OASIS Common Security Advisory Framework (CSAF) TC Meeting #18 August 29, 2018

Chair: Omar Santos

Attendees:

Beth Pumo
Dan Choland
Denny Page
Eric Betts
Eric Johnson
Jamison Day
Jared Semrau
Jonathan Bitle
Langley Rock
Mike Gorski
Paul Patrick
Rhonda Levy
Troy Fridley
Vincent Danen
Beth Pumo
Omar Santos

1. Call to Order and Welcome

Meeting called to order @ 13:05 PM EST (17:05 UTC).

2. Roll call

All participants recorded their attendance on the OASIS meeting calendar
- **quorum** was reached.

All participants were kindly encouraged to register themselves to optimize the use of the shared time during the meeting in one of two ways:

Either click the link with the text "Register my attendance" on the top of the event page or directly visit the per event direct "record my attendance link":
https://www.oasis-

open.org/apps/org/workgroup/csaf/record_my_attendance.php?event_id=46223&confirmed=1

2.1 Participants

2.1.1 Voting Members Present

- Jonathan Bitle, Kaiser Permanente
- Vincent Danen, Red Hat
- Jamison Day, LookingGlass
- Troy Fridley, Cisco
- Eric Johnson, TIBCO Software Inc.
- Denny Page, TIBCO Software Inc.
- Paul Patrick, FireEye
- Jared Semrau, FireEye
- Beth Pumo, Kaiser Permanente
- Omar Santos, Cisco

2.1.2 Members Present

- Mike Gorski, Cisco

2.1.3 Observers present

Note: Observers of this committee that are ready to become Members should follow the specific instructions displayed the OASIS Open Notices tab.

- None

2.2 Voting Right Changes Effective After the Meeting

2.2.1 Members who gained Voting Rights

- None

2.2.2 Members who lost Voting Rights

- None

3. Approval of Agenda

- After a review and brief discussion of the proposed agenda, XXXXX motioned for the agenda below to be approved. Seconded by XXXX. Motion passes by unanimous agreement. Approved agenda with no modifications.

Agenda approved.

4. Approval of Minutes from Previous Meetings

- Meeting minutes for CSAF TC Monthly meeting #17 approved. XXXXX moved to approve the meeting minutes of meeting #17 XXXX seconds. Unanimous consent, the motion carries, meeting minutes approved unchanged as published.

https://www.oasis-open.org/apps/org/workgroup/csaf/download.php/63332/Minutes%20of%202018-06-27%20Meeting#17.html

No meeting in July to approve.

Move to minutes Eric Johnson and Troy Fridley approved.

5. CSAF 2.0 JSON Schema Update

- Finish the discussion Localization support in schema and items discussed by Eric and the TC at: https://lists.oasis-open.org/archives/csaf/201806/msg00002.html

- Enhancement of Generic Software Identification Parameter/Attribute to be included in CSAF 2.0 schema
    - This will allow us to support CPE, SWID, or any other future nomenclature /standards.
    - Omar: After initiatives from NCIA – more items will evolve.

- **Vincent from Red Hat moved to approve this.**
- **Eric Johnson seconds**

Omar –

The topic for today is related to localization and translation; the tools that Cisco and TETCO use to translate data to machine readable language. Did Eric get feedback from 5 weeks ago regarding communications?

Eric J—

Just the same as everyone per mailing list.

At what point where we can move forward? Since this is an informational meeting only, the globalization team can discuss right approach.

The surprising thing is that the global team is working with what other companies are trying to do. Translation of documents: translate fields and keep original document in its original state.

JSON documents, determines what needs to be translated and runs it through the system. They have their own data model for translations. It amounts to an alignment regarding standardizations.

We need to have design discussions and then make implementation utilities. The goal is to have multiple languages for the same document. Recommends separate documents per original document, allowing separate local representation versus CSAT.

Omar –

Original translation would need to have a base language and have a field that indicates what that language that is. If it is only a single language then that should be indicated as well, just once at the top of the document. Localization versus CSAF Global information content.

Eric J –

Does anyone have concerns or objections about having a single translation?

Paul –

Asked if anyone else was addressing it.

Eric J –

Did not see how it fit with how they work, aligned industry practice JSON data that is. Came away with the impression that it is not a good fit for what we need with CSAT.

Paul —

We do not have a globalization group?
And agrees that we should have it translated without having it modified.

