CACAO Technical Committee

Meeting Minutes

Date: 17 September 2019
Time: 15:00 UTC

Attendees

Bret Jordan
Adam Bradbury
Allen Hadden
Anup Ghosh
Arnaud Taddei
Arsalan Iqbal
Jorge Aviles
Chris O'Brien
Duncan Sparrell
Emily Ratliff
Frans Schippers
Gerald Stueve
Jason Webb
Jim Meck
JP Bourget
John Morris
JR Jewczyk
Kamer Vishi
Mahbod Tavallaee
Marco Caselli
Karin Marr
Naasief Edross
Patrick Maroney
Paul Patrick
Ryan Hohmer
Shawn Riley
Srinivas Tummalapenta
Tim Zhan
Vasileios Mavroeidis

Quorum was achieved in this meeting.

Link to Meeting Presentation/Agenda

https://www.oasis-open.org/apps/org/workgroup/cacao/email/archives/201909/msg00019.html

Actions

1. Call for participants to start writing their ideas and requesting time to present on TC meetings
2. Establish mechanism for documenting use cases
3. Add Vendor independent interoperability requirement to requirements list
4. Create document for requirements
5. Create Official Template for Security Playbooks Specification
6. Create mechanism for documenting use cases
7. Logo for the TC is needed for speaking engagements

Secretaries

No objections raised.
Secretaries appointed - Vasileios Mavroeidis, Lior Kolnik, Emily Ratliff

Detailed Minutes

Bret Jordan updated the WG about the ITU telecom world meeting - he got a very positive feedback from many organizations – they supported the need about the orchestration of security playbooks (machine readable way). He proposed to take the standard when is matured enough to ITU for further ratification.

Borderless Cyber in DC October 8-10. Bret Jordan will give a talk about CACAO (automation and orchestration)

Duncan Sparell brought up the topic of designing a logo for CACAO. He mentioned that he is attending a FinTech conference in NY and he will include a slide for CACAO.

Jyoti Verma will also present CACAO in October at Grace Hopper.

Bret Jordan went through the requirements-actions for developing a CACAO playbook. More details in the slides

Bret Jordan recommended to start writing text as soon as possible (drafts) “formalizing the requirements” (work to be done).

Anup Ghosh – Playbook for spear-phishing – He asked about developing higher-level (more general) playbooks where we take into consideration for example how to address a spear phishing attack. Standardize the basic core elements that then expert can refine for specific incidents. Bret Jordan agreed that we should take into consideration such general cases as well.

Bret expressed the need for decision logic in CACAO playbooks such as temporal and conditional logic. Also support for Unique identifiers (like UUIDv4 – maybe not specifying the exact version in the specification) – fundamental for the building blocks that you can connect in a graph and process them. Also all transactions need to be able to be monitored (e.g., identifiers with timestamps). More details in the slides

Bret: Group targeting – including also humans as targets not only machines

Bret: Use cases and testing – machine automation – human actions/intervention and testing

Duncan: How do you see use cases been documented
Bret: write draft documents for the use cases – Bret asked the WG to start writing/contributing their use cases

Reporting: full reporting of each action. More details in the slides
Digital signatures: Bret: Use digital signatures to sign parts or the whole playbook
Examples actions for Cisco ASA firewall for a specific malware that an entity can sign and then potentially cisco can sign etc. Multiple signatures for correctness and accuracy

John Morris – There is a need to associate variations of 'plays' based on a hierarchy of play identifiers (or a superset of concatenation of associated play indicators) to address the need to identify the variant of a case that a user might have. Given the discrete nature of play identification UUIDs and the generality of the case supposed by others of spear-phishing, it would seem a play consumer should be made aware of the play options surrounding the issue they have detected so as to not 'treat' a lesser or similar issue while missing key components. This end may also be achieved by a simple hierarchical search response refinement within a sharing implementation in order to be made aware of the full horizon of an instance.
Bret Jordan – enough metadata that tooling can be developed

Jyoti: Higher Concepts of playbooks that can create a hierarchy (abstract level)

Duncan: Vendor independent interoperability , it would be good to bring a slide or write this down in a document to have some details of what we want to achieve. Bret confirmed that he is going to create a doc that we can write down all the requirements.

Bret talked about management separation where COAs may be defined in one environment and executed or deployed to a different environment. More details in the slides.

Bret remarked how important is to re-use of existing taxonomies in the development of CACAO (if available, for example taxonomy for targets/systems)

Duncan noted the additional non-functional requirements for the Technical Committee

- 'agile' requirement - break the work in phases and get 'minimum viable product out sooner rather than a 'complete' standard taking much more time
- requirement for 'use other standards' when possible and provide comments back to other standards when changes are needed

Jyoti remarked the importance of having members of the technical committee creating security playbooks as use cases

Meeting adjourned.