CPE Developer Day Winter 2010 Workshop

Brant A. Cheikes

bcheikes@mitre.org / 781-271-7505

22 February 2010

Logistics

- **Workshop Hours: 9:00 – 5:00**
- **Breaks:**
  - Morning 10:15-10:30
  - Lunch 12:30-1:15
  - Afternoon 2:15-2:30 & 4:15-4:30
- **Restrooms**
- **Cafeteria**

Schedule

- **0915-1015** **1: Introduction & Overview**
- **1030-1145** **2: CPE Community Needs**
- **1200-1415** **3: CPE Target State**
  - 1230-1315 Lunch
- **1430-1630** **4: Proposing CPE Changes**
- **1630-1700** **5: Action Planning**

Agenda for Segment 1

- Workshop Motivation and Objectives
- Target Milestones
- Process
- Survey Results
- Setting Expectations

Workshop Motivation

- **CPE is not succeeding, where success is defined as:**
  - Achieving significant and growing vendor support;
  - Stimulating increasing volumes of product data contributed by the community to the CPE Dictionary;
  - Acceptable to NIST for inclusion in a future release of SCAP;
  - Deployed in product offerings to foster inter-vendor tool interoperability;
  - Manageable across time and scale for large deployments.

Workshop Objectives

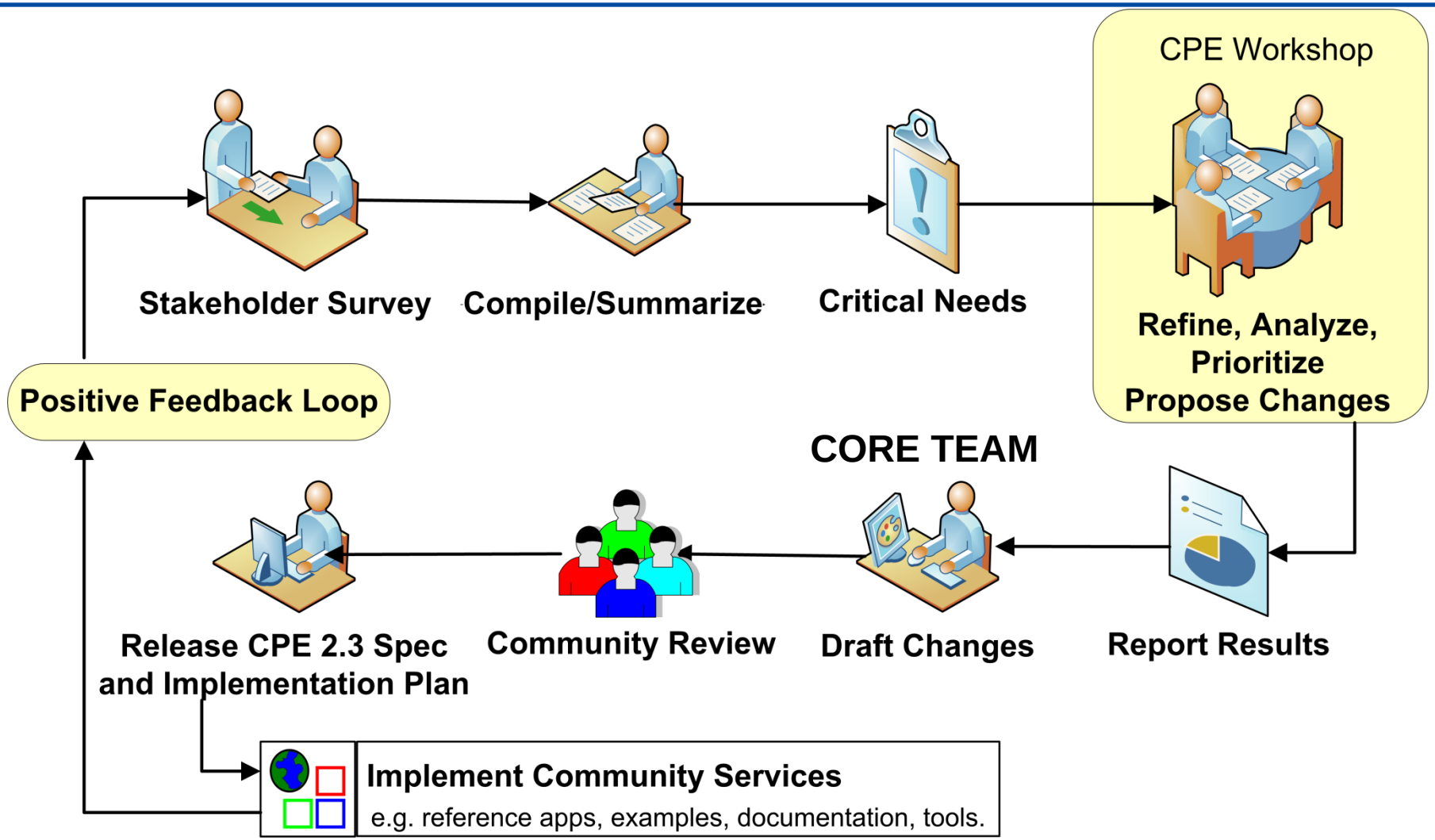
- Describe near- and longer term target capabilities that CPE spec and content management processes must support;
- Prioritize potential changes to the CPE specification and content maintenance process;
- Determine next steps that the CPE specification moderators and the user community need to take.

