Common Security Advisory Framework (CSAF) TC Working Session
Meeting Date: April 10, 2019
Time: 1:00 pm US EDT

---

1. Call to Order and Welcome

Meeting called to order @ 1:05 PM US EDT

2. Participants

2.1.1 Members Present

Company	Name	Role
Cisco Systems	Mike Gorski	Member
TIBCO Software Inc.	Eric Johnson	Voting Member
Cisco Systems	Rhonda Levy	Voting Member
TIBCO Software Inc.	Denny Page	Voting Member
Cisco Systems	Omar Santos	Chair
FireEye, Inc.	Jared Semrau	Voting Member

5. Meeting Notes

- Omar—
    - Two updates:
        - Will share notes after the meeting.
        - Updates from Oasis – Went back to Carol from Oasis and discussed maintenance charter. The answer was No, we do not need one. After deliverable, the final TC is closed or goes into maintenance mode. In most cases, being in maintenance is like closing a TC. Continue to be open to participation. Status is maintenance mode after final product. Will be externally viewable. Like CVRS, if not doing a maintenance standard then a different situation.
    - Suggestion – GITHUB. We know we want the final deliverable that currently supports one to two items, can work on things in parallel. Created google drive folder and doc in CVRF and edited draft; one, to make sure we cover everything and two, strong schema can document that they are there for collaboration purposes.
        - Eric - likes this and maybe use a markdown function approach. Has a concern regarding procedural point building in google versus Oasis. Should get repositories and we must approve a contribution.
          Formal process, like Stephen, conversion to their template. Omar agrees.
        - Omar - access control – has seen good and bad examples. Open C2, open edit mode, public stuff could be messed up. Must have a way to define a core team with edit capabilities to streamline some of the work.
            - Reviewing current schema, putting a map CVRF 1.2, CVSS score_set, about to open 3.0 for comments, which are expected in a couple of

years to be outdated. But everything now supports 3.0. We should think about how to represent it?

- Eric - XML and JSON are significant. In content to JSON, CVFS score_set 3.1. is unlike XML schema, and the schema will be rejected. Unless you specifically tell JSON schema, you must reject V4 or V5 etc., and it will be fine. Recommend that future users of this V3 or V3.1 use this naming convention. If in maintenance mode, can put in schema. Upside to JSON is you can just add and extend.
- Omar - agrees, do a score_set version. If 10.4 is not there, you don't have to define V3, etc.
- Eric - version JSON schema values can point to a specific version with a new property and it is done. Very easy.
- Omar - it is solid. Will have to define what it is, what functionality, and what is supports right now is a good starting point. Ok to put in document?
- Eric – said fine.
    - Existing schema limited around the products. It describes the product tree but does not make sense of the schema. Eric wanted to look at that.
    - Written some code to parse a CVRF doc to write out as JSON, and deal with vulnerabilities and doc metadata but no product tree. Want to parse product tree and put in JSON format and put in 1.2 in JSON format. A little bit of work. Roughly correct but want to validate it.
    - The biggest challenges are the limitations of JSON schema that XML does ok with. We can use key/keyraf, post schema logic to ensure that a document is valid and conforms to the schema. With a product references to an id, is the area that will look at.
- Omar – brought up an idea of creating code to translate from 1.1. to 1.2 format. Mike (a Cisco developer) opened a request from PSIRT and is doing this right now when converting Red Hat to TVC, into JSON format.
- Mike – is not sure about this. Will try to get other guys on the team to collaborate to do the same thing. We are now consuming docs from Microsoft to JSON and we are close.
- **Omar - next steps – will put document in Google drive. Will construct now.**
- Eric - ok with this but not the product tree. Otherwise the doc is where we want it to be.
- Omar - Commit to documentation, if we break the ice others will follow. When we formulize to the document, not the editor, but someone else will be assigned to do this. Once it is defined then we will complete the updates to the document.
- Eric - did we do this with existing schema? JSON does allow for documentation and examples. Might be productive to document from the schema itself. Might be a very useful thing to do. We can indicate the additional things that need to be validated. Did not go down that path,

because they might change. In retrospect wrong call, would have been ok with example fresh in brain. Might want to put schema documentation and then parcel out the work.

- Omar - will have to convert to Oasis standard format. But will be easier.
- Eric - take doc from schema put in XTL format and paste into document. More work but it makes it automatic. To generate Oasis material, involves three components: XML, vulnerability product tree and schema; they have different document structures and we don't want to maintain the different structures.
- Omar - good point. Main new case, CVE record supports 90% of notes, extra references, versions and is in the bundle of security info. If there is a vulnerability we will have specific notes.
- Omar – regarding schema from CV group, if it a good example to model from we will work with that.
- **Eric – will send and introduce some internal schema documentation and a pull request along.** Straight forward. **Write up some sample or actual document for metadata.**

6. Next Meeting

Next Meeting will be a **monthly meeting** on Wednesday, April 24, 2019 at 1:00 PM US EDT

7. Adjourn

The meeting was adjourned at 1:55 PM US EDT.