

OVAL Board Meeting (10/7/2013)

Attendees

Kent Landfield - McAfee Inc.
Steve Grubb – Red Hat Inc.
Randy Taylor – ThreatGuard, Inc.
Chris Wood – Assuria Limited
Blake Frantz – Center for Internet Security
Amaresh Shirsat – Symantec Corporation
Scott Armstrong – INADEV
William Munyan – Center for Internet Security
Steven Piliero - Unified Compliance

Jon Baker - MITRE
Matt Hansbury - MITRE
Dan Haynes - MITRE
Luis Nunez - MITRE
David Rothenberg - MITRE

Meeting Summary

Welcome

After introductions the group was welcomed to the 2013 4th quarter OVAL Board Meeting.

Status Update

A brief status update of the OVAL project was delivered. The following items were covered:

OVAL Adoption

Recognition as an Official OVAL Adopter

- Beyond Security Ltd. for their AVDS product

Update to the OVAL Adoption Program Requirements and Questionnaire

Additionally, Dan Haynes announced to the group that an update to the [OVAL Adoption Program Requirements](#) has been made to include a requirement for products/services to include the OVAL-supported assessment methods if applicable (see Requirement 3.3). The Adoption Questionnaire, a document that provides detailed responses to a set of questions about a particular product's OVAL support, has been expanded to include the following section:

Assessment Method - A specific method that a product or service uses to evaluate an OVAL Definition. OVAL supports assessment through:

1. Query to a database of an endpoint's (i.e., any computing device that can be connected to a network such as a system, network appliance, mobile device, etc.) current configuration settings.
2. An assessment of state by a host-based sensor.
3. An assessment of state by a remote-scanning sensor.

The team has reached out to the members of the Adoption Program to make them aware of this change and to ask for updates to include this new section as allowed. Several members have responded, though additional responses are encouraged.

OVAL Repository

The OVAL Repository's definition count at the time of the call was 16930. ALTX-SOFT, G2 Inc., and SecPod Technologies received the Top Contributor Awards for the 3rd quarter of 2013 for their submissions to the OVAL Repository.

OVAL Language

The OVAL team released the second draft of the 5.11 version of the Language on 9/25/2013. This draft contains a number of smaller updates, like documentation updates and other minor changes. A complete list of changes can be found in the [changelog](#). The team continues to work on additional updates to the Language.

In order for larger, more significant changes to be made, the team along with the OVAL Board and the larger community need to agree on OVAL Sandbox migration process. This was further discussed later during the call.

OVAL Interpreter

No major OVAL Interpreter updates have been made over the past quarter. As the 5.11 release process continues, the team will be implementing new tests and features where appropriate.

Sandbox Migration Process

Matt Hansbury discussed the team's plans for updating the Sandbox process by recapping an initial conversation that took place during July's Developer Days event. During the event, the group had a conversation about how to amend the Sandbox process to better facilitate moving changes from the Sandbox into the official Language. During the conversation, several suggestions were discussed and while the group agreed that the process needed adjustment, there was no clear agreement on exactly what that adjustment would look like.

The OVAL team took this feedback and based on it, Matt conveyed a proposal to move forward with updating the Sandbox process in this manner:

- Items that have been previously discussed at Developer Days with a general positive consensus would be posted to the oval-developer-list with a short comment period and then (assuming continued consensus) be moved into the Language.

- Items previously discussed, but without clear consensus would be posted to the oval-developer-list, but with longer comment periods to achieve consensus.
- Items previously discussed with a clear consensus against addition would also be posted to the oval-developer-list as items that will not be moved over at this time.

The Board members had some additional feedback on this topic. In general, the Board felt that in order for this to work, they should be empowered to vote on all of the significant changes to the Language. Several members shared their opinions that with significant time and financial investments into OVAL, it was important that the Board members have some say in what things belong or do not belong in the official Language.

After some additional discussion about the specific types of changes that would be voted on by the Board, the OVAL team conceded that it was reasonable to empower the Board members with a say on what gets into the Language early in the process. The team had always intended on putting the final approval of a new version of the Language to a Board vote, but it was rightly pointed out that by then it really was too late to affect significant change.

The group agreed that Sandbox items that made significant changes (that is, excluding things like documentation updates that do not change functionality, typos, minor updates to things like enumerations, and adding additional entities) would be collected periodically after some community discussion and rolled up into a Board vote. Things with clear positive consensus would be migrated into the Language, things with clear negative consensus would remain in the Sandbox, and things with no clear result would be further discussed. Lastly, introducing a dependency on a series of Board votes means that the not yet finalized Board Voting policy must be resolved before any further significant 5.11 progress could be made. The following section discussed that topic.

OVAL Board Voting Process

Next, Dan reviewed with the Board the status of the Board Roles & Responsibilities document, the Board Member Processes document, and the Board Voting Process document. Over the past few months, the OVAL team has been working with the Board to finalize these documents. At this point, only a couple of remaining issues need resolution before they can be finalized.

The first issue is how to handle corrected votes. As each organization is to receive a single vote (despite an organization potentially having up to 2 members) there has been concern about how an organization would handle this situation. In order to ensure that each organization is the result of thoughtful consideration, the policy will be that an organization's vote will only be changed if the Board explicitly agrees to allow it. The idea is to make this an exceptional case, and not a common one.

During this conversation, the question of how to handle non-official extensions to the Language came up. This topic involves things that do not achieve consensus to migrate into the official Language, but may be important to some organizations. Organizations could choose to still support these un-official extensions and a way of dealing with them is required. Matt Hansbury pointed out that the best solution for this would likely be to introduce a way to separate the Core part of the Language from the

platform extensions. By separating these, an official Language could be constructed of specific platform extensions (along with a version of the Core) and thus make un-official extensions more easily identified.

The other issue that was discussed is how what is voted on is determined. Dan made it clear that the OVAL team could not allow votes on items that would require the team to operate outside of the current scope of the sponsored project. The group accepted that this makes sense and generally agreed on the current wording around this topic.

The consensus was to move forward with the most recent version of the documents as final, with the idea that they could be revised as needed. The MITRE team is now able to move forward with the updated Sandbox process, which will achieve the goal of migrating mature items out of the Sandbox and into the official 5.11 Language.

Finally, it was also reiterated that the Board members themselves certainly could take on tasks that did not directly fall into the sponsored tasking of the MITRE team, thus allowing the Board to accomplish things that they deemed important. The OVAL team agreed that this could be something that helps move forward things that fall outside of the team's project scope.

Action Items

- MITRE team to send an email to the oval-developer-list to capture and announce the updated Sandbox policy agreed upon in this call.
- MITRE team to propose a way to separate the Core of the Language from the platform extensions.