Target Milestones

- **CPE V2.3: Fix as much as we can without breaking backward compatibility w/ 2.2**
  - Backward compatibility means that CPE 2.2 content is still acceptable under 2.3 specification
  - For entry into next release of SCAP, a stable draft needs to be completed by ~July 2010

- **CPE V3.0: Get it right**
  - Likely to break backward compatibility
  - Stable draft by ~July 2011 for SCAP FY12

Overall Process Vision



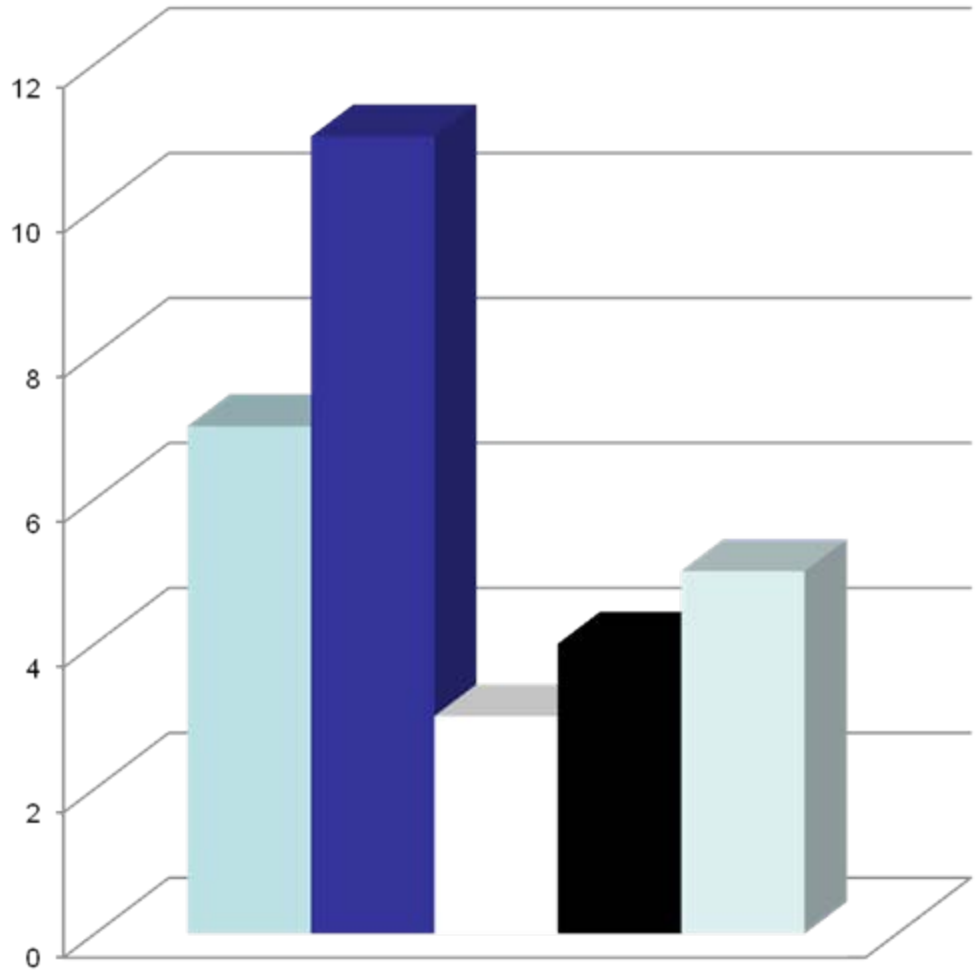
Today's Process: Overview

- **Structured, facilitated process**
- **Elicitation of specific and actionable recommendations from the community**
- **Work sessions:**
  - Community needs (2 hr)
  - Capabilities required to address needs (2 hr)
  - Changes required to provide capabilities (2 hr)
  - Action planning (30 min)
- **Work sessions seeded with, but not limited to, survey response data**

