NIST Security Automation

Tim Grance – Program Manager

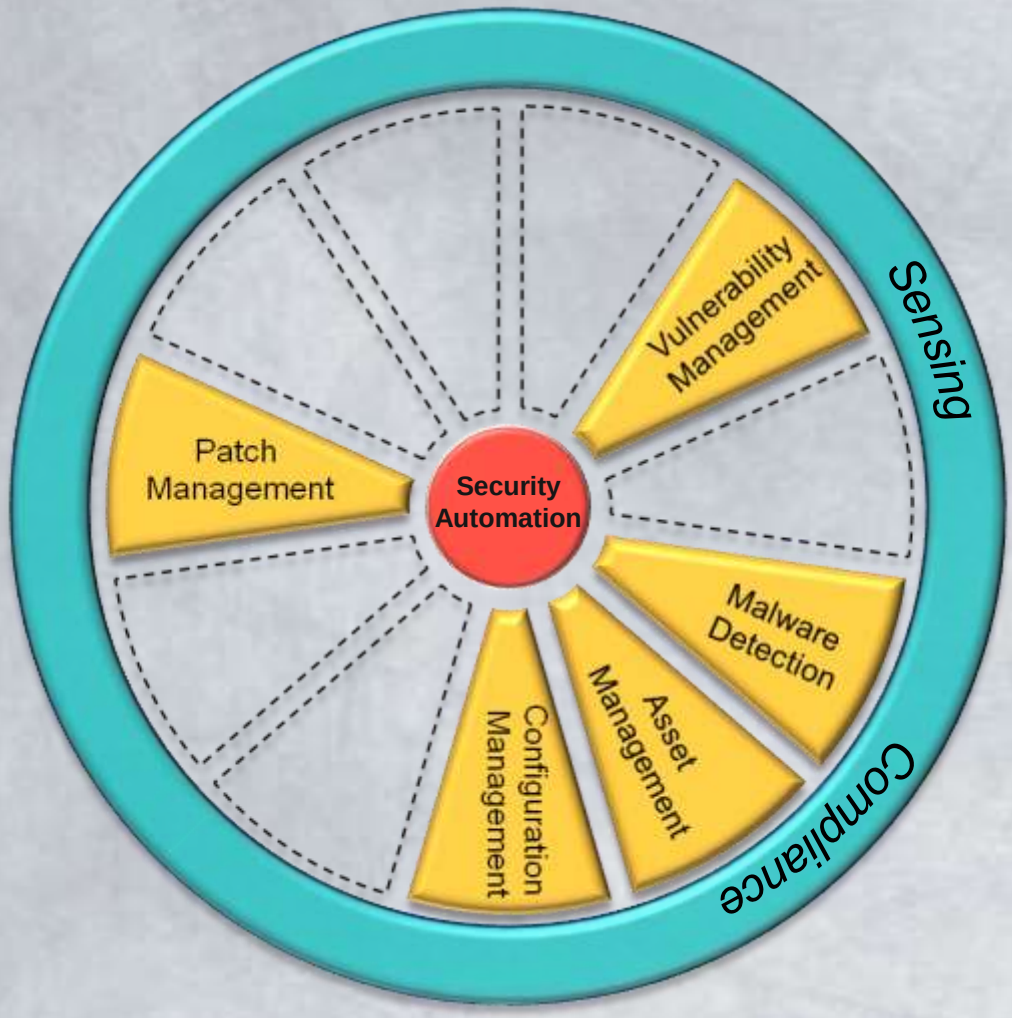
September 28, 2010

Agenda

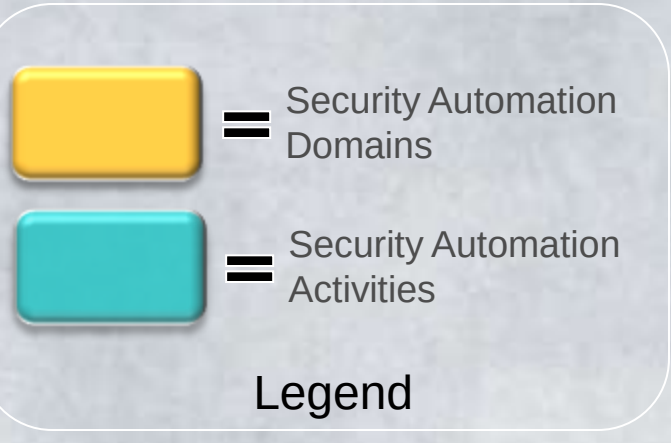
- Past, Present, Future
- Security Automation Efforts
- Security Automation Research
- The Way Ahead
- How can you help?

