
# Introducing XCCDF 1.2

Charles Schmidt – The MITRE Corp.

September 28, 2010

MITRE



Supported by NSA contract number W15P7T-10-C-F600

# Contents

- Intro to XCCDF 1.2
- The new features in XCCDF 1.2
- Looking forward





Supported by NSA contract number W15P7T-10-C-F600

# The Creation of XCCDF 1.2

- **Two in-person developer meetings**
  - **Oct 29, 2009 – 5th IT Security Automation Conference**
  - **Feb 23, 2010 – Winter 2010 Developer Days**
- **Six public developer teleconferences**

- **Thank you to the many, many contributors**
  - **Please continue to provide feedback – community input is what keeps standards relevant**





Supported by NSA contract number W15P7T-10-C-F600

# New in XCCDF 1.2

- Complex Values – XCCDF variables can now hold and pass lists or externally defined data structures
- Check negations – check results can be negated
- Update to use CPE 2.3
- Expanded metadata use – metadata fields are more flexible and exist in more locations
- Status fields also expanded to support Dublin Core elements
- Check-import – use was clarified and expanded to better support import of XML structures from the checking system
- Multi-check – support for reporting check results individually (e.g. patch scans can now report per-patch)
- Expanded descriptions/examples for several important features
- Deprecation of a few unused and confusing features
- Many minor fixes to improve document clarity





Supported by NSA contract number W15P7T-10-C-F600

# Complex Values

- **New structures for Values and Profiles**
  - **Can hold lists of simple data values**
  - **Can use externally defined, XML-based data types**
- **No longer forced to use one, simple value**
  - **Brings XCCDF in line with the current capabilities of OVAL**
  - **Ability to use external data types will help XCCDF remain current as check languages advance**





Supported by NSA contract number W15P7T-10-C-F600

# Complex Value Examples - Lists

- Previously only single values were allowed
  - E.g., string = “Bob Jones”
- OVAL can handle lists
  - Checks were written that scanned for lists of valid users
  - XCCDF unable to pass values to such checks
- New structures allow passing of lists
  - E.g., “Bob Jones, Mary Smith, Alice Johnson”
  - No longer need to hard-code this into the OVAL
  - Number lists and boolean lists also supported





Supported by NSA contract number W15P7T-10-C-F600

# Complex Value Examples – External Types

- Previously only number, string, and boolean
- OVAL 5.7 defines 10 data types
  - Currently, all can be represented by strings, but still…
- XCCDF 1.2 allows externally defined types
  - Can use OVAL schema to check data correctness
  - If checking language supports structured data, XCCDF 1.2 can support





Supported by NSA contract number W15P7T-10-C-F600

# Check Negation

- Check results can now be negated
  - Invert meaning of standard check-result to XCCDF-result mapping
- Example:
  - OVAL inventory definition can check for presence of IE 5
  - Inventory definitions map to “Pass” if software is found (OVAL result of “True”)
    - Stipulated in SCAP requirements – NIST SP 800-126
  - Now we can create a policy statement that IE 5 not be installed using the existing inventory check
    - Negate the check referencing IE 5 inventory check





Supported by NSA contract number W15P7T-10-C-F600

# CPE Compatibility

- XCCDF updated to use latest version of CPE
- Previously XCCDF 1.1.4 mandated use of CPE 2.0
- XCCDF can now…
  - XCCDF 1.2 requires CPE 2.3
  - All prior platform identifier support is deprecated
    - CPE 2.0 is valid under CPE 2.3 – no content deprecation
- CPE 2.3 is significantly refined over CPE 2.0





Supported by NSA contract number W15P7T-10-C-F600

# Metadata

- **Metadata field expanded**
  - **Any XML-structure accepted for metadata**
    - **Previously only Dublin Core allowed**
  - **Metadata fields added to all major structures**
  - **Also added dc-status field to major structures**
    - **Holds additional status details using Dublin Core**

- **Communities of interest can now mark-up content to add value**





Supported by NSA contract number W15P7T-10-C-F600

# Check Import

- Check-import property was clarified
  - Check-import is used to record findings
  - Clarify how imported information is to be identified
- Import-xpath attribute was added
  - Clarifications allow for the importing of XML structures
  - Import-xpath allows winnowing of these structures

- XCCDF can now…
  - Record reasons for results
  - Collect general findings for recordkeeping purposes





Supported by NSA contract number W15P7T-10-C-F600

# Multi-check

- New multi-check property
  - A single XCCDF Rule could be assessed by a series of several checks
  - Previously, this would produce one result
    - 45 pass, 2 fail = fail
    - Would need to dig through the OVAL results to see what caused the failure
- Multi-check provides means to report each check result in the XCCDF results
  - Easier to track causes of failures





