PGB Meeting – October 22, 2020
Attendees: Jason Keirstead, Kelly Cullinane, Forrest Hare, David Kemp, Steven Wood, Darren Thomas

Agenda

- Debrief on Discussion with IACD
- Progress on SCAP V2
- Discussion on C4 Modeling Tool

Topic 1 – Debrief on Discussion with IACD at Johns Hopkins by Stephen Wood and Forrest Hare

Mike Herring (NSA) is the focal point to work with on IACD and next steps. Forrest met with Johns Hopkins (Harley Parks); leads IACD effort. Automate SOAR actions to make response actions quicker is the objective. NSA is looking to subset IACD and turn it over to industry (planned for December). Juan Gonzalez (CISA lead for standardization). Forrest will talk to him Monday to get aligned. Government, industry and academia in same direction. We would be the logical body for NSA to transition to. Open C2 originated from IACD.

Discussions need to follow to discuss what this means and how we can work together. IACD wants industry to take over (adopt by industry, extend by another group). They could fund OASIS as part of the transition. OASIS has foundation in a box concept (we could possibly turn OCA into a foundation). This would make it easier to contract with other groups; but it is a heavier weight structure than OCA currently has.

Possible for John Hopkins to join OCA if this transition occurs. NSA had sponsored John Hopkins to run the conferences and plan for IACD. NSA is backing away from this sponsorship. Open C2 is feeling a lack of management support from this. Artifacts are all available and the money seems to be disappearing. IACD as a program (within NSA) has disappeared. It is unclear how IACD will transition.

Topic 2 – Progress on SCAP V2

Number of meetings with MITRE to progress. MITRE side is done for code hand-over. NIST side needs about 2 weeks to get their repro on Github. There are no expected blockers. Jamie (OASIS chief counsel) has requested a document concerning the SCAP trademark.
In parallel, Adam is working on setting up a call to discuss the project.

Topic 3 – C4 modeling work

Adam posted an initial pass using C4 and posted this to our Github. Asking people to look at it and provide feedback.

Other discussions

We discussed the endpoint workgroup activities (for visibility). We now have a Project defined in Github to make our actions visible and can track next steps and collaborate across the teams. The endpoint workgroup is the initial workgroup; we plan to start the others once we get cadence.

OpenC2 is having its Plugfest next week. An email has been sent out on how to join. Darren has managed to find some resources to do some work to get OpenC2 messages over OpenDXL. Darren wants to be part of the Plugfest. Eventbrite registration is available for the plugfest.