Survey Results Overview

- **Summary:**
  - 17 responses received: 13 commercial, 4 US Govt
  - 40 “top 3 challenges”, 36 “critical issues”, 15 “additional issues”
- **Analysis:**
  - Grouped inputs into10 categories of concern
  - Rank ordered categories of concern
  - Further consolidated items within each category
  - Results used to seed discussions during workshop segments 2 and 3

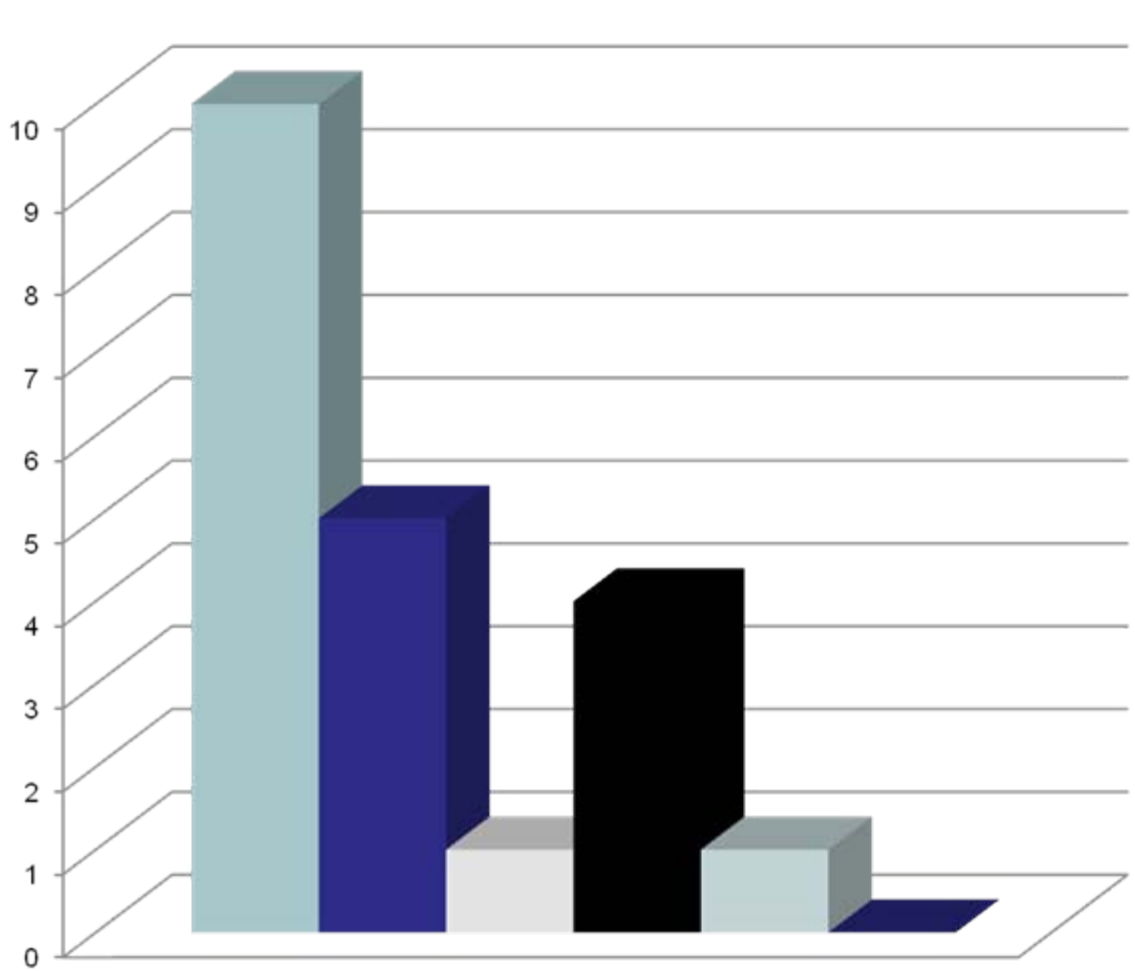
Q1: What is your Role?



- User of security automation tools (e.g. Network Security Engineers, Security Information Managers)
- IT security automation tool vendor, independent tester, consultant
- Moderator of related initiative (e.g. OVAL, XCCDF, SCAP)
- IT vendors whose software and hardware products will be described in the CPE dictionary
- Other