Eric J –

Yes, agrees one language and then have it translated. Could be a future problem regarding space, as roll up might include other languages. Document should represent a single language / object and then translate that. Important detail. Object includes original language. Agrees with Omar, indicate in a field that it was translated from "English" or whatever language; and then French version, second, etc., so you know to go back to the original. Translation flag of some sort.

One language per CSERT doc and then copies in other languages? Could have problem. What does a # hash mean? Same document – with a few bytes different? Maybe it's not an issue? Not experienced with JSON Data. On a document basis, take input data, and copy of both the original and translated copy. The copy can detect and recopy the data. They can note if it is different from the last time they looked through the document. Localization team would not care, and just look at it. If they are different, they can regenerate, change other fields, and produce output. Byte for byte identical is what's important; but the # meaning is important too. A more concrete base cannot point at something without including changes in copies. There are no mechanisms in place to enforce doing this.
Not sure how we would include # well. Signatures as well will have origin issues.

Vincent –

Hash in document is nice and it would be a good idea to not invent a process that someone already has a process in place to account for it.

Eric –

Propose a motion: CSAF 2.0 JSON representation, identify a single language per document and a translation for another document. Should adopt a language per document and have a field in the translated document indicating what language the document was originally translated from.

Denny seconded.
Motion passed.

Omar –

Open table for discussion of CPE and SWID or any other future nomenclature/standard.

Vincent –

Too many ideas. Too many revisions later. Attribute and then field, software identifier, and then contents, then translate to JSON. Instead of support for multiple fields, just add new content to it.

Eric –

Is all for clarity. Can identify a CPE and SWID property in the right place and then define and syntax them. Define at least one? Require that? We don't want the hurdle to use it because we would have to fully document supporting document?

The product tree in a CSAF document has a communication of products, can replace CPES and SWIDs; however, we may not communicate what is being used now. If we use what we have now, we can use those pieces of information and they may not align – as info is in two different places.

Include identifiers, it's a trivial thing to do, from an information model concern in CSAF. It's useful with a full product name and shows where they come from. That info may not be in the CPEs and SWIDs. We will need to have a plan on how to address them.

Omar agrees –

Maybe have a product ID as optional using a nomenclature standard.

Omar asked is it possible for CP attribute, name pattern, in the case of a SWID identifier attribute. SPVS – how is that represented? JSON?

Eric –

Said yes they have an identifier. Yes a random GUID or something.

Omar –

It must have an URL to associate the vulnerabilities in them.

Eric J –

An identifier should be mapped to human readable information. So this is an issue. The goal is for some of the mapping to exist, and the SPVS team is aware of this problem and they are going to have to come up with a solution. Not a generic solvable problem. We can validate the given reference to SWID or CPE but not if it refers to an actual document or something else.

Vincent –

Perhaps we can validate from a disk file or a collection of SWID tags, and specify a free form tool to determine how to process information.

Eric –

We can use a CPE key with an object structure with a CPE identifier and reference; a URL, template or something. SWID too. Get to a page that defines what is there.

Vincent –

Will have to have the standard to be flexible to point to documents that are shipped with it, computer, store, etc., and try to not put ourselves in bowls that we have to engineer out of.

Action: owner Troy Fridley – requested from Omar –

Would you mind summarizing this and we can review in the next meeting? Then we can make motions at the next meeting.

Troy said yes.

Eric –

Calls to adjourn meeting

Vincent - Seconds

8. Next steps

- Provide additional feedback on the current draft schema
- Suggest addition of generic software identification standard support instead of SWID, CPE, SPDX, etc.

10. Next Meetings

10.1 Next Meeting

- Next Meeting #20 will be on Wednesday, October 31, 2018 - 01:00pm to 02:00pm ET (i.e. 2018-03-28 19:00 to 20:00 CET (UTC+1)).
- Event page: https://www.oasis-open.org/apps/org/workgroup/csaf/event.php?event_id=47736
- Self-Registration link (available from approx. 15 minutes before meeting start): https://www.oasis-open.org/apps/org/workgroup/csaf/record_my_attendance.php?event_id=47736&confirmed=1

4.2 Other Subsequent Meetings

- All meetings monthly on last Wednesday during: `01:00pm to 02:00pm ET - 19:00 to 20:00 CET (UTC+1)`

11. Any other business

No other business

12. Adjourn

The meeting was adjourned at 14:00 PM EST (19:00 PM UTC).