Security Automation Past, Present, and Future

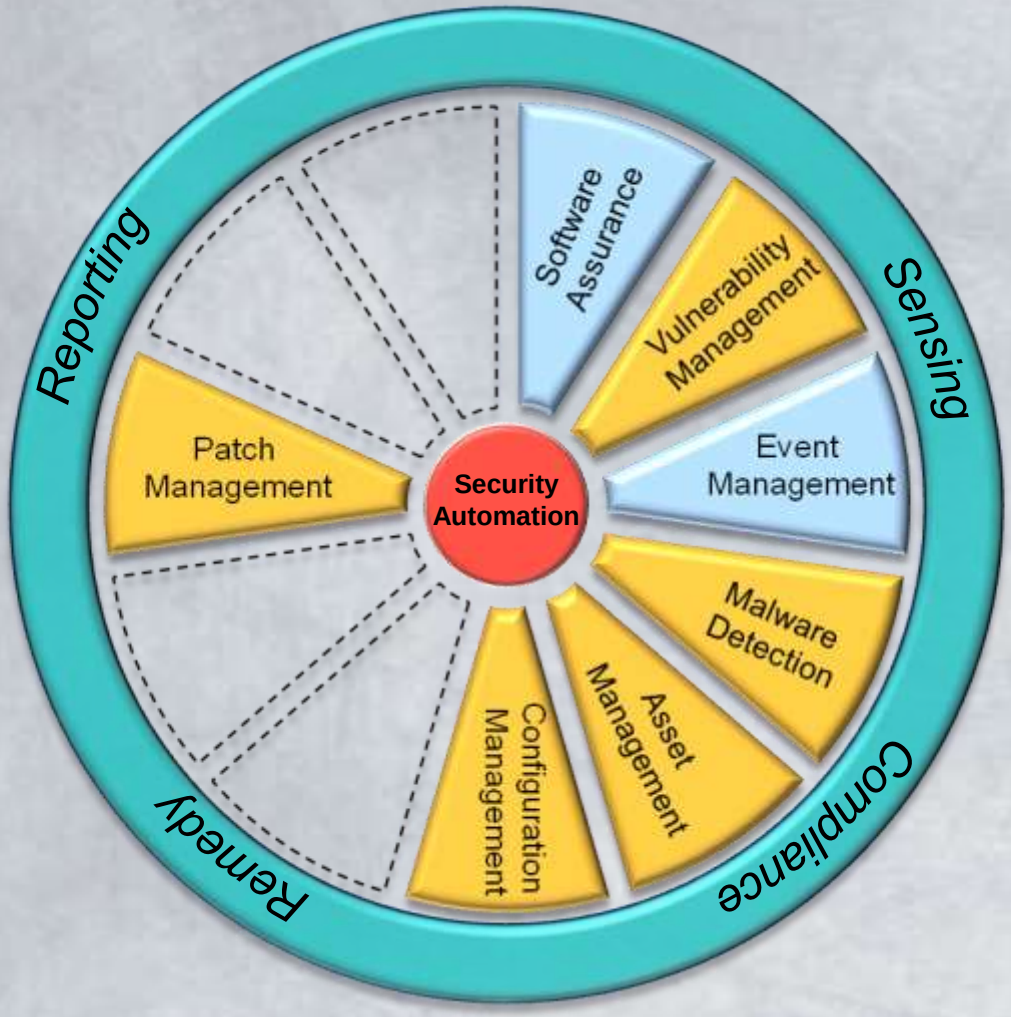
Past Scope of Security Automation Program



- Previous effort addressed network endpoints.
- Additional work remains within these domains and activities.



