***Sharing Actionable Windows Artifacts Using SCAP*** on **Fri. 9/11**
- **Panel Participants**: Ronald Nielson (NSA), Tom Millar (DHS), Jim Hanson (CyberESI), Paul Green (G2, Inc.)

  Time: 9:30am – 10:20am, Room 201
- **Demo session** : To follow the panel discussion in Room 203 from 10:35 – 11:25am

Summary and Conclusions

Conclusions

The NIST Security Automation Team is working to:

- Improve enterprise **situational awareness**
- Make security processes more **data driven**
- Provide **data sets** that support operational security processes
  - Software Metadata supporting software inventory
  - Checklists and baselines supporting configuration management
  - Vulnerability data supporting vulnerability management
- Improve the **assurance of** security automation **content** and **products**

Security automation supports a “virtuous cycle”:

- Through automation computers can **collect and analyze data to inform** timely, risk-based **human decision making**.
- Humans can **define policies** that instruct computers **to collect data and take automated action**.

How you can help?

Provide comments on NISTIR 8060 and create SWID tags for your software:
nistir8060-comments@nist.gov

Provide comments on SCAP 1.3:
800-126comments@nist.gov

Use the NVD website and data feeds:
https://nvd.nist.gov

Provide and review NCP checklists:
http://checklists.nist.gov

Review and use USGCB baselines:
http://usgcb.nist.gov/

Use SCAP Validated Products and related test content and utilities:
http://scap.nist.gov/validation/

Questions?

Visit the NIST booth #219

David Waltermire

Security Automation Team

Computer Security Division

Information Technology Laboratory

National Institute of Standards and Technology

david.waltermire@nist.gov