XCCDF 1.2

Charles Schmidt – The MITRE Corp.

November 1, 2011

MITRE

Approved for Public Release; Distribution Unlimited: 10-2908

© 2011 The MITRE Corporation. All rights reserved

Supported by NSA contract number W15P7T-11-C-F600

Contents

- Intro to XCCDF 1.2
- Changes in XCCDF 1.2
- Mapping between XCCDF 1.1.4 and XCCDF 1.2
- Looking forward

Approved for Public Release; Distribution Unlimited: 10-2908

© 2011 The MITRE Corporation. All rights reserved

Supported by NSA contract number W15P7T-11-C-F600

The Creation of XCCDF 1.2

- Under active development since 2009
  - First public draft released by NIST in late 2010
- 5 in-person developer meetings and a dozen public developer teleconferences
- 60 issues tracked and closed
  - About 50% led to changes in the specification
- Thank you to the many, many contributors
  - Please continue to provide feedback – community input is what keeps standards relevant

Approved for Public Release; Distribution Unlimited: 10-2908

© 2011 The MITRE Corporation. All rights reserved

Supported by NSA contract number W15P7T-11-C-F600

XCCDF 1.2

- New specification and schema finalized on Sept 30
- Referenced in SCAP 1.2
- Includes a completely re-structured specification
  - Better organized as a reference
- Schema has been more fully commented and a schema dictionary has been generated
- Revised reference interpreter available on SourceForge

Approved for Public Release; Distribution Unlimited: 10-2908

© 2011 The MITRE Corporation. All rights reserved

Supported by NSA contract number W15P7T-11-C-F600

New in XCCDF 1.2 - Checking

- **Complex Values – XCCDF variables can now hold and pass lists**
- **Multi-check – support for reporting check results individually (e.g. patch scans can now report per-patch)**
- **Tailoring – allow external files to tailor Benchmarks**
- **Check-import – use was clarified and expanded to better support import of XML structures from the checking system**
- **Check negations – check results can be negated**
- **Update to use CPE 2.3 – both format String and URI bindings**

Approved for Public Release; Distribution Unlimited: 10-2908

© 2011 The MITRE Corporation. All rights reserved

Supported by NSA contract number W15P7T-11-C-F600

New in XCCDF 1.2 – Organization & Presentation

- Expanded metadata use – metadata fields are more flexible and exist in more locations
- Status fields expanded to support Dublin Core elements
- Text classification – normalize presentation
- Use attribute in sub elements – control text substitution
- Standardized id formats – allow global uniqueness
- Asset Identification – new structures in TestResults
- External attributes for ident – allows extension by third parties
- Group extension and impact-metric now deprecated

Approved for Public Release; Distribution Unlimited: 10-2908

© 2011 The MITRE Corporation. All rights reserved

Supported by NSA contract number W15P7T-11-C-F600

Complex Values

- Values can now hold and export lists (in addition to singletons)
  - Better alignment with OVAL variables
  - Previously, complex values included export of arbitrary XML too; this was later removed
- New elements added, aligned with existing Value elements
  - <value> interchangeable with <complex-value>
  - <default> interchangeable with <complex-default>
  - <choice> interchangeable with <complex-choice>
  - In Profile/TestResult, <set-value> interchangeable with <set-complex-value>
- Complex structures consist of 0 or more <item> elements
  - 0 elements indicates an empty list
  - 1 item is a list of one (not a singleton value)
    - Most check engines probably don't care, but the option is there

Approved for Public Release; Distribution Unlimited: 10-2908

© 2011 The MITRE Corporation. All rights reserved

Supported by NSA contract number W15P7T-11-C-F600

Complex Values - Previously

```
<definition class="compliance" id="oval:org.example:def:602000" version="1">
    <metadata>
        <title>The 'Deny log on as a batch job' user right shall be assigned to the
               appropriate accounts.</title>
        <affected family="windows"/>
    </metadata>
    <criteria operator="AND">
        <criterion comment="Verify the input users have the correct privilege"
                   test_ref="oval:org.example:tst:1"/>
    </criteria>
</definition>

<variables>
   <constant_variable id="oval:org.example:var:1" version="1"
                      datatype="string" comment="list of users">
      <value>Support_388945a0</value>
      <value>Guests</value>
   </constant_variable>
</variables>
```

List values required OVAL constant variables. Only controlled in XCCDF through different definition selection.

