CACA0 Technical Committee

Meeting Minutes

Date: 1 October 2019 Time: 15:00 UTC

Link to Meeting Agenda/Slides

Attendees
Adam Bradbury
Allan Thomson
Allen Hadden
Andrew Storms
Anup Ghosh
Arsalan Iqbal
Bret Jordan
Chris Dahlheimer
Chris O’Brien
Emily Ratliff
Frans Schippers
Henry Peltokangas
Jason Webb
John Morris
Jorge Aviles
JP Bourget
JR Jewczyk
Lior Kolnik
Mahbod Tavallaee
Marco Caselli
Michael Rosa
Paul Patrick
Rodger Frank
Shawn Riley
Tim Zhan
Tom Maier
Vasileios Mavroeidis

Quorum was achieved during this meeting.

Action Items

● [All] Enrich the CACA0 requirements document

Notes

TC members were requested to start enriching the CACA0 requirements document and make comments. It is also recommended to use the suggesting mode for editing the documents.

People that want access to the Google docs of CACA0 send a message to Bret Jordan or Allan Thomson

CACA0 needs to support actions for automated machine to machine actions but also human interaction
Bret Jordan will have a talk at Borderless Cyber about CACAO

The TC spent a considerable amount of time in this meeting describing the architecture/building blocks of the CACAO playbooks. Playbooks have 3 main sections (check slides for more info)

- Identification of the playbook
- Control flow – logic
- Playbook Actions

TC member - Anup Ghosh: we need to specify the requirements for interoperable security playbooks

Operating model in mind, we may all have different operating models

Security service – inherently multi-tenant

Do we need to capture the operating models for each playbook?

Allan Thomson: capture this in the use case document. We need use-cases from an enterprise IT perspective. Service provider use case is missing.

Important to design so that this can be tested.

Questions raised:
TC member - Marco Caselli: Do we need different types of playbooks? e.g. executable vs template

TC member - Andrew Storms: use "type" for the workflow

TC member - Anup Ghosh: Borderless BoF – People that are interested to join send an email to the CACAO email list (to record interest)