All,

This is a continuation of the series of Selected OVAL issues from the June Developer Days section that we had to cut for time.  This email focuses on OVAL Results.  We would like to review a bit of history and goals with regards to OVAL Results and then share a couple of proposals.

**History**

With the release of OVAL 5.8, we expanded the capability to manage the size and content of OVAL Results. These enhancements arose from the fact that OVAL Results were seen as often being very large and bloated with unneeded information which was effectively hiding the real finding information that was needed. The OVAL Directives concept was expanded upon with the addition of a flag to allow for the explicit inclusion or exclusion of the source OVAL Definitions Document that was used for the evaluation. The community felt that in many cases the source definitions were simply redundant information and only really served a purpose when communicating OVAL Results between different tools. In addition the include/exclude source definitions flag, the ability to specify directives on a class by class basis was added. This capability allows a vulnerability scanner to specifically minimize inventory class results that might have been used while doing a vulnerability scan and provide full details for all vulnerability class results. These two capabilities allowed for a significant reduction in OVAL Results bloat that could be tailored to different OVAL Definition evaluation use cases.

As a reminder, directives give the ability to specify different levels of results following the evaluation of a set of OVAL Definitions. The current levels are ‘full’, which would provide all of the results data, including the OVAL System Characteristics, and ‘thin’, which indicates reporting only the ID and evaluation result for each OVAL Definition, and does not include the OVAL System Characteristics.

On the heels of this capability, a couple additional related capabilities were proposed and deferred while the updates to the OVAL Directives were digested and implemented by the community. These proposals included adding a level between ‘full’ and ‘thin’, and to allow content authors to better highlight the values observed during an assessment, as needed.

For more information regarding these proposals, please see:

NEED TO GET CORRECT REFERENCE

**Current State**

At this point, these OVAL Results capabilities have been in place for some time, and so we have begun reviewing the additional OVAL Results capabilities that had been proposed and deferred to some later release.

After a bit of team thought, we present slightly updated proposals:

1. Include System Data Attribute
2. Reporting/Observed Values

*Include System Data Attribute*

While considering the addition of other levels to the OVAL Directives (the original proposal was to add a level called ‘criteria’ to the ContentEnumeration, the enumeration used to list all of the available levels), the OVAL team realized that allowing such a level could be very difficult for tools to implement. Given the Directives can be set for each type of result (one level for unknown tests, another one for true results, etc.), adding a level in between ‘full’ and ‘thin’ would require extensive manipulation of the OVAL System Characteristics content. Please see the 2010 OVAL Developer Days minutes for additional information (<http://oval.mitre.org/community/docs/OVAL_Developer_Days_2010_Minutes.pdf>). While creating an OVAL Results Document, a tool would need to walk through the OVAL System Characteristics and remove data according to the specified directives.

Therefore, the amended proposal is to provide an optional attribute for the default oval-res:directives element, called ‘include\_system\_data’. This attribute would default to ‘true’, or the current behavior where the System Characteristics content is included as part of the results. When set to false, it would suppress the collected\_objects and system\_data sections of the System Characteristics content, providing the desired intermediate level of communicating OVAL Results. What would remain is simply the generator information and system information allowing a set of results to be connected to a specific system. Without the collected\_objects and system\_data sections a ‘full’ set of OVAL Results would include all criteria information and test information. This would in effect create the desired intermediate level of verbosity.

Combining this new attribute with the existing ‘include\_source\_definitions’ attribute that can suppress the OVAL Definition source, will allow a good deal of control of how much information is included in the OVAL Results. We believe it accomplished this without adding the same level of implementation difficulty that the original proposal did.

Are there questions regarding this proposal?

*Reporting/Observed Values*

Another results-related capability that has been requested is the ability for content authors to better control how important, observed data is reported.  Currently, in order for one to interpret OVAL Results, several steps are required in order to traverse the OVAL Result file until locating the actual assessed values within the OVAL System Characteristics.  With the assumption that the content authors will best know the important values for a given check, this proposal allows those authors to mark values that are particularly important, and should therefore be made more accessible.

Our proposal is to add an optional ‘report\_value’ attribute to all OVAL State Entities in the OVAL Definitions Schema.  This attribute would be optional, defaulting to ‘false’ – or the current behavior where the only place to find observed values is within the System Characteristics.  When set to true by a content author, a tool would be instructed to report the specific value at a much higher level, within the ‘oval-res:test’ construct of the OVAL Results.

The mechanism for the higher level reporting will be an ‘observed\_value’ element added to the OVAL Results Schema to communicate the assessed values.  A ‘oval-res:test’ would have an unbounded set of child ‘observed\_value’ elements.  The ‘observed\_value’ element would hold the ID of the reported item, the instance ID (because a named entity can appear multiple times in an item), the name of the field, its value, and possibly a record ID, if it is part of a record.

**Conclusion**

When combining the two proposals, it would give the ability to provide very useful, but more abbreviated OVAL Results. By suppressing the full OVAL System Characteristics from being included in the results, and allowing content authors to indicate the critical observed values to include in the results, we could achieve a level of results that provides a good indication of why an OVAL Definition was evaluated in a specific manner, but without providing quite as much a volume of data.

Are there additional thoughts or reservations about these features? Will the added capabilities give the level of control that the community will find useful?