© 2011 The MITRE Corporation. All rights reserved

Supported by NSA contract number W15P7T-11-C-F600

Complex Values - Example

```
<Value id="xccdf_org.example_value_DenyLogOnUsers">
   <complex-value selector="Support">
      <item>Support</item>
      <item>Guest</item>
   </complex-value>
   <complex-value selector="AllDepts">
      <item>Finance</item>
      <item>Engineering</item>
      <item>Marketing</item>
      <item>Support</item>
      <item>Guest</item>
   </complex-value>
   <value selector="GuestOnly">Guest</value>
</Value>
```


© 2011 The MITRE Corporation. All rights reserved

Supported by NSA contract number W15P7T-11-C-F600

Multi-check

- New multi-check property
  - A single XCCDF Rule check could be assessed by a series of several checking language definitions
  - 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
  - More granular scoring
- Attribute of <check> elements; use Profile selectors to chose between multi-check/non-multi-check assessment

Approved for Public Release; Distribution Unlimited: 10-2908

© 2011 The MITRE Corporation. All rights reserved

Supported by NSA contract number W15P7T-11-C-F600

Multi-check - Previously

```
<Rule id= "xccdf_gov.nist.usgcb.rhel_rule_security_patches_up_to_date"
      selected="false" weight="10.0" >
   <status date="2010-07-01">draft</status>
   <version update="1"/>
   <title>Ensure software is up to date</title>
   <description>The following command prints a list of packages that need
                to be updated:<xhtml:br/>
                 <xhtml:code># yum check-update</xhtml:code>
   </description>
   <check system="http://oval.mitre.org/XMLSchema/oval-definitions-5">
      <check-content-ref
          href="http://www.redhat.com/security/data/oval/com.redhat.rhsa-all.xml"/>
   </check>
</Rule>

<rule-result idref="xccdf_gov.nist.usgcb.rhel_rule_security_patches_up_to_date">
   <result>fail</result>
   <check system="http://oval.mitre.org/XMLSchema/oval-results-5">
      <check-content-ref
          href="file:/C:/scanner/rslt/06102011-091919/com.redhat.rhsa-all.xml"/>
   </check>
</rule-result>
```

?

© 2011 The MITRE Corporation. All rights reserved

Supported by NSA contract number W15P7T-11-C-F600

Multi-check - Example

```
<rule-result idref="xccdf_gov.nist.usgcb.rhel_rule_security_patches_up_to_date">
      <result>pass</result>
      <check system="http://oval.mitre.org/XMLSchema/oval-results-5">
        <check-content-ref name="oval:com.redhat.rhsa:def:20030315"
                href="file:/C:/scanner/rslt/06102011-091919/com.redhat.rhsa-all.xml"/>
      </check>
</rule-result>
<rule-result idref="xccdf_gov.nist.usgcb.rhel_rule_security_patches_up_to_date">
      <result>pass</result>
      <check system="http://oval.mitre.org/XMLSchema/oval-results-5">
        <check-content-ref name="oval:com.redhat.rhsa:def:20030317"
                href="file:/C:/scanner/rslt/06102011-091919/com.redhat.rhsa-all.xml"/>
      </check>
</rule-result>
<rule-result idref="xccdf_gov.nist.usgcb.rhel_rule_security_patches_up_to_date">
      <result>fail</result>
      <check system="http://oval.mitre.org/XMLSchema/oval-results-5">
        <check-content-ref name="oval:com.redhat.rhsa:def:20030324"
                href="file:/C:/scanner/rslt/06102011-091919/com.redhat.rhsa-all.xml"/>
      </check>
</rule-result>
...
```