Present Scope of Security Automation Program



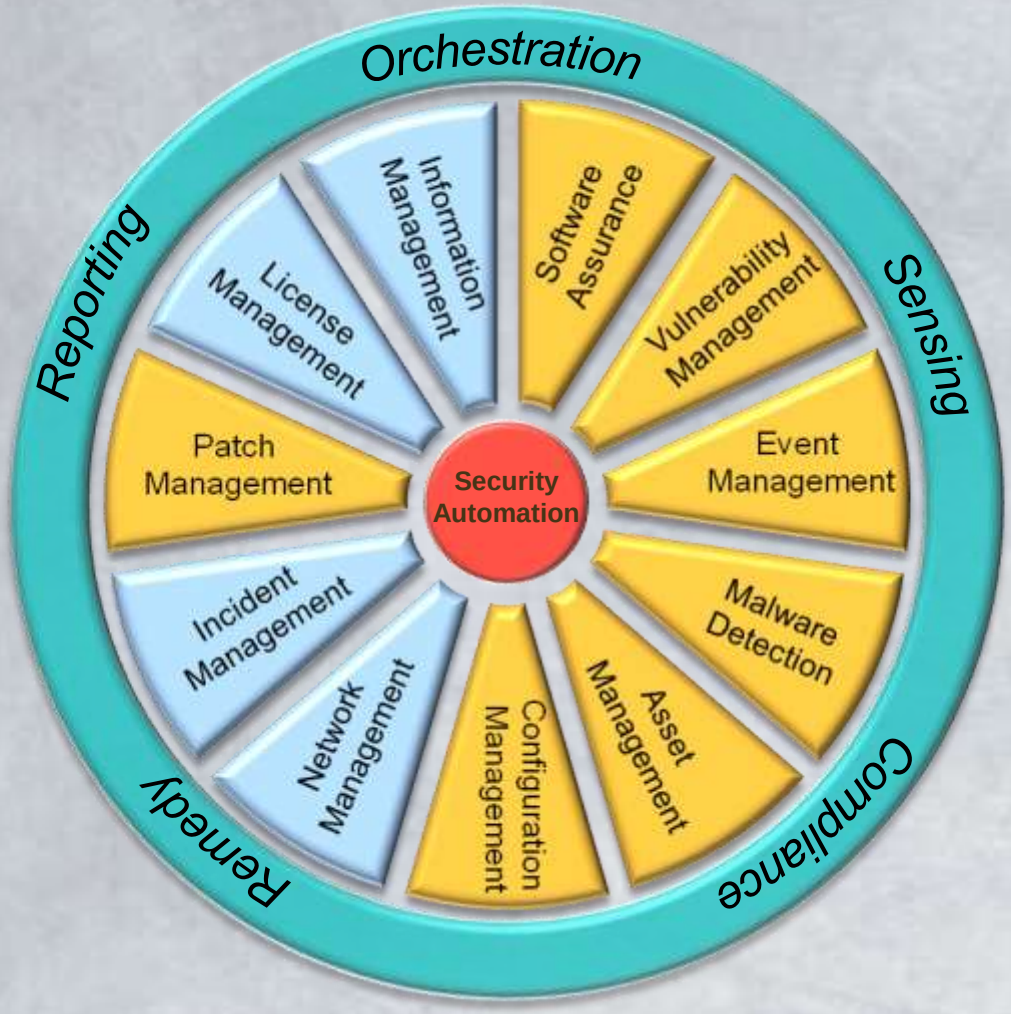
- Current work is expanding into Asset Management space.
- Efforts are also underway to standardize the way Reporting and Remediation data is communicated.

= Security Automation Domains

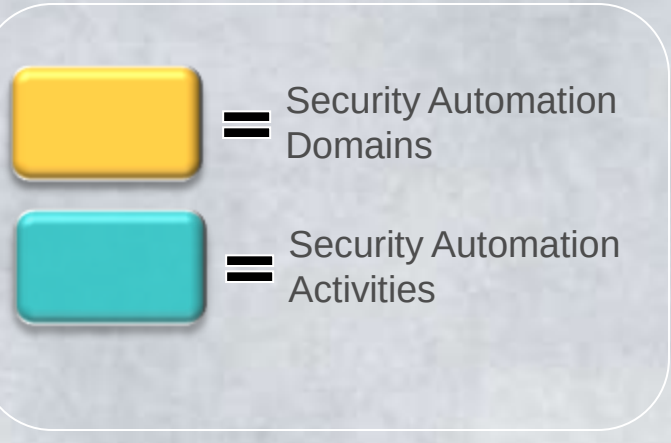
= Security Automation Activities

Legend

Future Scope of Security Automation Program



- Future work may expand into domains and activities beyond those listed here.
- Security Automation specifications are required in each domain/activity area to achieve interoperability across the IT security landscape.



Security Automation Efforts

USGCB

US Government Configuration Baseline (USGCB)

- OMB, Federal CIO Council committees
- Developed baseline settings, supporting documentation, e.g., virtual machines, spreadsheets, SCAP content
  - Field testing, agency champion, tier 3 NCP submission
- Released USGCB for Windows 7 and Internet Explorer 8
- Currently working on RedHat Enterprise Linux 5 Alpha release
- Initiated discussions with Apple on the development of baseline settings for OS X.
- Will harmonize existing FDCC settings for Vista, XP, and IE 7.

