OVAL Board Meeting (5/18/2015)

Attendees

Blake Frantz – Center for Internet Security
Adam Montville – SACM
Kent Landfield – Intel Corporation
Randy Taylor – ThreatGuard, Inc.
Steven Piliero – Unified Compliance
Steve Grubb – Red Hat, Inc.
Tigran Gevorgyan, Qualys, Inc.

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

Guest Attendee

David Ries – Joval Continuous Monitoring

Meeting Summary

Welcome

The Board members were welcomed to this follow up conversation on the topic of an OVAL transition. The purpose of this call was to provide an overview of a draft of a more resource-oriented OVAL moderator transition plan from David Ries of Joval Continuous Monitoring. Additionally, Adam Montville gave a short IETF SACM update.

Discussion

SACM Update

Adam Montville began the meeting with a short update on last week's virtual interim IETF SACM Working Group meeting. He noted that Matt Hansbury gave a short introduction to the OVAL/SACM paper that was recently submitted. He also pointed out that the Requirements document was approaching working group last call and is nearly complete and that the Endpoint Identification Design team was nearly prepared to offer updates to the Information Model document based on their findings. Finally, he called out to the OVAL Board to show participation in the Working Group, especially where OVAL was involved.

Resource-based Moderation Proposal

David Ries of Joval Continuous Monitoring discussed the draft document he put together with help from the folks from the Center for Internet Security (CIS). The overall idea is to provide structure to a model for OVAL moderation that leaned heavily on community resources, as opposed to funding CIS to

exclusively moderate the OVAL Language itself. CIS would remain the main organization responsible for OVAL, but would use resources from the community to do things like schema development, review, documentation, etc. Heavy usage of GitHub and mailing lists would allow for a light footprint and collaboration.

David noted that this is a draft and, as such, is a work in progress. He asked for those on the Board to assist in reviewing the document (which was posted to the oval-board-list on the morning of this call) to achieve a consensus on this backup plan to CIS taking on the entire OVAL moderation by itself.

Discussion of the document and the ideas therein occurred following David's introduction. One Board member believed that the best path for success would be to extend the existing CIS subscription model, noting that while his company would have difficulty in donating funds outright, a new or increased, existing fee for CIS subscription would be doable. Several other members countered that money is challenging regardless of type and that putting resources towards the effort remains the more likely path for them. Blake of CIS noted that while CIS has thought about how to structure their subscription fees in general, he has viewed the OVAL funding option as something separate to avoid the appearance of putting OVAL behind a "paywall". One Board member asked if we heard back from DHS about funding. Matt explained that we haven't, but, that we will follow up with them.

Other members asked whether assigning a specific leader per platform extension would be a feasible plan. In general, the consensus of the group was that David's plan was a good and reasonable starting point, though all believe that more discussion and revision is required. Members agreed to continue this discussion over the mailing lists in order to facilitate progress. Many suggested that a hybrid approach of allowing willing primary source vendors take on more responsibility, along with continued support for 3rd party security researchers for those platforms without a participating primary source vendor might work. This would still require some, limited, centralized moderation, but would be limited to essential roles only, such moderation of GitHub sites, ensuring resources like email lists and basic web site presence, etc.

The topic of the OVAL Repository came up, with members asking for an update on what will happen with it. Blake mentioned that he believes that CIS will take on the Repository without any additional funds. Conversations on how best to implement this are ongoing, ranging from options like simply taking on the MITRE tools as they are today, to implementing a GitHub-based solution. More details will soon be made available.

Finally the group agreed that a follow up all should take place in two weeks and that during the interim time, conversation over the list should occur to discuss the proposal from David.

Actions

1. MITRE to schedule a follow up Board call for the week of 6/1.
2. MITRE to begin to identify potential leaders for each of the platforms of the OVAL Language to gauge interest and feasibility in assigning one to each platform. MITRE to informally reach out to potential leaders to gauge interest in participation.

3. All Board members to review David Ries' proposal and comment where appropriate over the mailing list.