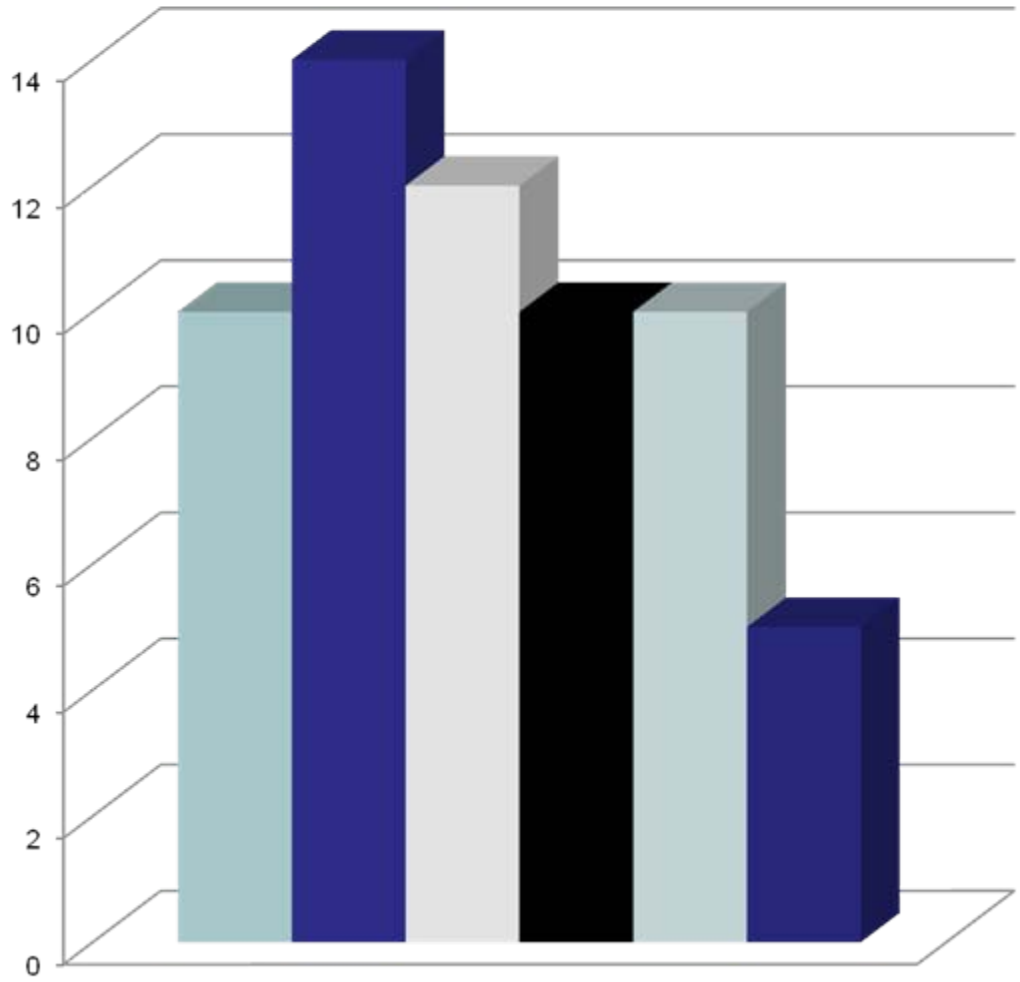
Other Specified:
- NIST NSRL
- Belongs to the developer community of an open-source tool for vulnerability management (sigvi)
- CPE Dictionary Moderator, CPE-related Service Provider
- Internal use in research related databases
- Vulnerability database service provider in Japan

Q2: Status of Organization's Use of CPE?



- Currently using CPE
- Planning to use CPE (specify when)
- Considering the use of CPE
- Using another standard that includes CPE
- Not using CPE, but would if the standard were different (specify deficiencies that would have to be addressed
- Other

Q3: Other SA Standards Being Used?

