Common Security Advisory Framework (CSAF) TC Monthly Meeting
Meeting Date: March 27, 2019
Time: 1:00 pm US EDT

---

1. Call to Order and Welcome

Meeting called to order @ 1:05 PM US EDT

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:

- Clicking the link with the text "*Register my attendance*" on the top of the event page
- Or directly visiting the per event direct "*record my attendance link*"

2.1 Participants

2.1.1 Members Present

Company	Name	Role
Kaiser Permanente	Jonathan Bitle	Voting Member
Oracle	Feng Cao	Voting Member
Cisco Systems	Troy Fridley	Voting Member
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
FireEye, Inc.	Paul Patrick	Member
Kaiser Permanente	Beth Pumo	Voting Member
Cisco Systems	Louis Ronnau	Voting Member
Cisco Systems	Omar Santos	Chair
Tenable, Inc	Lucas Tamagna-Darr	Member
LookingGlass	Allan Thomson	Member

Note: Voting right changes effective after the meeting and it is automatically calculated by the Kavi OASIS tool.

2.1.2 Observers present

Carnegie Mellon University	Deana Shick	Observer

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

3. Approval of Agenda

Approved. Motioned by Eric and seconded by Troy. No modifications requested.

4. Approval of Minutes from Previous Meetings

Approved. Motioned by Eric and seconded by Troy. No modifications requested.

5. Meeting Notes

- Omar—
  - Noted that this is the first meeting with a quorum in 3 months.
  - Update of action items from last meeting: scheduling of ongoing meetings complete.
  - Art suggested, in the last meeting, that not a lot of changes schema etc., of CVRS for CSO; and made a motion to move to a maintenance mode. A lot of the dynamics have been more to assign to CV / JSON and there is an overlap. Therefore, maintenance mode was considered to push and convert to product integration.

- Allan – asked for an explanation of what that means.

- Omar – explained that in last month's meeting we were talking about the next version of CDEF, customers don't or do adopt; a Cisco vendor perceptive, scanners etc., top adopters. We have been going over what is the future of CDEF – since we are not seeing that MIDOR can create a JSON advisory. Omar will see Art next week and will follow up with him. He is not able to make this meeting today and we did not receive the email explaining his thoughts.

- Allan – MIDOR explanation makes sense. We submit in machine readable format and publish our CVES in that format.

- Troy – we use MIDOR and need and leverage it. We do not have a lot of choice here. To assess CVEs and to issue advisories you must use MIDOR format. Can we expand and make this better?

- Allan – is "maintenance" the right word? Sounds like no further development would be needed?

- Troy – idea was to convert MIDOR to CVRF, people do it and enjoy it. That format will expand and change, even in a maintenance mode.

- Eric – there is a gap from what CVRF and JSON format does. Two things:
    - One, is that the MIDOR data uses individual identifiers. Frequently we issue a lot of alerts to customers, not just one. Not related to MIDORs criteria of issues. Including a bunch of things and having them communicated together, is better than one by one. Sees a value in the future in including multiple events together. Event of the day. Not just 5 different things. CVRF is a good resource to think about that.
    - Two, CVRF and MIDOR – do not use the same format. Version ranges are different in MIDOR. Additional data is in CVRF and it is not in JSON format. Not easy to extend over time. If we do anything, we would include use cases, and it hasn't emerged. Maybe we would get that if we get the different representation in the group. Scanner people perhaps.

- Lucas – what CVE provides is to focus on a single advisory. Not more. CVRF whether it solves it or not -- it is a gap. There's a gap that needs to be filled.

- Eric – key issue and question, is maintenance work a direction for CVRF not emerging from use cases? This could take a long time. And an opportunity to define a JSON schema representation, as it currently exists; then we can maintain going forward and in JSON and HTML representation. If want to use CVRF to generate data, it's easier with JSON than HTML format. Might be beneficial in that regard. If there was a tool that takes JSON to CVRF, then that might be good. JSON is easier to use and process right now. No clear path other than doing maintenance.

- Troy – move from HTLM to JSON is good goal.

- Omar agree with everything that has been said. One comment regarding gaps, a format for CV assignment, cannot have multiple vulnerabilities. Not all vulnerabilities require taking action. There could be a machine-readable format issue for something requiring action but is not a vulnerability. The maintenance word may come into play.

- Omar – Since we have quorum we can take a motion to formalize our next steps. Allan is in favor of a maintenance mode. Allan moves to bring this group into maintenance mode.

- Feng – We do have gaps to get covered.

- Lucas – there are individual vulnerabilities, and some weaknesses or failures that don't warrant CVEs, when relevant.

- Feng – at the CVR/MIDOR summit, heard that some people don't want to use MIDOR anymore. They created working groups to work on CVEs.

- Allan – MIDOR is not going anywhere anytime soon.

- Allan – whether MIDOR goes away or not; or maintenance mode or not, or exist or not they are different questions. Will this group go into maintenance mode.

- Feng – wants this group and get involved and fill the gap.

- Denny – if going into maintenance mode, there should be no added next steps to evolve the standard.

- Eric – a general rule of order – does Oasis have a specific meaning for maintenance mode?

- Omar –
    - One, regarding the use and word of "maintenance mode," will check out with guys from Oasis.
    - Two, will try to clarify and document offline, and will go from there.
    - Allan – Good point. Allan is ok with that. This group will pause our work after finishing "TBD" and will have meetings until "TBD" time and then a monthly meeting at that time.

- Allan set forth the following motions:
    - Motion for this group to finish the effort of converting the existing CVRF 1.2 to JSON (calling it 2.0) with no additional use cases, features, or data other than what is required to convert CVRF 1.2 elements into JSON format.
    - Eric seconded the motion.
    - No objections. Motion has been approved and passed.
- Allan set forth the following second motion:
    - Motion to propose a statement of direction for the CSAF TC that will limit the work to maintaining the published artifact after CSAF 2.0 JSON format is available.
    - Denny Page seconded the motion.
    - No objections. Motion has been approved and passed.
- Eric suggested that someone should talk to someone at Oasis.
- **Omar to take the action: Omar will work with them, specifically will reach out to Robin on this**. Passes with group.

- Next steps, all agree that we need to convert to JSON format. If someone in org has an expert in JSON, please use them. We are close to needing them. Latest version available in GITHUB now.

- By next meeting we can see status of what's been done.

- Working session and monthly meetings have been setup through the end of the year.

6. Next Meeting

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

Event page: https://www.oasis-open.org/apps/org/workgroup/csaf/event.php?event_id=47738

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=47738&confirmed=1

Note: All monthly meetings take place on the last Wednesday of each month at 1:00 PM US EDT.

7. Adjourn

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