Federal Security Automation Initiatives

A few key security automation initiatives within the Federal government:

- NIST – Automation of 800-53/800-53
  - Wider application of CCE i.e. HIPAA and other areas
- DoD - Malware detection and quarantine
- DISA – STIG conversion
- State Department – Continuous Monitoring
- DHS – CAESARS and CyberScope

SCAP Validation Program

- Continued growth in the number of SCAP validated products
- Increased vendor participation
- Enhancements to the validation test processes

Web Portal (NVD/NCP)

- A security automation web portal that hosts services and tools for the creation, submission, validation, search and retrieval of well-formed SCAP content.
  - Web service & interactive web portal that will streamline and expedite the NCP checklist submissions and help ensure the completeness of submission packages
  - SP800-126 Content Validation Tool can be used by SCAP content authors to ensure that their SCAP content bundles conform to NIST guidelines prior to submission to the NCP or use in an SCAP validated tool
  - SP800-53 to CCE mappings reference data feed
  - Automatic SCAP content generation from CVE data feed

National Vulnerability Database

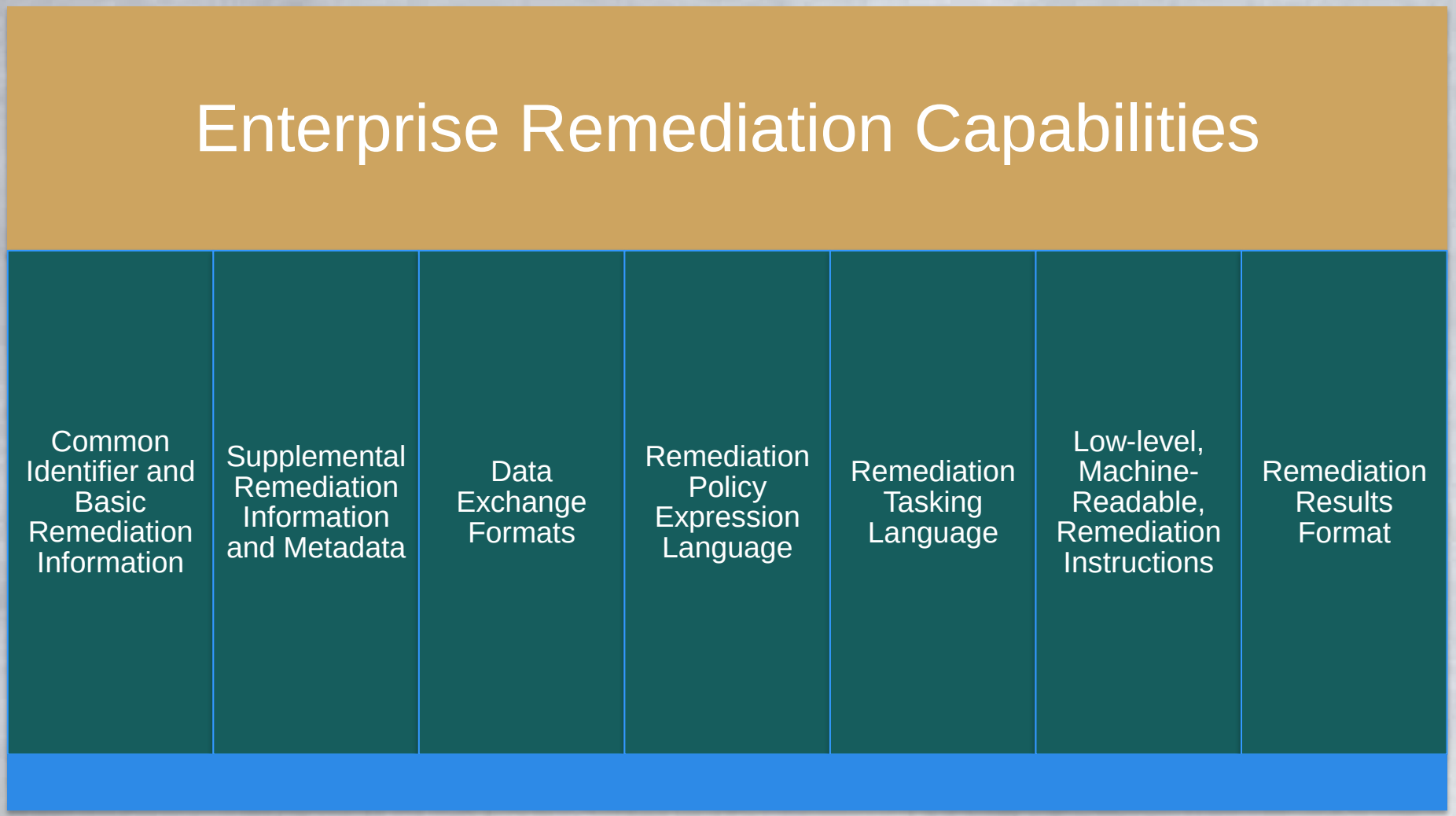
- NVD is the USG repository of public vulnerability management information.
- NVD website received over 40 million hits in CY2009
- Contains over 43,000 CVE entries with the NVD Analysis Team analyzing ~6,000 vulnerabilities a year
- Machine-readable vulnerability data feeds
  - 15,207 individual downloads of the NVD RSS feeds in July 2010
  - 7,825 downloads of the NVD XML feeds in July 2010
- Product dictionary containing over 21,600 unique product names
  - 992 downloads of the NVD CPE dictionary file in July 2010
- National Checklist Program site contains 159 checklists
- Used extensively by government, industry and academia
- Spanish and Japanese language translation