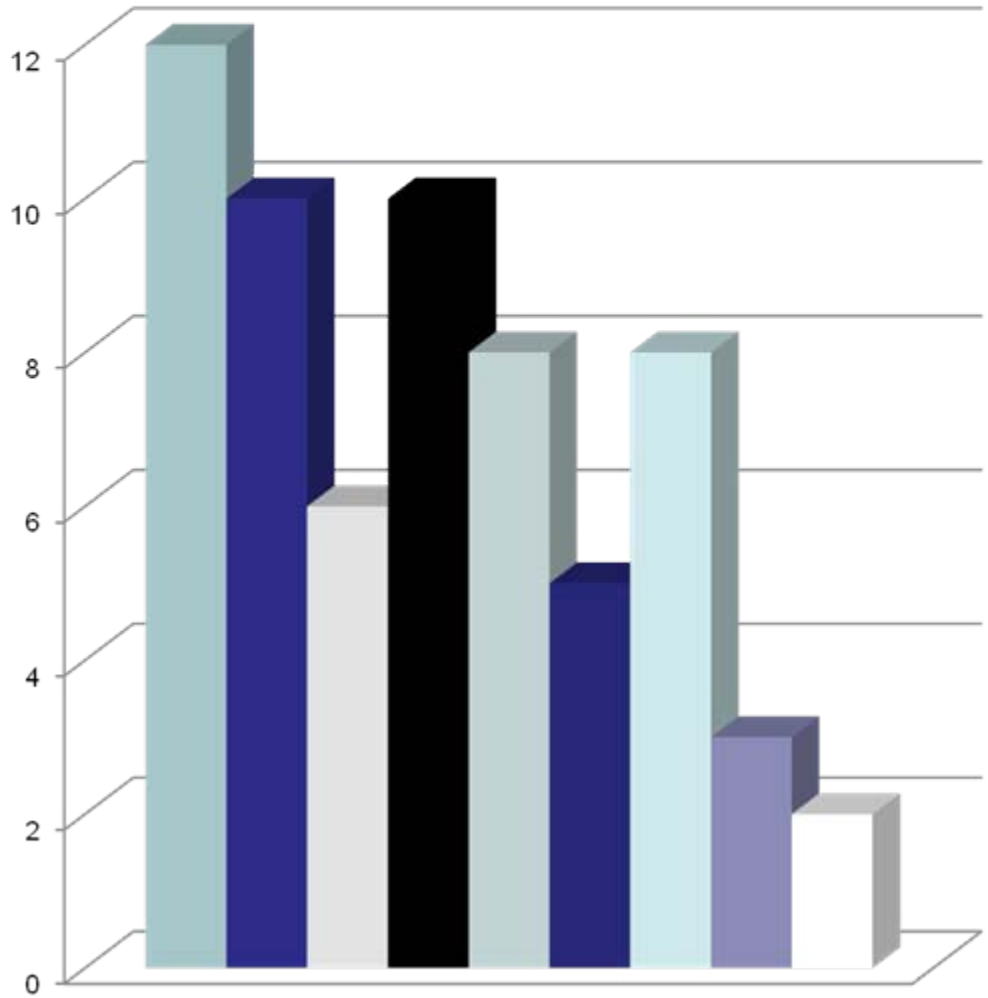


- Common Configuration Enumeration (CCE)
- Common Vulnerabilities and Exposures (CVE)
- Common Vulnerability Scoring System (CVSS)
- Extensible Configuration Checklist Description Format (XCCDF)
- Open Vulnerability and Assessment Language (OVAL)
- Other

Other Specified:

- NVD CVE XML feeds
- OCIL, SCAP, Developing data standards, web services, etc., using CPE
- ARF/ASRF
- CWE
- ARF/ASR

Q4: Planned Automation Areas (Next 2 yr)?



- Software Inventory (authenticated scanning)
- Network-Based Device and Software Discovery (unauthenticated scanning and event management)
- Forensic Analysis/System Architecture (identify the footprint of a piece of software)
- IT Management (e.g. configuration management, patch management, remediation, license management
- Security Compliance Management (FDCC or other checklist compliance)
- Network Knowledge Management
- Incident or Event assessment and management
- Software Build/Release Management
- Other

Other Specified:
- Lots of research based areas under investigation
- Confidential

CPE Survey Questions 5-7

- **Q5: Describe your organization's top three security automation-related technical challenges that are related to CPE.**
- **Q6: Describe the issues that you feel are critical to improving CPE's ability to support your organization's automation-related challenges in the future.**
- **Q7: Describe any additional issues (technical or other) that you think are important to address at the upcoming CPE workshop.**

MITRE

10 Response Categories

Dictionary Content	The elements, attributes, and instances that comprise CPE Dictionary content
Best Practices	Best practices in the development, maintenance and implementation of CPE
Governance	Policy oversight of CPE Specification development, change management, interoperability, and stakeholder interests
Specification Changes	Changes to version 2.2 of the official CPE Specification
Quality Assurance	CPE Quality Assurance practices and measures
CPE Language	The CPE Language (contained in version 2.2 of the CPE Specification)
Outreach	Activities that raise awareness of CPE, solicit participation in the CPE community, and make a business case for CPE adoption
Usability	The ease of use of CPE and CPE-related artifacts (e.g. specification and documentation)
Implementation Support	Shared methods, tools, and documentation that facilitate the implementation of CPE in Security Automation tools and systems
Adoption	Community acceptance of CPE as evidenced by the deployment of CPE-compliant product offerings

