20190805 - Endpoint Data Collection Telecon

Attendees: Chris Argenio (MITRE), Charles Schmidt (MITRE), Jess Fitzgerald-McKay (NSA), Adam Montville (CIS), Bill Munyan (CIS), David Solin (Joval), Thomas Henry (??), Phil White (CIS)

This is the second quick sync-up call of the Endpoint Data Collection group to see where things stand and what the next steps are. Jessica started by confirming that everyone had read the Scoping and Work Goals document for SCAP 2.0 Endpoint Data Collection and asked if anyone had any edits to add or if it was ok to release as is.

Bill Munyan - Is there is a format in which these work goals will be achieved? What’s the definition of “done” for some of the bullets like Characterization, Normalization, and things like that?

Jess – You’re thinking if we could get down to a description of what items we’ll produce?

Bill M. – Yes. I have no issues with the four bullets just wondering what would be considered achieving the goals.

Jess – I’d be happy to do a capture of workgroup items either in this document or in a separate one this document could point to. Any suggestions or thoughts?

David Solin – Bill, do you want to say we’re done when we have a reference implementation? Seems ambitious for a charter.

Bill M. – It is ambitious. I guess a draft of what the capabilities entail and if it’s a specification? It doesn’t really need to go as far as a reference implementation.

Jess – Reference implementation may be too much.

David – Let’s start with a goal in identifying specification.

Jess – We don’t need to solve this problem now but let’s get a GitHub. As we talk through these goals we can capture and track there. Bill, do you want us to add words to our scope saying the workgroup will identify work items and capture them in a document that’s not this one?

Bill – Yes.

**Jess will take action to do that. Will edit in the GitHub site and email group asking for final questions.**

Jess - The reason why I want to get that document sorted is because there is a face-to-face coming up in September and I was hoping to have something to share there: this document in particular and what our next steps are. We met with NIST, MITRE, and DHS and spent time developing an agenda for the face-to-face. Looks like NIST wants read outs from each workgroup – what’s done, what people are working on, what do we plan to do. We’ll have to identify who is best to share the reports to the group. Any volunteers?

Bill – I’m not sure any CIS people are going to be able to attend due to different conferences. Adam will not be attending. David Solin said he will attend but thinks it’s lame if no one else is there.

Chris Argenio gave agenda details for the three days.

Jess – David and I can collaborate offline for presentation.

David S. – It would be nice to have more than just the charter and scope. What can we do between now and then?

Jess – Bill, Adam, and I met at the IETF meeting and spent time chatting of what to produce. I took an action to pull out data specific to Endpoint Data Collection prior work. It’s a useful starting point. We could use this to iterate in advance of the face-to-face.

David S. – Sounds good. Post it on the GitHub site.

Bill M. – I’ll post it and will leave comments in.

Jess asked to keep it a work in progress, beat it up, rip it apart, add what you want, etc. Jess mentioned that **MITRE should schedule another Endpoint Data Collection telecon in two weeks** (8/19). <Jess left conversation>

Bill M. – Right now, it’s a word document. If you attended a number of the previous calls with some intros to SCAP 2.0, it involves similar ideas that are on a few of the slides but focused on the ones that are specific to data collection. It’s focused on what are the components that make up the section of the architecture that are dealing with Endpoint Data Collection, the responsibilities of posture collection service and relationships to other components. Collaborating on a document on GitHub might not be the best but if there’s a way to get this into a different format for ease of collaboration, I’m willing to get this document in a format that’s better to use for collaboration.

David S. – Looking at the doc would be a good start, but it could get clunky with major changes.

Bill M. - We can change format and use issues to move forward with merging changes.

David S. – If this is all SCAP 2.0, let’s rip out everything not Data Collection. Then make sure it gets modified that it encompasses concepts we’ve discussed. Then anything else we’ve decided to do.

Bill M. – The document has ideas behind a posture collection service. Ideas behind that service would be good to discuss – establishing and managing secure connections, etc. I think there’s terminology to iron out (service vs server). It discusses the two components - endpoint and Posture Collection Service.

David – Sounds like a good place to start. Let’s start with someone else's document – easier than starting from scratch. Get that up there and we can discuss over email list and schedule a meeting for two weeks from now. (8/19)

Bill – Document is a good base draft to go off of. If there are requirements we can put in, that would help.

David – Sounds good. I’ll read the document and other people should, then we can start a conversation. I’d say we can be productive without being on the phone. Email is fine until the two week call. Still gives us a month before the meeting. We can increase meeting frequency if we feel we have to.

Bill – I’ll shoot email about document when it is uploaded in GitHub.