Security Automation Partners

- US Government
  - National Security Agency (NSA)
  - Department of Homeland Security (DHS)
  - Defense Information Systems Agency (DISA)
- Foreign Government
  - Japan - **JVN/IPA** - Japan Vulnerability Notes / Information Technology Promotion Agency
  - Spain – **INTECO** - InstitutoNacional de Tecnologías de la Comunicación
- Not-for-Profit
  - MITRE
- Private Sector
  - Major Operating Systems and Application Vendors
  - Security Product Vendors

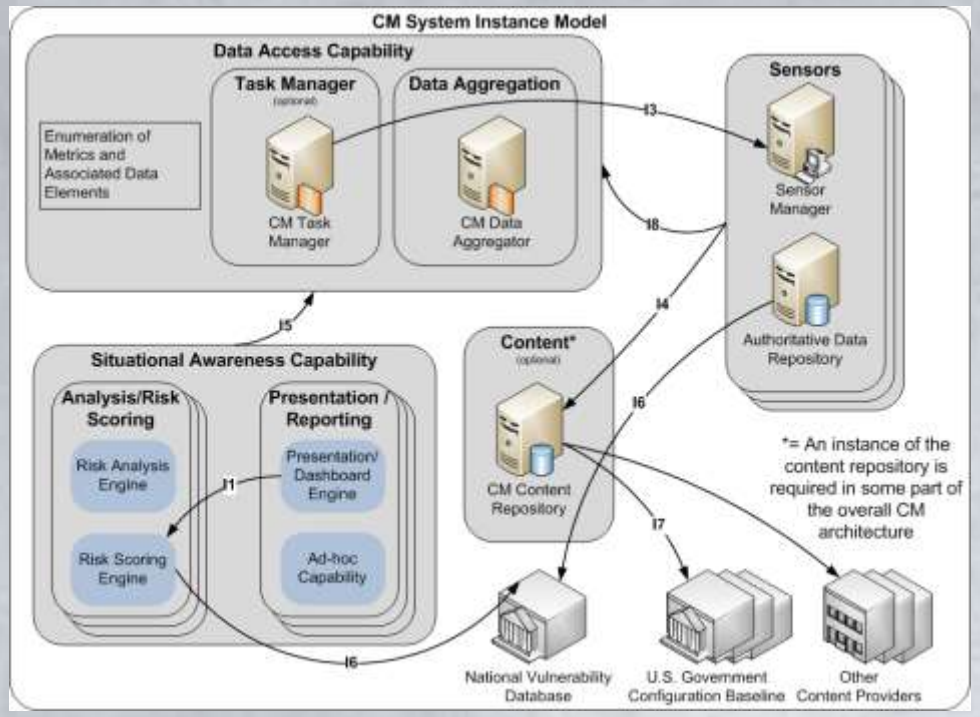
Security Automation Research

Enterprise Remediation



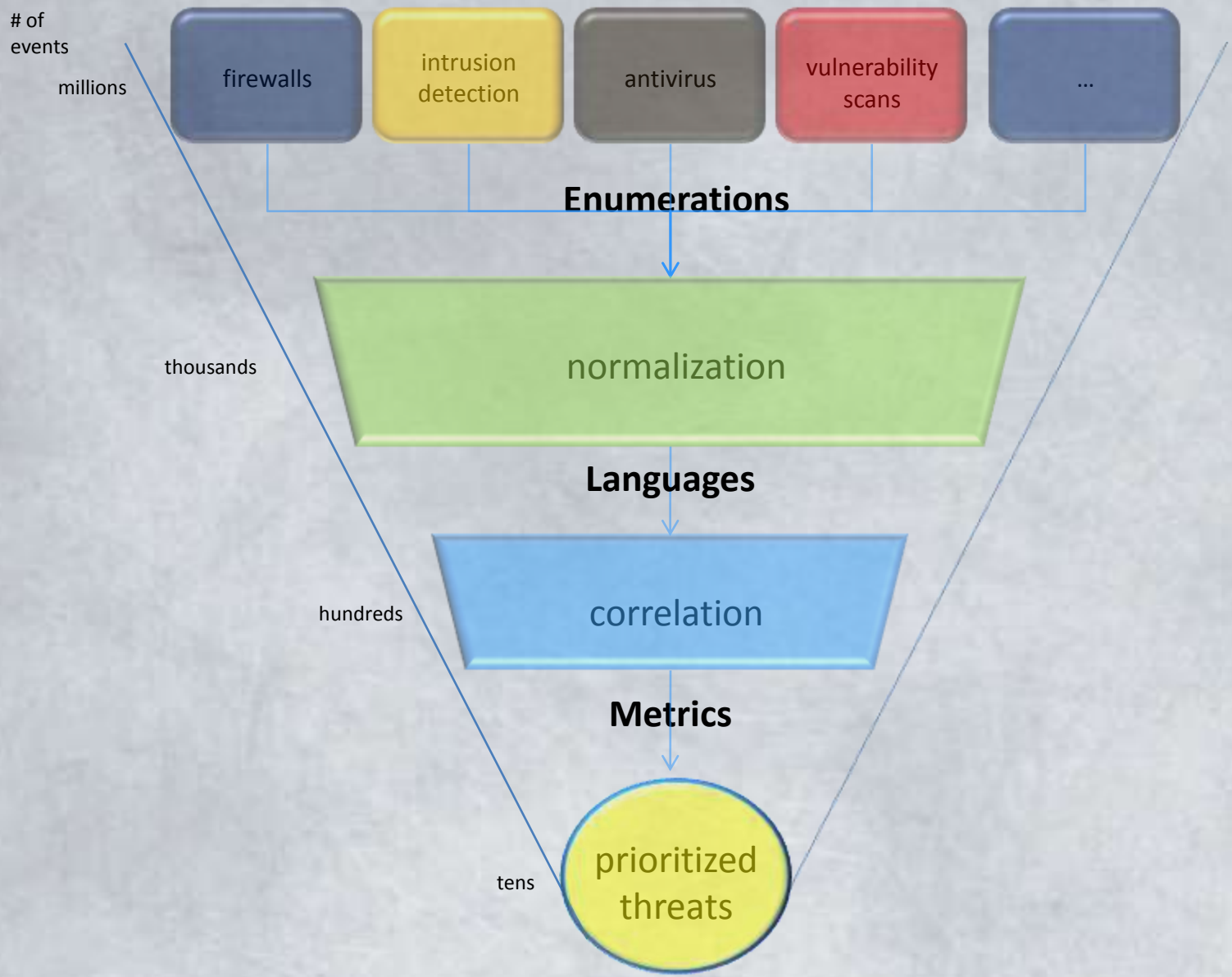
Continuous Monitoring

Defining a continuous monitoring reference architecture that uses core security automation capabilities that:



- Depicts organizational security risk posture
- Provides visibility into assets
- Leverages automated data feeds
- Quantifies risk
- Ensures continued effectiveness of security controls
- Informs automated or human-assisted implementation of remediation
- Enables prioritization of remedies

Event Management



Additional Research Areas

- Standardizing enterprise IT security workflows
- Malware detection and response
- Enhancing enterprise enforcement
- Security Automation and Cloud Computing