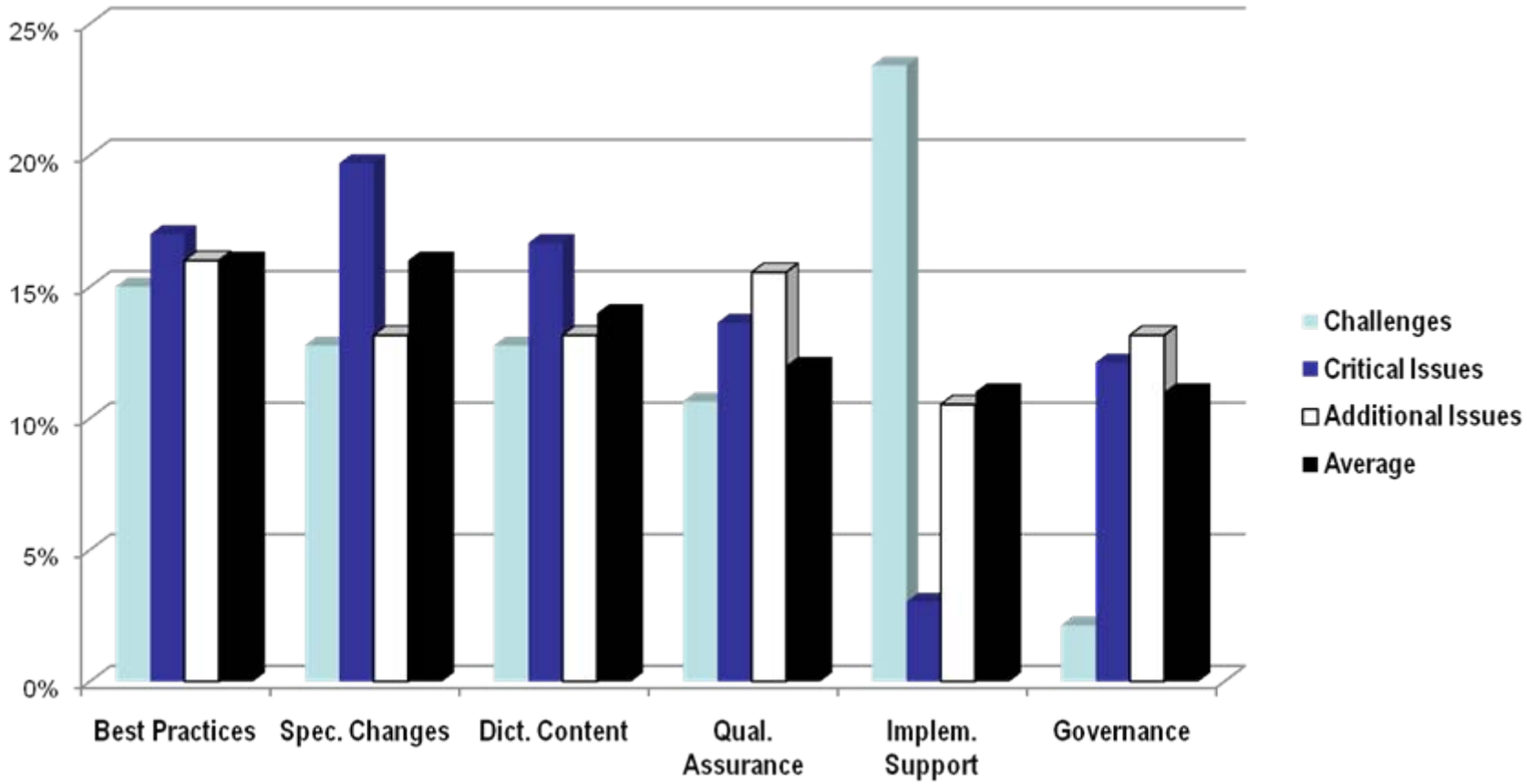
Top 80% of Responses by Category

Top 6 response Categories in Rank Order

Rank	Category	Percent Total
1	Best Practices	16 %
2	Specification Changes	16 %
3	Dictionary Content	14 %
4	Quality Assurance	12 %
5	Implementation Support	11 %
6	Governance	11 %
Total		**80%**

