OVAL Developer Days

April 28-29, 2008

The MITRE Corporation
Bedford, MA

Agenda

Monday April 28th 2008

10:00 - 10:15 **welcome**

- *Introductions*
- *MITRE's Role*
- *Goals for the Next Two Days*

10:15 - 10:30 **overview**

- *What Goes into a Major Version*
- *Additional Minor Releases*
- *Timeframes*

10:30 - 11:30 **v6 working session**

- *Better <affected> Element*

  One of the biggest areas of confusion in the current version of OVAL is the use and purpose of the <affected> element in the metadata section. For Version 6 we would like to merge the <affected> element into the criteria section somehow and avoid the need for duplicate information that currently exists.

  - Topics:
    - review the <affected> element as it exists in Version 5
    - discuss the needs for this information
    - work through proposals

11:30 - 12:00 **discussion**

- *Definitions as the Focal Point*

  The focal point of the OVAL Language is currently the Definition. The expectation is that this is the unit that external languages (i.e., XCCDF, etc) reference. It has been suggested that we treat all OVAL units (Definition, Tests, Object, States, Variables) the same and allow external references into each. Is this a good idea? Related to this in some way, metadata is associated only with the definition. Should we expand the metadata and associate it with each unit?

12:00 - 1:00 **lunch**

1:00 - 2:15 **v6 working session**

- *Reusing Content Across External Repositories*

  OVAL has always strived to facilitate the reuse of content. Many of the changes in Version 5 were an attempt to allow more reuse with an OVAL Document. But reuse is also important across repositories. For example, a patch definition may want to include an existing inventory definition in its criteria.

  - Topics:
    - overview of external repositories found in the OVAL Community
    - discuss the needs and benefits for reuse
    - identify ways to improve support for reuse
    - signing content

- *Supporting Network Devices*

  A number of community members have been asking for better support of network devices. This section will work though the current schemas looking for ways to improve on what is being supported, as well as explore possible additions that will enhance the ability to use OVAL for routers, switches, etc.

  - Topics:
    - overview of current network device schemas
    - examination of the deficiencies in the current schemas
    - possibility of a higher level network platform schema

2:30 - 3:15 **discussion**

- *Repository and Reference Implementation Transition*

  The release of a new major version of OVAL will mean that the reference implementation and the content that exists in the OVAL Repository will need to be updated. For the last major release, we just picked a date and did a conversion. But today, the content is the OVAL Repository is being used by many more community members. Do we need a different plan this time around?

3:30 - 5:00 **v6 working session**

- *Stand-Alone Objects*

  Should objects stand on their own? Currently, each test has its own object. There are a number of tests related to a file, but there is no notion of a shared file object. This could be changed and possibly allow greater flexibility within the language.

  - Topics:
    - overview of OVAL Test and Object structure
    - work though proposals
    - how does this relate to sets?

- *Choice Structure*

  For certain objects, there is a need to have different ways of identifying them. For example, Windows accounts need to be identified by both name and SID depending on the use. The current OVAL Object structure does not allow this. Another example is with the path and filename entities that sometime need to be referenced as a single entity.

- Topics:
  - overview of current objects that need change
  - work though proposals

5:00 - 5:30 **wrap-up**

- *Summary of day's accomplishments*

6:30 - 8:00 **dinner**

Tuesday April 29th 2008

9:00 - 10:00 **v6 working session**

- *Agility*

  New tests and component schemas are constantly being proposed for inclusion in the OVAL Language. How can we make the language more agile to better respond to these additions? Maybe the change needs to be with policy rather than with schema. This session will explore some proposals and try to uncover new ideas that might improve the situation

  - Topics:
    - overview of the current upgrade process
    - discussion about the downfalls of the current process
    - work through proposals

10:00 - 10:30 **discussion**

- *Future of OVAL Compatibility*

  The future of OVAL Compatibility will be discussed. How has this program benefited OVAL and has it been a success? What improvements are needed? We will also discuss the proposed transition to NIST and what criteria must be met before this can happen.

10:45 - 11:30 **v6 working session**

- *Regular Expression Syntax*

  When the pattern match operation was first added to OVAL, POSIX was chosen as the allowed regular expression syntax. There have been a number of discussions recently about changing to a more common syntax as users of OVAL have found it hard to find POSIX compatible engines to use. This session will look into different regular expression syntax and which might be best for OVAL version 6.

  - Topics:
    - overview of different regular expression syntax
    - advantages and disadvantages of each
    - discuss what is needed for OVAL

11:30 - 12:30 **lunch**

12:30 - 12:45 **discussion**

- *XML Footprint*

  As the OVAL Language has grown in both power and flexibility over the past few years, the XML footprint has also grown. Is this a concern of ours? Would a 10% reduction in size provide any benefit? What can we do to reduce this footprint?

12:45 - 3:00 **growth session**

- *Remediation Language*

  One area for improvement that has been identified is in standardizing how one expresses a remediation once an assessment has been made. This session will be used to explore this idea and help determine where such a language should live. Should it be part of OVAL similar to the system characteristics and results schemas? Or should it live on its own?

  - Topics:
    - discuss what is needed in a remediation language
    - mock-up some example XML to express these needs
    - discuss what is needed for this language to flourish

3:00 - 3:30 **wrap-up**

- *Summary of day's accomplishments*