Security Automation
The Way Ahead

SCAP Roadmap

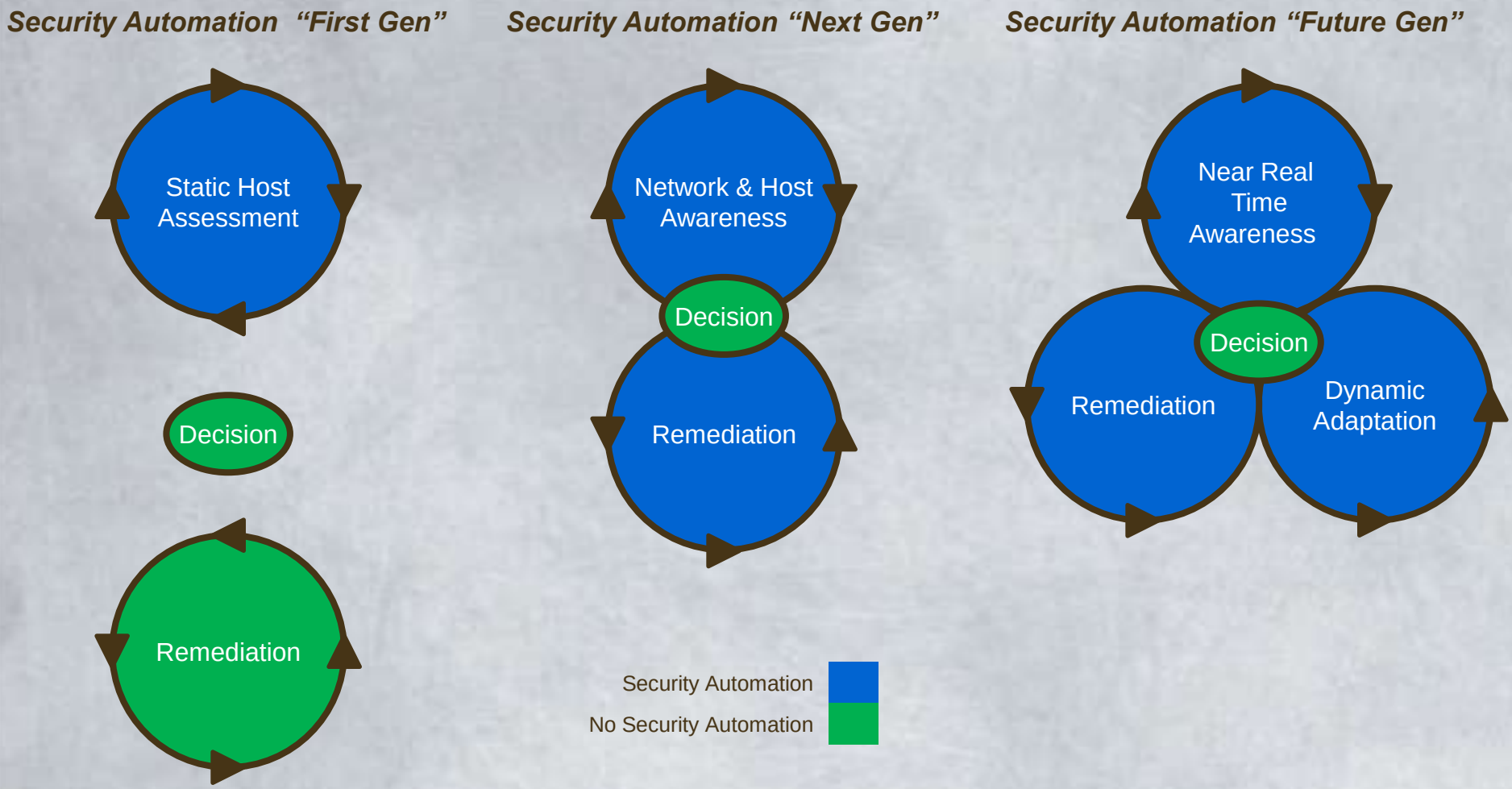
FY 2010
- FINAL SCAP 1.0 Specification and DTRs
- DRAFT SCAP 1.1 Specification and Derived Test Requirements

FY 2011
- FINAL SCAP 1.1 Specification and DTRs
- DRAFT SCAP 1.2 Specification and Derived Test Requirements