Top 6 Categories Per Question

Challenges and Issues by Percent Category



Setting Expectations

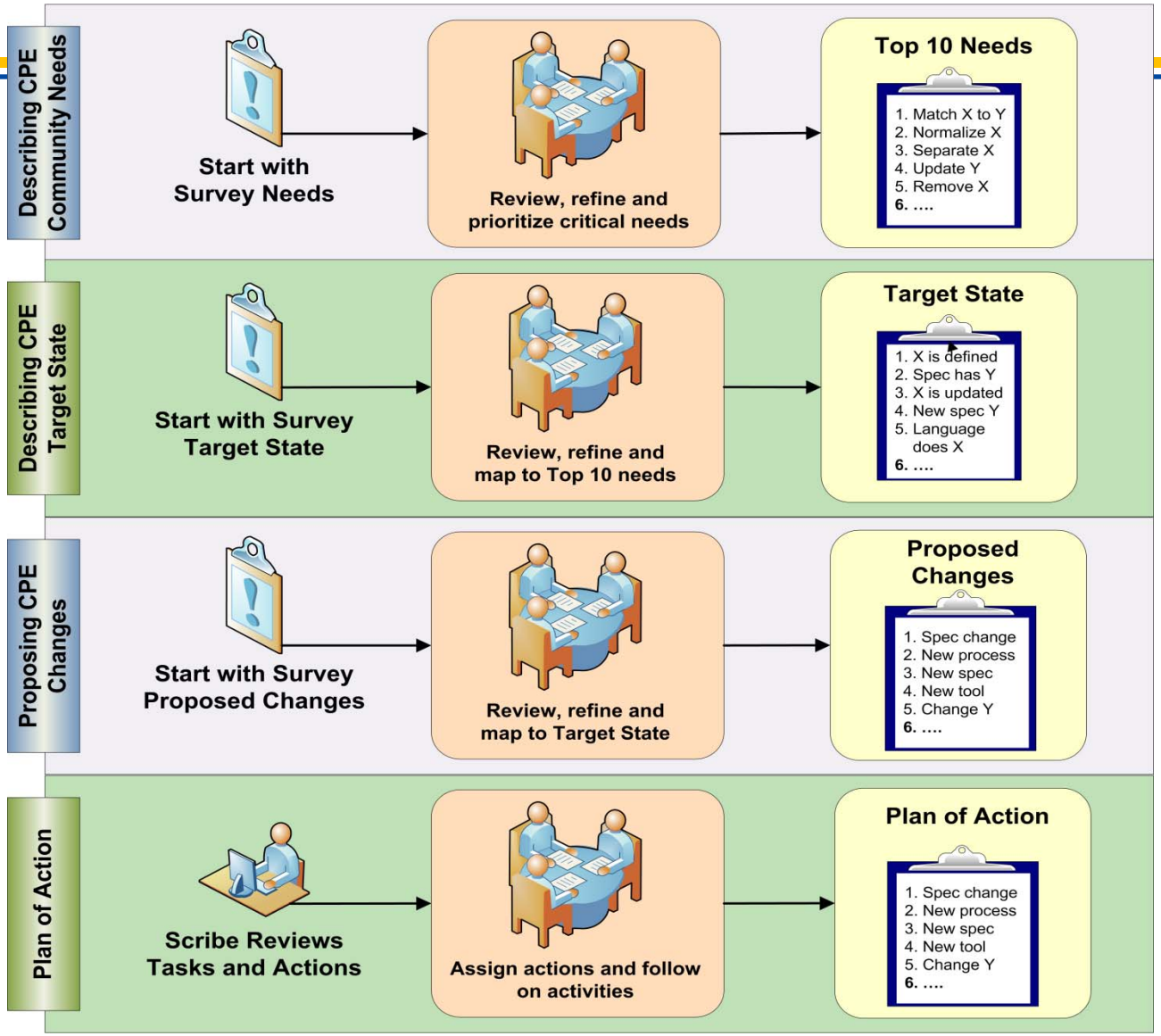
- **Need active participation from all attendees**
  - Especially the vendors
- **Goal is consensus, not necessarily agreement**
  - Consensus guidance to the Core Team on what we need to do to make CPE successful
- **Emphasis on specific, feasible recommendations**

Simpler May Be Better

- **"As with CVE, a smaller focus is better and easier to use and then other things can be built on those initial building blocks. Currently we are overdoing it."**
- **"Change the mentality from an academic endeavor to a production mentality. It is currently being used and cannot be radically changed."**
- **"Put a stake in the ground and quit trying to constantly change it."**

