Architectural Reference Working Group

Meeting Minutes

18 May 2020

Attendees: Kent Landfield, David Lemire, Michael Stair, Russ Warren, Forrest Hare, Stephen Wood

Agenda: Time for us to get back together and review the progress to date on investigation other standards efforts that could relate to what we plan to do as well as discuss the architecture picture. Please take a look at this (posted in our Github) and add your input.

Summary of Discussion:

1) The group reviewed their research on groups developing standards to determine how our efforts can be complementary and not create duplication of their efforts.
    a. Forrest covered the IACD (interactive adaptive cyber defense) and its objectives. He also covered the Software-Intensive System Acquisition (SISA) Programs. These programs are aimed at standardizing cybercops language/data model and improve symentec meanings. The IACD is focused on automating cyber defense. Key players include John Hopkins, NSA and SysOp. The NIM (National information exchange model) via its cyber-exchange subproject is working on terms and definitions. CISA (Cybersecurity and Infrastructure Security Agency) is focused on leading the effort to enhance the security, resiliency, and reliability of the Nation's cybersecurity and communications infrastructure. The IACD looks like it is harmonious with OCA. For OCA, we can see what we can do for integration; as we are focused on integration of products. We may be able to benefit from the IACD architecture and help tie from the IACD focus on research to the operational level and the integration of technology solutions. Next steps would be to reach out to CISA and IACD. Forrest and Kent have contacts in these groups. Kent was going to write up some paragraphs on how we OCA, IACD and CISA can connect.

    b. Kent covered the activities currently underway in Europe. He had met with the ENISA(European Union Agency for Cybersecurity). This group is focused on recommendations on cybersecurity and independent advice, activities that support policy making and implementation, 'Hands On' work, where ENISA collaborates directly with operational teams throughout the EU, bringing together EU Communities and coordinating the response to large scale cross-border cybersecurity incidents and drawing up cybersecurity certification schemes. This group is currently focused on COVID for the foreseeable future.

        DG Connect is concerned with the use of Information and communication technologies (ICTs). The DG's role is to

i. conceive and implement the policies required to create a Digital Single Market for more growth and jobs, where citizens, businesses, and public administrations can seamlessly and fairly access and provide digital goods, content and services.
ii. foster a modern, secure, open, and pluralistic society building on Europe's cultural diversity, creativity and respect of creators' rights and values such as democracy, freedom of expression and tolerance.
iii. help drive the digital transformation of European industry and public services through the use of innovative digital technology and support for the development of digital skills.
iv. develop a long-term vision investing in potential technology breakthroughs and flagships, which can improve peoples' lives and to increase the competitiveness of the European economy at large and its key sectors.

This is a new commission and is starting out defining their works scope. They are working on a toolkit (Informatics) and have a desire to open source it. They want to develop this tool for the EU first, then go opensource. There is a meeting planned for this Fall where we can learn of their progress and we can try and align with their efforts.

c. Michael and David discuss Open C2. Open C2 is focused on command and control standardization (the IACD acting function). We discussed the desire to align Open C2 with the OCA Open DXL ontology project. We discussed the need for a working group to follow up on this. David is going to create a few slides to frame this discussion.
d. Draw out architectural reference diagrams – The object is to describe the system that OCA should be undertaking. This can be thought of as a vision or scope document. It is not intended to constrain work as this is decided by members. It is to suggest where known work items are so that people can assign efforts to things which align with their interests and our needs. Please flush out the missing pieces. Modify (even minor changes!) the existing architecture diagram.

2) Housekeeping tasks
   a. A doodle poll will be circulated to set the time for next meeting. We will try to make meeting day/time regular thereafter. We are shooting for a monthly cadence.
   b. Meeting minutes will be posted on our Githib Wiki.