FY 2012
- FINAL SCAP 1.2 Specification and DTRs
- DRAFT SCAP 1.3 Specification and Derived Test Requirements

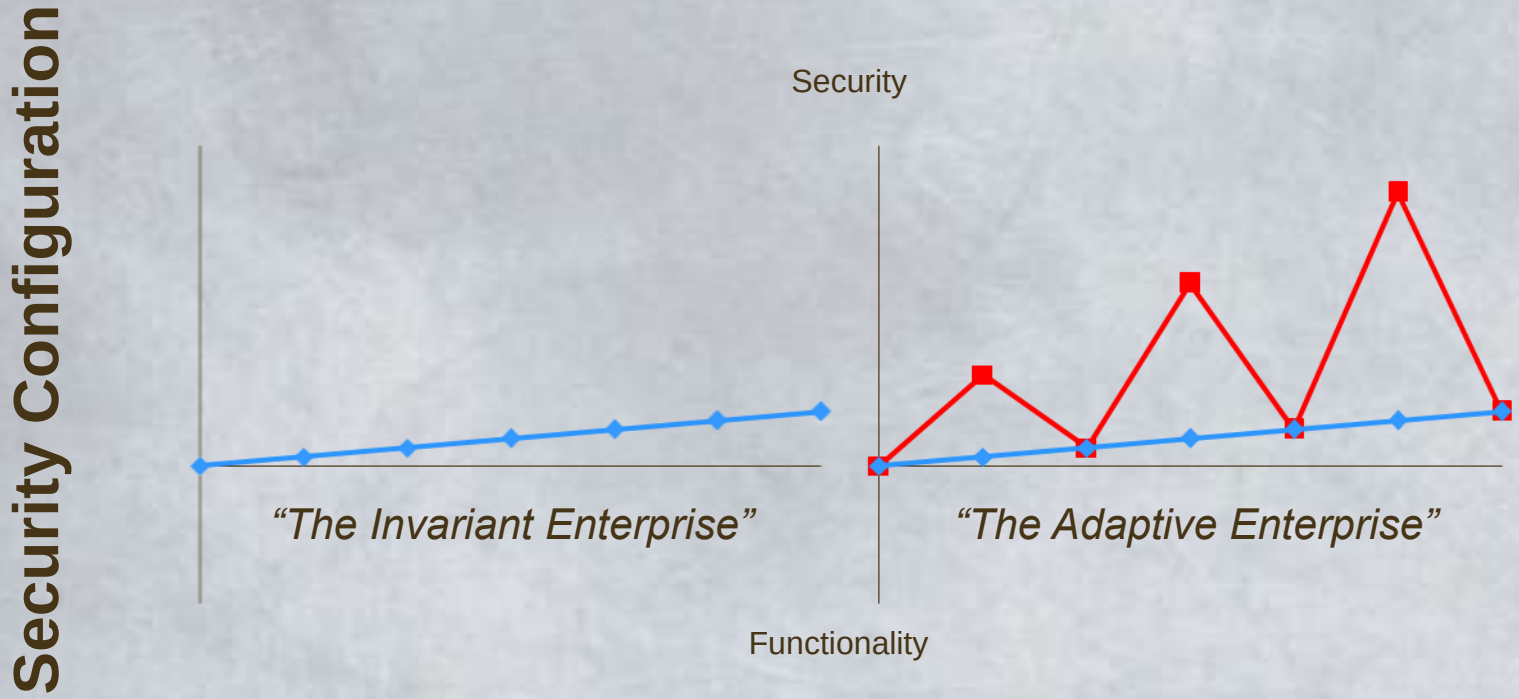
FY 2013
- FINAL SCAP 1.3 Specification and DTRs
- DRAFT SCAP 2.0 Specification and Derived Test Requirements

