Common Security Advisory Framework (CSAF) TC Working Session
Meeting Date: August 14, 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

<table>
<thead>
<tr>
<th>Company</th>
<th>Name</th>
<th>Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco Systems</td>
<td>Rhonda Levy</td>
<td>Voting Member</td>
</tr>
<tr>
<td>Cisco Systems</td>
<td>Omar Santos</td>
<td>Chair</td>
</tr>
<tr>
<td>Tibco Software</td>
<td>Eric Johnson</td>
<td>Voting Member</td>
</tr>
<tr>
<td>FireEye, Inc</td>
<td>Paul Patrick</td>
<td>Voting Member</td>
</tr>
</tbody>
</table>

5. Meeting Notes

- **Omar** —
  - Did not get any new feedback in the last 2 weeks ago regarding GitHub issues. Will remind people after the call.
  - Will need help with documentation for initial release. Oasis will be helping and monitoring and looking at meeting notes. They have volunteered to help too. It is what it is.
  - Regarding issues from GitHub, close on two items and don’t expect disagreements. Will help with edits. Looking for volunteers to document release. It’s not changing dramatically.

- **Eric** —
  - Progress made on implementation of parsing CVRF to generic model to JSON. Mapping to JSON - no working implementation yet; however, have started it.
  - CVRF data modeling for JSON should be simple. Will have a working version of CVRF lead into JSON to read back and then back to CVRF.
  - By next TC meeting will demo it.
  - Will show test cases that verify a round trip CVRF. All validation code is in place. Must have non-empty descriptions. Have all in place but have not tested yet.
  - JSON piece of it is something that can be demonstrated and expect to do this week.
  - To test this – will output JSON and run through JSON schema validator. If it works that’s a test case that passes.
  - Multiple implementation cases (will go through XML schema line by line) and to look at all aspects of CVRF. Will get a sample document that has everything to import and get byte-by-byte match.
  - Goal is that will get a full match with JSON and 150 lines of XML.
• Worked with legal and will have the correct license. Will do very quickly. Hope to have open source for people to look at by next meeting.

• Omar shared:
  o A tool that can be used to visualize and navigate through the schema
  o The tool is now available at: https://json.csaf.io/

• Eric –
  o 2 or 3 gotcha things.
  o Schema things due any day now? JSONschema.org in final review – will publish draft during August timeframe. Guessing to see it land in late August.
  o Potential risks? Draft of schema tools can be harder to adopt.
  o One other area, because implemented JSON format, may discover something along the way – i.e., time values? Also, some short cuts for consumable to mark down tool. Might make updates to tooling for better documentation.
  o Another thing that’s occurred to Eric, from a validation point of view, might want to generate 2 schema definitions: one strict to disallow extensions, and a not-strict to allow extensions. Should be the only properties allowed there. Properties must be there, and again the only properties allowed.
  o For compatibilities, allow only things are pre-defined “XYZ.” From that last schema, would be what you can allow / expect, and you can add an attribute; something to a note for example. For testing an instance of something, must make sure it conforms to schema but nothing extra. May be a typo not a feature? To support that what does it look like? Build a schema that allows restrictions defined and generate the last version. Strip out restriction clause. What we might want to do to properly to comply with extensions.

• Omar – validator – thinking about type of module – GO has validation logic. Wrote some for every constraint to make product ID to product. Key ref values, no empty stream. Lax versus strict. Only these properties.

• Omar – makes sense – extensive – relaxed schema.

• Eric – for purposes of enabling tools that are compliant can use JSON strict versus lax schema. Something complies to strict can round trip document, lax schema may drop Cisco or Red Hat properties and would have a different document.

• Omar may have elements from other companies so interesting ideas. Implementation that Eric is doing is the impact for new release this week.

• Eric –
  o When mapping stuff to memory of CVRF stuff, product and properties on product would map differently to JSON.

• Omar – implementation very inconsistent with how to use it with examples in Red Hat. Don’t have something to represent products in industry. Kind of a “Wild Wild West.” Need an association with the product, in some standing way, then we can leverage that.

• Eric sees plenty of CVRF installed on Red Hat and vice versa.
• Omar – impacted by Red Hat or Linux we would collect the negatives. Would not be covered by CVRF? Don’t think product tree is flawed – just would structure differently for JSON.

6. Next Meeting
Next Meeting will be **OASIS CSAF TC Monthly Meeting on Wednesday, August 28th, 2019 at 1:00 PM US EDT**