Supported by NSA contract number W15P7T-10-C-F600

# Text Classification

- **Enhanced text representations**
  - Old way – manual inclusion of HTML
    - **Could result in non-uniform appearance**
  - **New tags usable by stylesheets**
    - **Uniform appearance in prose documents**
    - **Tools can impose own style conventions**

| Class Value | Meaning |
|---|---|
| license | Indicates licensing and use information |
| copyright | Indicates copyright and ownership information |
| tangent | Indicates a block of text that contains tangentially related information (possibly appropriate for inclusion as a sidebar or a pop-up) |
| warning | Indicates pitfalls or cautions relative to the surrounding text. High-level and general warnings should appear in designated warning fields, if available. |
| critical | Indicates content of critical importance to the user |
| example | Indicates an example of some kind |
| instructions | Indicates special instructions to the user |
| default | General information. Empty or absent class attributes also imply "default" appearance. This tag allows authors to explicitly indicate text should appear in the default format. |





Supported by NSA contract number W15P7T-10-C-F600

# Selector Processing

- **Profile selectors now can overlap**
  - **Previously: specification prohibited two refine-value (etc.) statements that tailored the same id**
  - **Now no restriction**
  - **Any ambiguities removed by further clarifying Profile processing: strictly top-down**
- **Primary use is for creating extended Profiles**
  - **Allows more efficient re-use of Profiles**

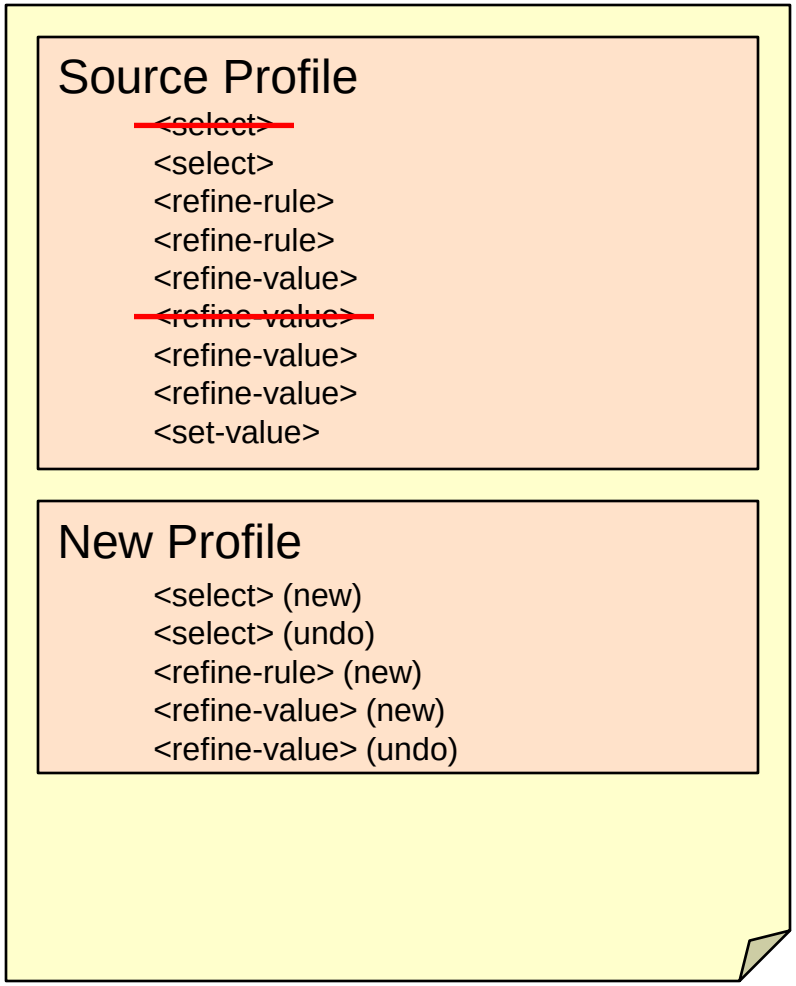




Supported by NSA contract number W15P7T-10-C-F600

# Selector Processing Example

- **Source document with Profiles**
- **Add new Profile**
  - **Profile can add new tailoring actions (1.1.4)**
  - **Profile can undo actions in the extended Profile (1.2)**
- **No need to manually duplicate Profiles just to remove an action**



# Looking Forward

- There are still a couple open issues
  - Other feature requests are welcome
- XCCDF 2.0
  - Looking at options for XCCDF 2.0
  - Everything is on the table
- Will have regular developer meetings to continue the community dialog on XCCDF
  - First of these meetings is tomorrow





Supported by NSA contract number W15P7T-10-C-F600

XCCDF
security
benchmark
automation

# Thank You!





Supported by NSA contract number W15P7T-10-C-F600