

# Security Automation

September 17<sup>th</sup>, 2014

David Waltermire

---

Enabling Security  
Measurement Through  
Security Automation

# Agenda

---

- Define security automation
- Describe the NIST Security Automation Program
- Discuss current activities

---

# 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

- Carrying out well-understood security and security-related operational activities using computer assisted mechanisms
- Applying technologies and techniques that support security-oriented risk-based decision making

# Security Automation Benefits

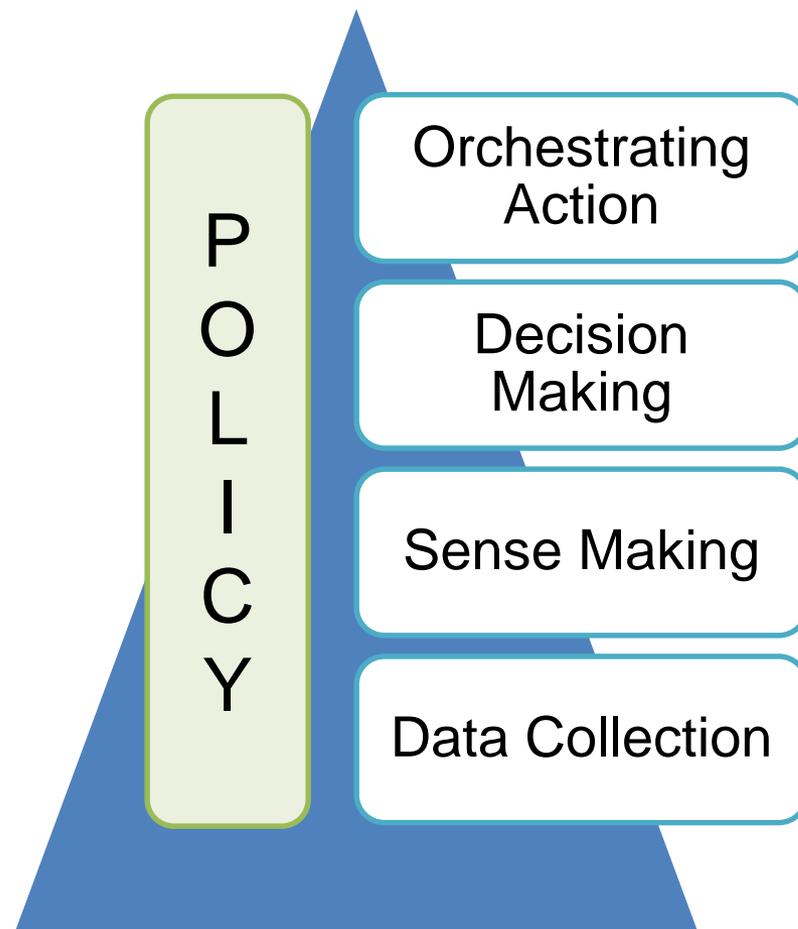
---

- Obtain accurate and timely situational awareness
  - Assets, controls, threats, events, responses, measurements
  - Supports informed decision-making
- Share info with other defenders
  - One organization's detection is another's prevention
  - For speed, must be machine-readable and actionable
- Enable manual or autonomous response
- Plug in new sensors and capabilities as needed
  - Requires open architecture and standards

# Policy-based automation to support risk-based decision making and action

Machine processing of organizationally-defined policies to:

- Automate methods for collecting data from humans and computers
- Support computer assisted contextualization, correlation, aggregation, and analysis of collected data
- Present information to decision makers; automate decision making for well-understood situations
- Use automation to ensure decisions are carried out by appropriate individuals and tools.



# Fundamental Use Cases

---

Foundational capabilities include:

- Hardware and Software Inventory
- Configuration Management
- Vulnerability and Patch Management