Simpler May Be Better

CPE Workshop Activities

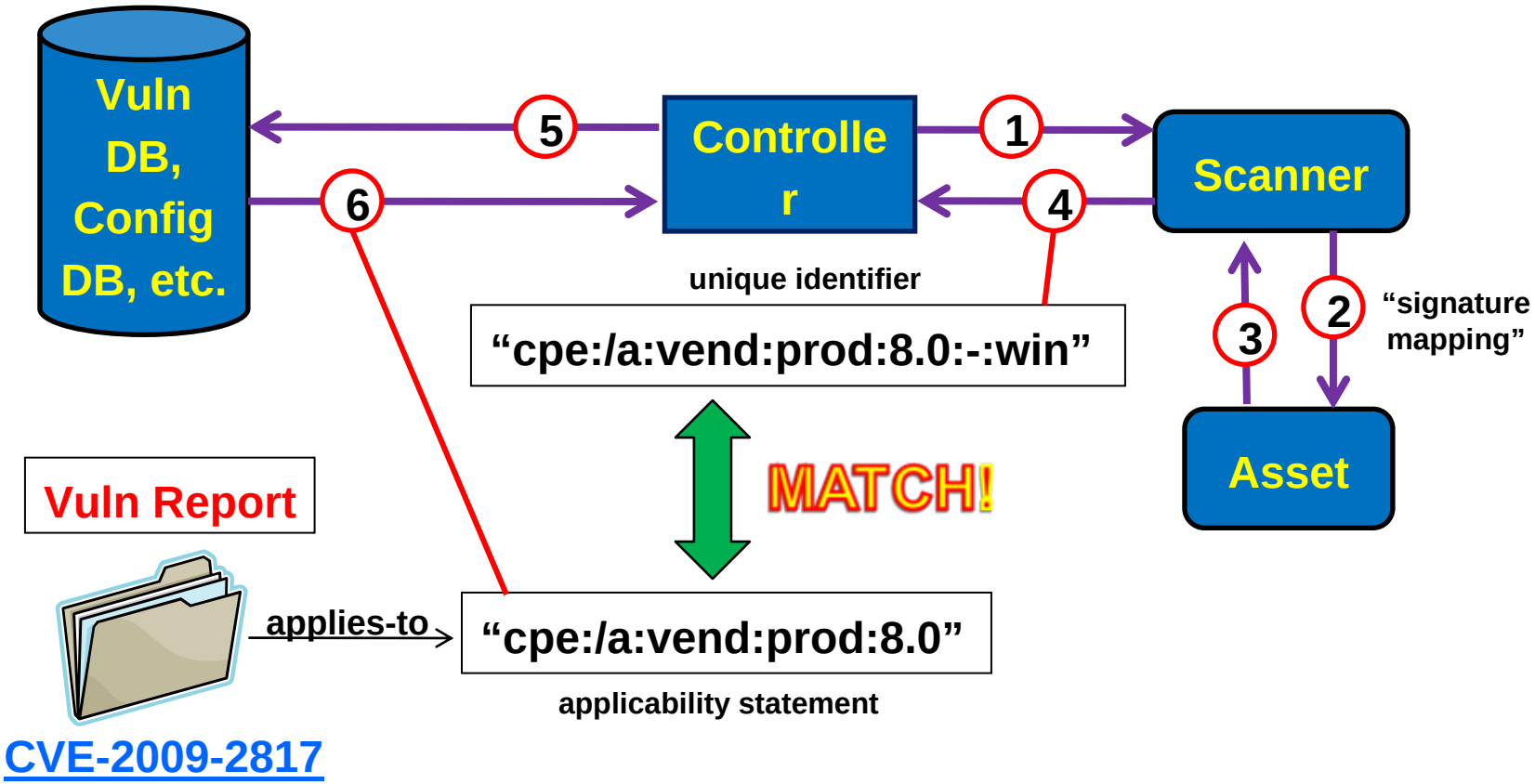


Ground Rules

- **This meeting is at the UNCLASSIFIED level**
- **Please sign in:**
  - Initial next to or add your name
  - Verify and correct/add contact information
- **One conversation at a time**
- **Must display visitor badge at all times**
- **Please return from breaks on time**
- **Workshop roles**
  - Facilitators: foster polite on-topic discussion
  - Moderators: keep us on track
  - Scribe: records workshop

CPE WORKSHOP SEGMENT 2: COMMUNITY NEEDS

CPE 2.x CONOP: Overview



CPE WORKSHOP SEGMENT 4: PROPOSING CHANGES

Segment 4: Thematic Question

- **What specific changes (additions, deletions, documented implementation guidance) do we need to make to the CPE specification in order to achieve the target state?**

Approach

- **Iterative elicitation:**
  - Propose a specific change (ideally, with champion)
  - Tie it back to a target capability
  - Triage it: would it break backward compatibility?
  - Straw poll: does the proposal have support?
  - Rinse and repeat
- **Prioritize:**
  - Group into “for 2.3” and “for 3.0” bins
  - Consensus rank if possible (H/M/L)

Some Candidates

1. Limit scope of Dictionary to only those products with reported vulnerabilities
2. Limit dictionary scope to “concrete” products
3. Drop the “prefix property” requirement
4. Unpack “edition” component
5. Break CPE up into a set of controlled vocabularies, a naming format, and a Dictionary standard
6. Define an alternative (non-URI) transport format
7. Drop the CPE Language from the spec
8. Make CPE names “searchable”
9. Exclude “hardware” from CPE

More Candidates

- Assign GUIDs to CPEs
- Reserve tentative vendor names
- Define translation algorithm from complex version to standard CPE version

CPE WORKSHOP SEGMENT 5: ACTION PLANNING

Wrap-up

- **Action items and responsible parties?**
- **Monthly Core Team web conferences?**
- **When next DevDay workshop?**
- **Actions for all:**
  - Send feedback on today's workshop to cpe-list or bcheikes@mitre.org
  - Please continue today's work on the discussion list, e.g., continue to post proposed changes
  - Stay engaged!