CACAO Technical Committee
Meeting Minutes

Date: 04 February 2020

Attendees

Allan Thomson
Andrew Storms
Anup Ghosh
Bret Jordan
Emily Ratliff
Frans Schippers
Jason Webb
Jim Merk
Jorge Aviles
Jyoti Verma
Karin Marr
Lior Kolnik
Mahbod Tavallaee
Marco Caselli
Michael Rosa
Paul Patrick
Rodger Frank
Shawn Riley
Vasileios Mavroeidis
Tim Zhan

Agenda:

1. Review the working drafts
2. Discuss next steps for working drafts
3. Review playbook graphics
4. Review notional logic concepts

Meeting Notes

Bret: All info about CACAO is included in the cover page doc. They updated the requirements doc and use cases doc based on the comments and added explanation text. They are uploaded in Kavi

Bret asked for feedback, if there are any changes we can release a new committee draft.

Allan: This is our understanding of the CACAO requirements, what orchestration entails and move forward on working these requirements.

Bret: Review the docs (make comments) - it is important to create and approve a ballot so we can start working on the actual specifications. Find them from the Cover Page doc or in Kavi (they are uploaded).

Bret: explained the difference between committee notes and specification docs
Allan: There will be a motion at the next meeting in two weeks, so all voting members should review the documents.

Bret: the documents are not very long. You should be able to review them quickly.

Bret reviewed the example and the graphics that represent the example. Johns Hopkins builds these graphics using BPMN based tooling.

Anup: Example is useful and productive. Would like to see how it goes into the next phase.

Bret: Plans to add the next phase.

Bret went through his cacao example defined in json

Different types of playbooks investigative, preventative, mitigative etc.

Visual Playbooks (examples)

- Preventative playbook: receive IOC and update your defense tools (steps/methodology)
- Investigative- receive IOC - yes i want to mitigate something but this playbook will also check if i have this IOC in my infrastructure. It includes decision logic and actions.

The visual examples are included in the call's slide deck

Anup: Goal is to represent these examples in a vendor independent language that can be exchanged...

How do we declare all these in a common language / vendor independent / anybody can consume (absorb)

Allan: A standard that is usable in an actual product / progress for the industry / concrete implementations. Vendor neutral and independent. This is the reason we have the requirements doc to be able to define everything in an implementable way

Anup: We have examples of playbooks
Most of us work with tools / hive open source/ But also commercial from palo alto and splunk/phantom

Allan: WE reached the hive people to try to get them involved
We do have TC members working in some of those orchestration platforms. Product dependencies

Allan: Not only the platforms that create the orchestration but also the tools that receive the orchestration need to be interoperable. When we have some work produced all the aforementioned companies and more will start contributing.

Anup: Market place (free or commercial) for playbooks - to create and publish playbooks that are signed
Allan: We need to develop something that can be implemented, we are thinking about the broader requirements based on multiple vendor products.

Bret: Demisto round table at RSA
Phantom has participated in the past in other work

Bret: Cisco and IBM has considerable amount of work related to playbooks and orchestration

Bret: Many companies that want to enter this market and enable this capability
Open standard that can be hooked into CTI
Also critical infrastructure

Bret: If anybody has diagrams/playbooks please share them with the TC

Bret: cacao playbook specification 00 proposal 2: bret elaborates

We are working on the Temporal and control logic. We are not sure yet what's the best way of defining conditional logic, its work in progress. We want to keep the actual actions separate from the actual conditional logic. This is not a formal proposal, there are two proposals on the table. We have defined data types.

There are slight differences - number 2 is copied from 1 with small differences (text is almost identical) such as how they propose control flow and actions, some differences in naming conventions

Allan: Proposal 1
Action steps flow - control logic
Action model

Allan explained his example (reference Section 5.1.1 actions steps and action model in draft cacao playbook specification 00 proposal 1)

Allan: Fairly similar approaches, tc needs to check them both and say if they agree or not. If somebody has another idea of how to define those things in a better way please write a new proposal or comment. Please check both.

Requirements from Version 1 and the proposals can actually address them.

Lior - Palo Alto: How does it match our existing model and to see the effort that it would need to integrate in our products

- What do we expect from vendors and what kind of resources we can provide them to support them in integrating what we create. At the management level to support and prioritize this effort.

Allan: Standards can help us all, cacao will help us with playbook orchestration

Bret: They can all hook together from a threat intelligence point of view (cti and playbook integration)
Bret: We have talked to People and are very excited especially in the operational side, tie the playbooks with CTI and share them (Enisa and FIRST)

The 2 different ideas for playbooks are going to be merged in the future

AI: Review the documents, start looking at control logic
Bret: Prepare for the motion - read the documents

Bret: Plugfest and interoperability testing - we want to do that fast Q3 and also F2F
CACAO playbooks can be adjusted by products - it's aggressive but doable.

Bret: RSA 2021 - TALK proposal in the summer - about cacao - operational level of cyber defence advantages

Bret: Provide feedback in any form.

Next working call February 18