# Information Needs: Software Inventory

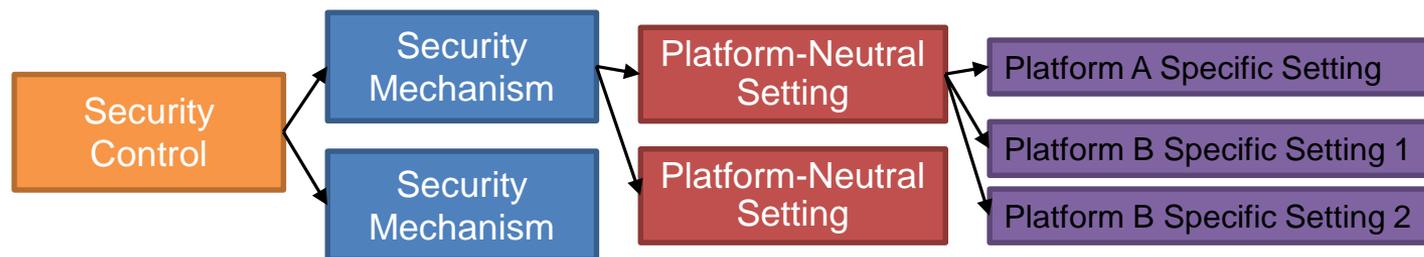
---

- **Stable software identifiers** for OS, application, firmware, and associated patches that enable correlation
  - Down to patch/update level
  - Enable metadata association (e.g., editions, bundles)
- An **understanding of software composition**
  - Libraries – Shared and statically linked
  - Redistributable components
- computing **asset identification**
- Software **installation context**

# Information Needs: Configuration Management

For a given security control:

- **Identify** possible **security mechanisms**
- **Determine** set of **platform-neutral** setting **value(s)**
- **Determine** set of **platform-specific** setting **value(s)**
- Related installed **software context**
- **Collection** of **actual value(s)**
- **Comparison** against **defined expected value(s)**



# Information Needs: Vulnerability Management

For a given software flaw:

- **Identify** the **vulnerability** and all vulnerable **software**
- **Identify** available **patches** and software **updates**
- **Identify** the software **feature**, **protection**, and/or **configuration** it **bypasses**.
- **Determine** the resulting **security mechanism** **bypassed**
- **Determine** the resulting **security control** **bypassed**



# Security Automation Standards are Needed

---

We need standards-based approaches that:

- Provide visibility into all organizational network-connected assets
- Support measurement of the effectiveness of security protections
- Enable understanding of the potential impact of a software-related defect on operational systems
  - Software flaws
  - Misconfigurations
- Inform risk-based decision making based on shared-situational awareness

---

# **WHAT IS THE NIST SECURITY AUTOMATION PROGRAM?**

# The NIST Security Automation Program

---

Working to enable:

- Interoperable, standards-based, automated cybersecurity solutions
- Commercial capabilities that support:
  - Compliance to organizational risk-based policies
  - Measurement of the ongoing effectiveness of deployed security controls
  - Detection and prevention of cyber-attacks
  - Rapid recovery from cyber incidents

# What are we doing?

---

The NIST Security Automation Program is focused on:

- Standardizing data formats and communications protocols that:
  - Enable automating data collection and analysis
  - Support automated security policy assessment and enforcement
- Providing reference data for enterprise security measurement, network defense, and operation
- Defining best-practices for implementing and using security automation tools and techniques
- Product testing to ensure proper specification implementation

---

# WHAT ARE NIST'S CURRENT SECURITY AUTOMATION ACTIVITIES?

# Current Activities

---

- The Security Content Automation Program (SCAP) and SCAP Validation Program
- Security automation reference data
  - National Vulnerability Database (NVD)
  - National Checklist Program (NCP)
- Continuous monitoring reference architecture
- Standards development organization (SDO) activities

# What is SCAP?

## Security Content Automation Protocol

- Brings existing specifications together to provide a standardized approach for measuring the security of enterprise systems
- Provides a means to identify, express and measure security data in standardized ways.
- Currently in 3<sup>rd</sup> revision – SCAP 1.2
  - Defined by Special Publication (SP) 800-126 revision 2
  - Project website: <http://scap.nist.gov>
- SCAP Validation – Validation of conformance testing reports by 3<sup>rd</sup>-party testing labs
  - Validation website: <http://nvd.nist.gov/scapproducts.cfm>
  - Currently 3 SCAP validated products – additional in process

