Architectural Reference Working Group

Meeting Minutes

12 November 2020

Attendees: Adam Montville, Mitch Thomas, Russ Warren, Bill Munyan, David Lemire
Forrest Hare, Doug Austin, David Kemp

Agenda: Completing a 'version 1' of our architecture by the end of this year.

(1) Review the updated C4 diagrams that Bill/Adam/Mitch have done
(2) Review use cases that Doug Austin has sent out
(3) Identify next steps

Mitch took us through the diagrams (forked initial-c4-diagrams). SACM context diagram, container diagram, and component diagram. New material added showing the manager component diagram. They did not map to existing OCA picture. They looked at the use cases as well.

What are we trying to do on C4? Option – take OCA diagrams and rework as C4 diagrams. Request – describe the boxes. They can fill in the descriptions on the picture. We can use the OCA picture to fill in the context more (as a checklist for things). Landscape diagram is a higher level (users included). Green box (OCA) are functions that support activities. Workgroups will help add flows to show between the components.

Next steps: Take OCA diagram and make C4 images (iterative). C4 images will have better descriptions on the boxes. Diagrams will have text inside of them. Adam, Bill and Mitch will work on this.

SIEM or SOAR should have flows and data can flow to one or both of these.

Doug walked through the use cases. We can use these to show users point of view (SOC analyst). First one covers endpoint protection software. Second one was a firewall use case. The third one a vulnerability assessment use case. Vulnerability scanner indicates an issue.

David Kemp is looking for these to give context (users involved, data that flow). Perhaps we can take the landscape diagram and use cases to show how the architecture applies. Doug Austin offered to help us work with marketing and the work groups if they need some use case work.

Our next meeting with be Tuesday, November 24.