© 2011 The MITRE Corporation. All rights reserved

Supported by NSA contract number W15P7T-11-C-F600

Tailoring

- New Tailoring element
  - Associated with a specific Benchmark, but in a separate file
  - Holds Profile elements (and some metadata)
  - Can record manual tailoring actions for auditing
  - Can be used as input to Benchmark processing, tailoring settings
- Effectively adds one or more Profiles to a Benchmark (without modifying the Benchmark file)
  - Tailoring Profiles can extend Benchmark Profiles
  - Tailoring Profiles can shadow Benchmark Profiles
- TestResults point reference Tailoring file if used
  - Allows tracking of changes to be recorded in results

Approved for Public Release; Distribution Unlimited: 10-2908

© 2011 The MITRE Corporation. All rights reserved

Supported by NSA contract number W15P7T-11-C-F600

Tailoring - Example

```
<Tailoring id="xccdf_org.example_tailoring_usgcb_local_mods">
  <version time="2011-10-06T09:19:19-04:00">1</version>
  <Profile       id="xccdf_gov.nist.usgcb.win_profile_USGCB_version_1.1.0.0"
          extends="xccdf_gov.nist.usgcb.win_profile_USGCB_version_1.1.0.0">
    <title>Local modifications of USGCB profile</title>
    <description>This contains tailoring of the USGCB v1.1.0.0 for Windows,
                 modifying it to reflect local domain requirements.</description>
    <refine-value idref="xccdf_gov.nist.usgcb.win_value_sensitive_privilege_use"
                  selector="failure">
      <remark>Root profile sets to "success_failure"</remark>
    </refine-value>
    <select idref="prevent_the_computer_from_joining_a_homegroup"
            selected="false">
      <remark>Root profile sets to "true"</remark>
    </select>
  </Profile>
</Tailoring>
```


© 2011 The MITRE Corporation. All rights reserved

Supported by NSA contract number W15P7T-11-C-F600

Tailoring – Example Results

```
<TestResult id="xccdf_org.example_testresult_usgcb_6-10-2011"
            end-time="2011-10-09T011:21:11-04:00" version="1.1.0.0">
  <benchmark
      href="file:/C:/scanner/src/USGCB/Win7/USGCB-Windows-7-xccdf.xml"
      id="xccdf_gov.nist.usgcb.win_benchmark_USGCB-Windows-7"/>
  <tailoring-file
      href="file:/C:/scanner/tlr/USGCB/Win7/USGCB-Windows-7-xccdf.tlr.xml“
      id="xccdf_org.example_tailoring_usgcb_local_mods" version="1"
      time="2011-10-06T09:19:19-04:00"/>
  <profile
      idref="xccdf_gov.nist.usgcb.win_profile_USGCB_version_1.1.0.0"/>
  <target>testmachine.example.org</target>
  <rule-result …
```


© 2011 The MITRE Corporation. All rights reserved

Supported by NSA contract number W15P7T-11-C-F600

Check Import

- Check-import property was clarified
  - Check-import is used to record artifacts (not populating Values)
- Import-xpath attribute was added
  - Clarifications allow for the importing of XML structures
  - Import-xpath allows winnowing of these structures
- XCCDF spec alone cannot ensure compatible use of feature
  - Requires a mapping between a name and a check result structure
  - Similar to how check-content-refs map IDs to check structures
    - Mapping is spelled out in SCAP
  - Currently, authors/vendors must define own mapping
  - Future works will define “official” mappings
    - But not in the XCCDF spec

Approved for Public Release; Distribution Unlimited: 10-2908

© 2011 The MITRE Corporation. All rights reserved

Supported by NSA contract number W15P7T-11-C-F600

Check Import - Example

```
<Rule id="xccdf_gov.nist.usgcb.rhel_rule_minimum_password_length">
  <check system="http://oval.mitre.org/XMLSchema/oval-definitions-5">
    <check-import import-name="oval:gov.nist.usgcb.windowsseven:obj:27"
                  import-xpath="/passwordpolicy_item/min_passwd_len"/>
    <check-export export-name="oval:gov.nist.usgcb.windowsseven:var:22"
                  value-id="password_minimum_length_var" />
    <check-content-ref href="USGCB-Windows-7-oval.xml"
                       name="oval:gov.nist.usgcb.windowsseven:def:7" />
  </check>
</Rule>
```

- Collect the entity mapped to the name “oval:gov.nist.usgcb.windowsseven:obj:27”
- From that entity, display the value found at the Xpath “/passwordpolicy_item/min_passwd_len”