# Security Automation Reference Data

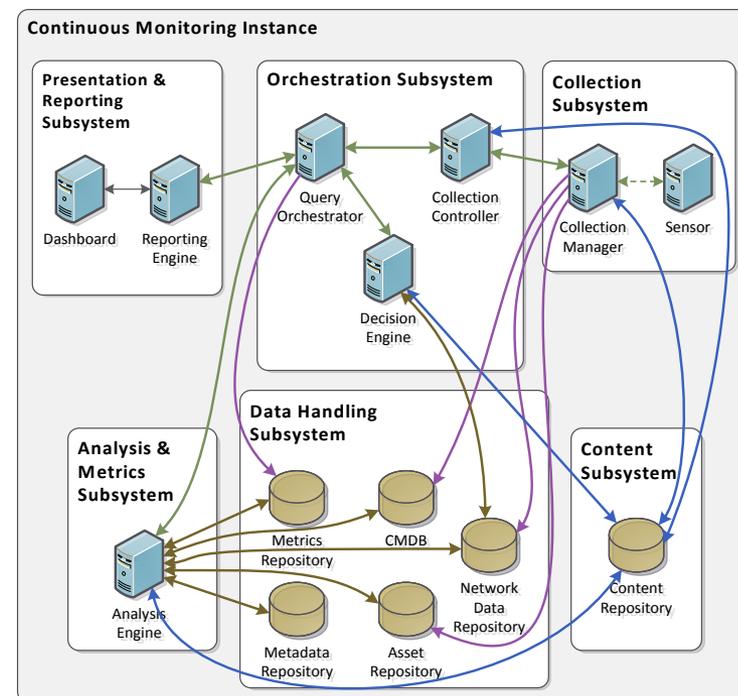
---

Reference data supporting automated measurement:

- National Vulnerability Database (NVD)
  - Provides over 64,000 analyzed vulnerabilities identified by CVE including CVSS scores
  - Provides ~96,000 CPE product names mapped to vulnerabilities
  - Project website: <http://nvd.nist.gov>
  
- National Checklist Program (NCP)
  - Defined by SP 800-70 revision 2
  - Provides human prose and machine readable configuration checklists
  - 248 configuration checklists provided from many organizations
  - 51 SCAP expressed checklists usable by SCAP validated products
  - Project website: <http://checklists.nist.gov>

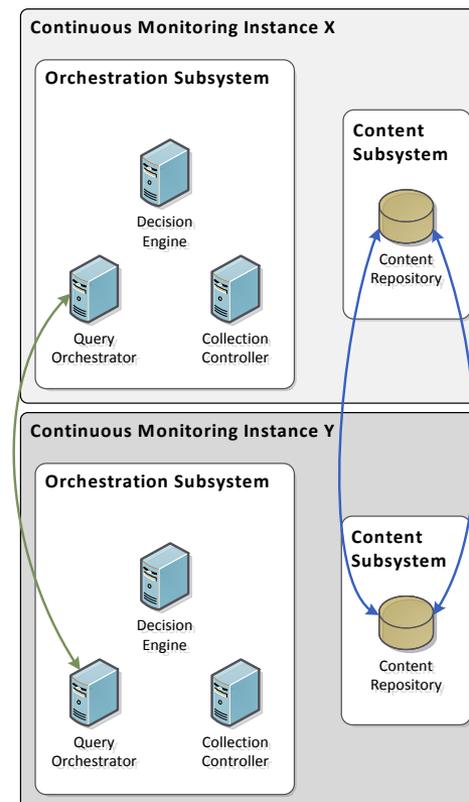
# The Continuous Asset Evaluation, Situational Awareness, and Risk Scoring Framework Extension (CAESARS-FE) Reference Architecture

- Defined by NIST Interagency Report (IR) 7756 and related documents
- A distributed system architectural approach to continuous monitoring
- Decouples data collection, data storage, and analysis
- Supports human and machine consumption of security data
- Enables orchestration of data collection and analysis across multiple tools
- Integrates with SCAP tools for data collection



# CAESARS-FE (Continued)

- Supports inter-instance orchestration of data collection and analysis
- Data analysis is federated with only aggregate, summary data provided to calling instances
- Supports enterprise risk management through analysis of collected data and synthesis of information sources



# Standards development organization activities

---

- International Organization for Standardization(ISO)
  - JTC1 SC7 - Software Identification (SWID) tags
- Internet Engineering Task Force (IETF)
  - Security Automation and Continuous Monitoring (SACM) Working Group

