



XCCDF Technical Deep Dive

October 29, 2009

Significant Remaining Open Issues

Proposed Dates	Topic
Oct 29, Security Automation Conference	XCCDF Values: appropriate data types, appropriate formats (singleton, list, RDF?), and global vs. local variables
~Nov 17-18	External Profiles
~Dec 8-10	Multiple proposals regarding XCCDF extension processing
~Jan 12-14	Value population
~Feb 2-4	Mapping of XCCDF-check language results & scoring model suggestions
~Feb 23-25	Miscellaneous clarifications of ambiguous items

Wrap-up from Previous Discussion

- **Explicit versioning in check-refs and results**
- **2 follow on discussions**
 - **What is the appropriate format of a URI reference**
 - href="file", name="name#version"
 - href="file#name#version"
 - **Practicality**
 - **Noted that, without meticulous adherence to policy specifications, OVAL Definitions won't reflect low-level changes**
 - **Solutions**
 - Rely on policy
 - New definition_trace structure in OVAL
 - Drop use of versions and go to signatures

New Topic: XCCDF Values

- **More standardized approach to Value datatype?**
- **Support for more complex Value structures**
 - Lists, named records, etc.
- **Support for global vs. local mappings**

XCCDF Values – Discussion Questions

1. Is allowing Values to contain lists sufficient or do we need named-values?
2. Do we want to have new structures in profiles to add/removed members from lists/name-value pair?
3. Do we want to have each element of a list/name-value pair added in its own XML element in Value, or do we want to force an encoding so special characters are not confused.
4. Is it necessary for XCCDF to identify the data-type of its contents? If so, should this typing utilize standardized types and which standard list of types should be used?
5. Is there a need for global Values?
 - a. Where would a global mapping be declared? Current location? A separate section? Profiles?
 - b. Could local mappings override global mappings or would this be an error?
 - c. How would multiple mappings of the same scope be handled? Error? Last one (structurally) prevails?