© 2011 The MITRE Corporation. All rights reserved

Supported by NSA contract number W15P7T-11-C-F600

Check Import – Example Results (No XPath)

```
<rule-result idref="xccdf_gov.nist.usgcb.rhel_rule_minimum_password_length">
    <result>pass</result>
    <check system="http://oval.mitre.org/XMLSchema/oval-results-5">
      <check-import import-name="oval:gov.nist.usgcb.windowsseven:obj:27">
        <passwordpolicy_item id="374">
          <max_passwd_age datatype="int">15552000</max_passwd_age>
          <min_passwd_age datatype="int">0</min_passwd_age>
          <min_passwd_len datatype="int">12</min_passwd_len>
          <password_complexity
                  datatype="boolean">true</password_complexity>
          <reversible_encryption
                  datatype="boolean">false</reversible_encryption>
        </passwordpolicy_item>
      </check-import>
      <check-content-ref
          href="file:/C:/scanner/rslt/06102011-091919/USGCB-Windows-7-oval.xml"
          name="oval:gov.nist.usgcb.windowsseven:def:7" />
    </check>
</rule-result>
```


© 2011 The MITRE Corporation. All rights reserved

Supported by NSA contract number W15P7T-11-C-F600

Check Import – Example Results

```
<rule-result idref="xccdf_gov.nist.usgcb.rhel_rule_minimum_password_length">
    <result>pass</result>
    <check system="http://oval.mitre.org/XMLSchema/oval-results-5">
      <check-import import-name="oval:gov.nist.usgcb.windowsseven:obj:27"
                    import-xpath="/passwordpolicy_item/min_passwd_len">
        12
      </check-import>
      <check-content-ref
          href="file:/C:/scanner/rslt/06102011-091919/USGCB-Windows-7-oval.xml"
          name="oval:gov.nist.usgcb.windowsseven:def:7" />
    </check>
</rule-result>
```


© 2011 The MITRE Corporation. All rights reserved

Supported by NSA contract number W15P7T-11-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

Approved for Public Release; Distribution Unlimited: 10-2908

© 2011 The MITRE Corporation. All rights reserved

Supported by NSA contract number W15P7T-11-C-F600

External attributes in ident

- A rule's ident attribute used for permanent identifiers
  - E.g., CVE, CCE, or CPE ids
- SCAP adds a specific meaning to the ident field
  - CPE in ident = test is for presence of that platform
  - This meaning goes beyond the meaning imposed by XCCDF
- There was interest in SCAP in adding nuance to this meaning
  - E.g., add a negate: !CPE = test is for absence of platform
  - But a negate attribute would only be meaningful in SCAP
- Solution: allow any external attribute in ident
  - Other authorities add their own custom attributes
- Consider: Other places where similar treatment reasonable?
  - Existing proposal to open XCCDF to other namespace content

Approved for Public Release; Distribution Unlimited: 10-2908

© 2011 The MITRE Corporation. All rights reserved

Supported by NSA contract number W15P7T-11-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
  - Formatted String binding recommended
  - URI binding accepted

Approved for Public Release; Distribution Unlimited: 10-2908

© 2011 The MITRE Corporation. All rights reserved

Supported by NSA contract number W15P7T-11-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**
  - **Proposals to standardize meanings of certain types of metadata are under consideration**

Approved for Public Release; Distribution Unlimited: 10-2908

© 2011 The MITRE Corporation. All rights reserved

Supported by NSA contract number W15P7T-11-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**
- **Precise style conventions now in hands of consumers**

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.

Approved for Public Release; Distribution Unlimited: 10-2908

© 2011 The MITRE Corporation. All rights reserved

Supported by NSA contract number W15P7T-11-C-F600

Text Classification - Example

```
<description xml:lang="en">
    <xhtml:span class="default">The minimum password length must be
        set appropriately.</xhtml:span>
    <xhtml:span class="warning">This setting only applies to new
        passwords. Existing passwords may not be compliant.
    </xhtml:span>
    <xhtml:span class="critical">A minimum password length of 0 allows
        accounts without any password.</xhtml:span>
</description>
```


MITRE

Approved for Public Release; Distribution Unlimited: 10-2908

© 2011 The MITRE Corporation. All rights reserved

Supported by NSA contract number W15P7T-11-C-F600

Text Classification – Example Output

XCCDF
security benchmark automation

The minimum password length must be set appropriately.