# Use of Software Identification (SWID) tags

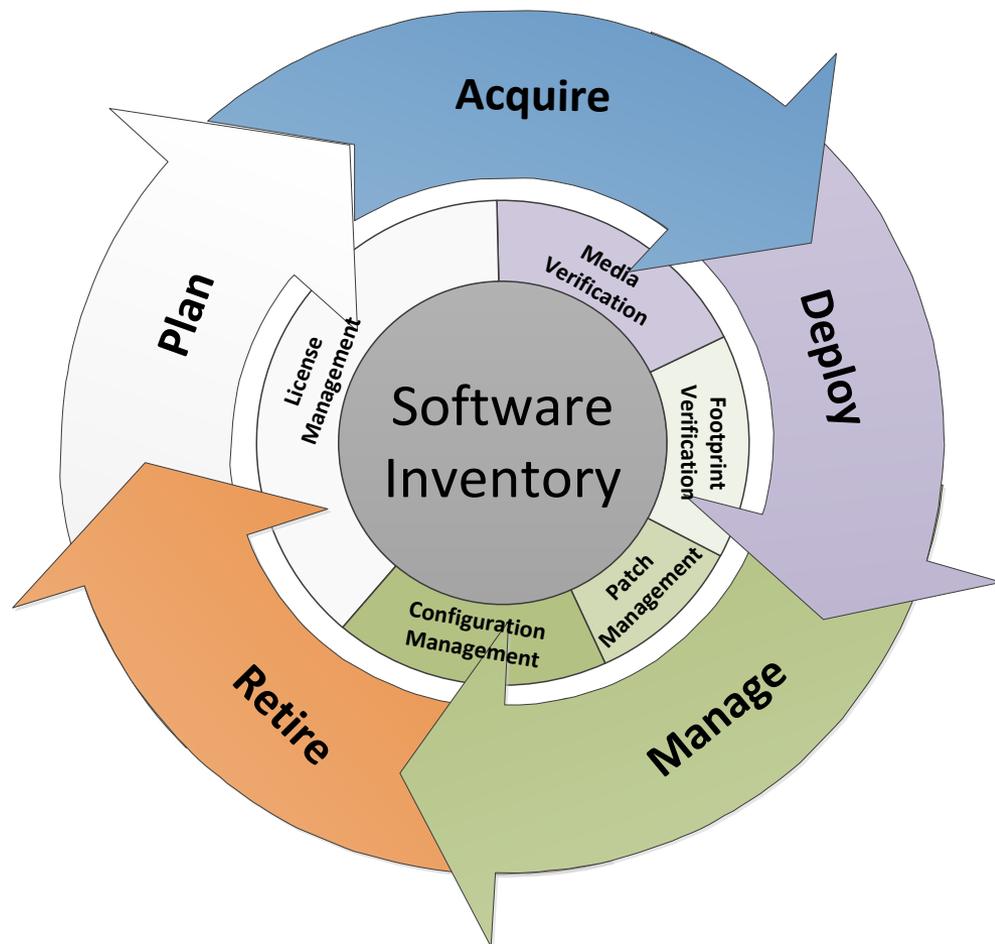
---

- Defined by ISO/IEC 19770-2:2009
- Provides an XML-based software identification token managed during software installation and patching
- Designed to support software asset and license management use cases
- Currently working with vendors and the ISO community to develop guidance to ensure necessary data elements are provided to support security use cases

# Use of SWID Tags in the Software Asset Lifecycle

SWID tags support:

- Software inventory across the software lifecycle
- License management for planning and acquisition
- Media verification at acquisition and install
- Installation verification at deployment and ongoing
- Patch and configuration management of installed software



# IETF SACM Working Group

---

- Established in July 2013
- Focused on development of a set of standards to enable assessment of endpoint posture.
- A set of standards for interacting with repositories of content related to assessment of endpoint posture.
- Currently developing use cases, requirements, architecture, and information model documents.
- Website: <https://datatracker.ietf.org/wg/sacm/charter/>
- Mailing list: [sacm@ietf.org](mailto:sacm@ietf.org)
- List Subscription and Archive: <https://www.ietf.org/mailman/listinfo/sacm>

# Conclusions

---

To measure security we need:

- **Standards**: To enable data to be collected using data driven methods and to be securely exchanged
- **Interoperability**: Standardized interfaces to orchestrate tools, expose collected data, and enable robust analysis processes using secure and reliable methods
- **Automation**: To enable machines to securely carry out well-understood, repetitive tasks

# Questions?

---



**David Waltermire**  
**Security Automation**  
**Program Manager**

Computer Security Division  
Information Technology Laboratory  
National Institute of Standards and  
Technology

[david.waltermire@nist.gov](mailto:david.waltermire@nist.gov)

(301) 975-339033