OVAL Board Meeting (4/13/2015)

Attendees

Blake Frantz – Center for Internet Security
Adam Montville – SACM
David Solin – jOVAL.org
Tigran Gevorgyan – Qualys, Inc.
Scott Armstrong – INADEV Corporation
Randy Taylor – ThreatGuard, Inc.
Kent Landfield – Intel Corporation
William Munyan – Center for Internet Security
Jamie Cromer – Symantec Corporation
Amaresh Shirsat – Symantec Corporation

Matt Hansbury – MITRE
Danny Haynes – MITRE
Mike Cokus – MITRE

Meeting Summary

Welcome

The Board members were welcomed to the 2nd Quarter OVAL Board call.

Discussion

Dan Haynes began the call with an update on the OVAL 5.11.1 release. More changes were required to finalize the release than first anticipated. These included corrections to the use of namespaces to support the separate versioning policy, fixes to Schematron rules, and updates to the Cisco schemas among other changes. A complete list of changes can be found here[1]. The release should now be ready to publish.

Matt Hansbury then gave an update on the OVAL Repository. At the time of the call, the OVAL Repository contained 25,287 OVAL Definitions. The 1st Quarter Top Contributors were Hewlett Packard, Altex-Soft, and SecPod Technologies.

Next, Dan Haynes gave a quick update on the whitepaper mapping OVAL to the SACM Information Model as part of the transition update. It was noted that the updated version would be sent out to the oval-board-list very soon. One OVAL Board member asked if there was a specific timeframe for when the updated version would be available. Matt Hansbury explained how the updated version would be sent out to the OVAL Board early next week.

---

[1] https://github.com/OVALProject/Language/wiki/Changelog

Adam Montville provided an update on IETF Security Automation & Continuous Monitoring (SACM) Working Group activities. The group is currently discussing endpoint identification attributes, and the working group last call for the SACM architecture draft is expected in two weeks. The SACM Working Group is also working on a new set of milestones for future development.

Matt Hansbury then recapped the overall transition status for the Board. Over the course of the past few months, MITRE held several calls to discuss how best to transition OVAL. Matt talked first about the transition of the OVAL Language, noting that the Center for Internet Security (CIS) has shown interest in taking on the moderator role. During subsequent calls, what this would mean for OVAL was discussed, with CIS deciding that external funding would be required to take this one and with several Board member organizations showing some willingness to provide funding in some fashion. That conversation continues still, with MITRE providing information to the Board and CIS as to how a more minimal approach could be accomplished to help drive down the funding requirements.

Matt then mentioned that CIS has also showed interest in hosting the OVAL Repository, and while conversation has occurred on the topic, it is currently on hold while the OVAL Language transition plan is finalized. Additionally, he mentioned that little action was currently being taken on the OVAL website and the OVAL Interpreter transitions, but that they will also need to be handled at some point. Finally, Matt noted that the DHS legal team was continuing to review the legal aspects to transition of any parts of OVAL.

The OVAL Board spent the majority of the meeting discussing the OVAL transition. Dan Haynes led a review of the updated spreadsheet documenting the expected level of effort involved with maintaining OVAL after its transition. Two versions of the spreadsheet have been presented to the OVAL Board. The first version gave the approximate level of effort that MITRE expends currently for the various moderator activities, while the second presented a minimalist version of the effort required to keep OVAL alive. The minimal effort version emphasized that while many tasks that MITRE now does would need to be scaled back or ceased, with a reasonably small amount of effort, the truly critical activities could be achieved. The success of the plan is predicated on the continued involvement of the OVAL Community and primary source vendors.

The reason for the reduced moderator effort is that it is expected that the OVAL Community will take on most of the responsibilities which were handled by MITRE in the past. Historically, MITRE would step up to handle gaps no one else in the community was addressing, and the minimalist approach does not include these kinds of tasks. MITRE has been disengaging from these duties as the community has stepped up to take on more responsibility and the expectation for the future is that community members would be completely responsible for developing, testing, and advocating detailed change proposals. In addition, it is expected that community members who anticipate making frequent proposals would be given submission privileges to reduce the amount of direct action required from the moderator.

One Board member asked if the Board believed the Developer Days events were valuable or if they could be discontinued. A couple of Board members explained that the events were valuable, but, there

were lots of opportunities to lessen the cost and time burden associated with them. Specifically, the events could simply be virtual events rather than face-to-face. A similar question was asked about the OVAL Adoption Program. A couple Board members explained how it was more of a nice to have and probably not critical to the success of OVAL. It was also noted that the OVAL Adoption Program, and other nice to have items, will come back up if it turns out they are really needed at which point they can be reconsidered. Another OVAL Board member explained how they see OVAL becoming more of a federated effort moving forward where vendors will need to bring the changes, that they need, to the OVAL Community and move them towards acceptance rather than MITRE being responsible for it.

One Board member noted the importance of taking more practical steps to realizing the OVAL transition given that we are nearing the July deadline. With this in mind, the Board member proposed that CIS develop an updated proposal of the minimalist tasks which they are willing to take on and the associated cost. The Board member also proposed that MITRE review the updated CIS proposal to identify essential activities which would not be addressed. The group agreed with the proposal and CIS and MITRE agreed to take on the respective actions.

Finally, one Board member requested a discussion about MITRE's expected role in SACM so that the OVAL Board could align their efforts with MITRE's activities. MITRE agreed to coordinate with DHS to discuss this topic at a future OVAL Board meeting.

Actions

1. CIS to update their proposal to sustain OVAL, based on the "minimalist" level of effort which MITRE has documented in the updated spreadsheet.
2. MITRE to review the CIS proposal to identify which essential activities are not covered by the CIS proposal.
3. Intel and CIS to coordinate a face-to-face meeting at next week's RSA Conference to further discuss the OVAL transition.
4. MITRE to discuss direction and its role in SACM with DHS.
5. MITRE to schedule a follow up meeting in 2 weeks. (27 April).