Security Automation Vision



The Adaptive Enterprise

The Way Ahead



When under duress, the modern IT enterprise must have the ability to momentarily favor security over functionality. Once circumstance returns to normal, the enterprise must resume the normal balance between security and functionality. This process is different than normal enterprise remediation.

Looking Forward

- International Adoption
- Balancing operational needs in the community against a comprehensive, long term view
- Ensure that the Validation Program continues to meet operational needs.
  - Additional Automated tests

How can you help?

- IT Vendors
  - Issue CPE's and CCE's for your products
  - Produce SCAP checklists and submit them to the National Checklist Program
- Integrate SCAP into your infrastructure
- Plan for future security automation in your infrastructure
- Produce alerts using SCAP
- Buy and use SCAP Validated products
- Engagement and feedback
- Innovate

Some Final Thoughts

- SCAP has experienced significant public and private sector adoption, we want this trend to continue across the security automation landscape
- Need to represent a broad set of use cases
- Collaboration with the security automation community and other standards organizations is essential
- To remain relevant, security automation initiatives must be able to adapt and evolve
- Continue to focus our automation efforts on game-changing capabilities

Conference Acknowledgements

- Government Sponsors
  - NSA, DHS, DISA, NIST
- Corporate Sponsors
  - Platinum: Intel, Symantec
  - Gold: RedSeal Systems, Fortify
  - Silver: McAfee
  - Ice Cream Social: Qualys
  - Directional Floor Decal Sponsor: CompTIA/Pearson VUE
  - Water Bottle Sponsor: Patriot Technologies/BIGFIX
- Conference Special Recognitions
  - Track Leads

Resources

SCAP Homepage:
http://scap.nist.gov
SCAP Validation 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
United States Government Configuration Baseline:
http://usgcb.nist.gov

Q&A / Feedback

Supplemental Slides

What are we achieving with Security Automation?

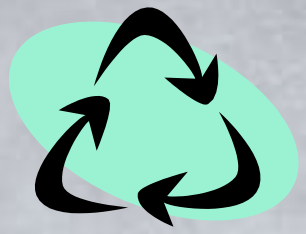
Minimize Effort

- Reducing the time and effort of manual assessment and remediation
- Providing a more comprehensive assessment of system state

Increase Standardization and Interoperability

- Enabling fast and accurate correlation within the enterprise and across organizations/agencies; Reporting
- Shortening decision cycles by rapidly communicating:
  - Requirements (What/How to check)
  - Results (What was found)
- Allowing diverse tool suites and repositories to share data
- Fostering shared situational awareness by enabling and facilitating data sharing, analysis, and aggregation

What are we achieving with Security Automation and Standardization?



Standard data, economy of scale, and reuse

- Standardized security content can be developed once and used by many
- Common definitions for vulnerabilities, software, and policy statements

Speed

- Rapidly identify vulnerabilities and improperly configured systems and communicate the degree of associated risk

Thoughts on Current State of Vulnerability and Configuration Management

- ***Automation and communication is normally limited to a single discipline*** - vulnerability, compliance, configuration, and asset management remain compartmentalized
- ***Automation and communication usually occurs through proprietary methods*** - therefore data sharing, analysis, aggregation, etc. is typically only possible within a product line
- ***Increasing number of mandates*** - means increasing number of frameworks, standards, regulations, guidelines, sometimes these documents conflict
- ***Relatively static number of security configurations***
- ***Increasing number and complexity of vulnerabilities and threats***

Security Automation

The Way Ahead