PGB Meeting – June 25, 2020
Attendees: Jason Keirstead, Adam Montville, Darren Thomas, Kelly Cullinane, Lodrina Cherne, Mitch Thomas, Forrest Hare, Jory Burson,

Agenda

Please find the agenda for tomorrows call. It’s a small agenda, but there is lots of discussion to be had around each item. Specifically, we expect the bulk of discussion to focus around mapping the categories that are the output of the Architecture group to different workstreams. We are proposing that the workstreams, which are made up of PGB members that are in each category, are used to drive the development of the OpenDXL Ontology project forward. JK and I have done some initial mappings of PGB members to one or more workstreams, please see agenda item 3 below. We can discuss specific mappings and if members need to move categories or be in additional categories on the call.

Overview and Approval of the new submission template
Architecture Working Group Readout
Discussion of Architecture categories to workstreams

Initial Pre-mapped Group Categories:-

Threat Intelligence – Threatq, ElecticIQ, Cyware, Reversing Labs, Recorded Future, New Context

Endpoint- McAfee, Crowdstrike, ACS, Cybereason, Cyberark, Armis

SIEM - IBM, Fortinet, McAfee, Artic Wolf

SOAR – Threatq, IBM, DFLabs, Cydarm, Cyware

Infrastructure - Gigamon, McAfee, Corsa, Fortinet

Vulnerability, Compliance, Policy- CIS, Tripwire, Tufin, CyberNB, Safebreach (+NIST folks later?)

OT/Embedded - Armis, New Context, EPRI

Security Overlay/Consolidators/Consultancy - Raytheon, SAIC, sFractual

Topic 1 - Overview and Approval of the new submission template

Arcangel project proposal to drive submission process – then run a ballot/vote
Need a majority vote

Arcangel - Debugging, dev integration testing with OpenDXL

Need a why. What problem does it solve? Value? End user perspective. How does it contribute to OCA's overall goals (ex interoperability)?
Any existing license? Proposed open source open source licenses)
Implementation language(s)
Link to IPR policy for open projects, CLA requirements, open source requirements
How is it going to be resourced? Scope/expected lifespan of this project development lifecycle? Screenshots, Architecture, Whitepapers, Demo Video,
What are the OCA's expectation on the project
Maintainers, resources for ongoing work

Create a public catalog of proposals
Github with issues to track the proposals
Submissions in Github – stages of the proposal can be separate folders
Separate repro for these documents will be set up

JK will update the template the week after July 4 – have submission in github, review and create a ballot the following week

Topic 2 – Review the group assignments

Overview of the architecture diagram
Motivation - Structure around OCA and move agenda items forward
Ask of PGB members – commit an hour/week of technical time from SME to work on these workgroups
Contribute back to dxl ontology
Some key focus areas to add to the picture (infrastructure)

Mitch shared Kubernetes diagram
Overlays working groups and committees
https://github.com/kubernetes/community/blob/master/SIG-diagram.png.

Boxes to overlay interest groups and working groups – get people to engage, where to get involved.

Assignments to working groups?
Formal ask? Members present agree to proceed; send out formal ask to the group
Deliverables? Additional actions/alerts that formulate ontology

Define the actions; pick one and define in ontology
Ontology – 2 contributors so far; we want more activity and these workgroups will help us organize and drive actions
Want to demonstrate progress in dxl (Darren)
Darren will initialize the definition of the output

Adam can take template back to the SCAP group for their feedback

Darren – delayed leave coming up (July, Kent Landfield to sub in for 2-3 months for PGB)