This setting only applies to new passwords. Existing passwords may not be compliant.

A minimum password length of 0 allows accounts without any password.

The minimum password length must be set appropriately.

This setting only applies to new passwords. Existing passwords may not be compliant.

A minimum password length of 0 allows accounts without any password.

Approved for Public Release; Distribution Unlimited: 10-2908

© 2011 The MITRE Corporation. All rights reserved
Supported by NSA contract number W15P7T-11-C-F600

Use attribute in <sub>

- The <sub> element used for text substitution
  - In XCCDF 1.1.4, substitution was context dependent
    - Value title or value depending on activity
- Added @use attribute
  - Can have value of “value”, “title”, or “legacy” (default=“value”)
  - Allows explicit control of text substitution
  - “legacy” indicates XCCDF 1.1.4 behavior

Approved for Public Release; Distribution Unlimited: 10-2908

© 2011 The MITRE Corporation. All rights reserved

Supported by NSA contract number W15P7T-11-C-F600

Standardized id formats

- The id attribute of Benchmark, Rule, Group, Value, TestResult, and Tailoring elements must match pattern
  - xccdf_*namespace*_benchmark_*name*
  - xccdf_*namespace*_rule_*name*
  - Etc.
  - Namespace is a reverse-DNS string
  - Name is any NCName-compatible string
- id attribute is still NCName compliant
  - Compatibility with the XML ID type
  - The reason for _ instead of : as separator
- Trivial to convert XCCDF 1.1.4 ids to XCCDF 1.2 ids
- Authors would have their own namespace value
  - Allows better practices for globally unique ids

Approved for Public Release; Distribution Unlimited: 10-2908

© 2011 The MITRE Corporation. All rights reserved

Supported by NSA contract number W15P7T-11-C-F600

Asset Identification

- In XCCDF 1.1.4 assessed targets identified by “target” elements
  - target, target-address, target-facts
  - All use XCCDF-specific structures
- In XCCDF 1.2, fields added to allow use of other standards
  - target-id-ref can be used to point to external identification structures
  - Non-XCCDF elements also allowed in TestResults
- Nominal example: Asset Identification language
  - Specified in NIST IR 7693 (DRAFT)
  - Used to identify a network asset through a variety of mechanisms
    - Identifiers either intrinsic or synthetic

Approved for Public Release; Distribution Unlimited: 10-2908

© 2011 The MITRE Corporation. All rights reserved

Supported by NSA contract number W15P7T-11-C-F600

Converting 1.1.4 to 1.2

- Content is not “transparently” backwards compatible
  - It is “mechanically” backwards compatible
- Several changes needed for schema compliance
  - Update XML namespace
  - Update id formats
  - Add use attribute to <sub> elements
  - Shift deprecated fields to <metadata>
  - Resolve any Group extension
- Appendix A of the XCCDF 1.2 spec outlines all steps
- An XSLT will come out in the next month that automates all this

Approved for Public Release; Distribution Unlimited: 10-2908

© 2011 The MITRE Corporation. All rights reserved

Supported by NSA contract number W15P7T-11-C-F600

Looking Forward

- The XCCDF Interpreter supports all checking changes
  - http://sourceforge.net/projects/xccdfexec/
- An XSLT stylesheet is being developed to convert content from XCCDF 1.1.4 to XCCDF 1.2
- Try the new features

- 29 more issues currently open
  - Other feature requests are welcome
- Will have regular developer meetings to continue the community dialog on XCCDF

Approved for Public Release; Distribution Unlimited: 10-2908

© 2011 The MITRE Corporation. All rights reserved

Supported by NSA contract number W15P7T-11-C-F600

XCCDF
security
benchmark
automation

Questions?

Approved for Public Release; Distribution Unlimited: 10-2908

© 2011 The MITRE Corporation. All rights reserved

Supported by NSA contract number W15P7T-11-C-F600