Endpoint Workgroup Meeting – November 17, 2020
Attendees: Bill Munyan, Forrest Hare Stephen Wood, Jason Flood, Sergey, Bruno Silva, Nalini Kannan

Agenda

- Jason Flood. He has been working with OpenDXL and wants to share his experiences around OpenDXL. He will provide a discussion and proposal around extending the openDXL ontology to encompass a wider base of security data source types. I think this will be very valuable as we evolve our endpoint work group and we will learn from his work.
- Continue endpoint group discission: You have been asked to review the file reputation change use case and comment on the message format (what should be changed (added/deleted) from this sample). Our goal is to come to agreement on this message format as a group. We will follow on the group activity by dividing up other common use cases and proposing message formats that we think should be common across the security components.

Topic 1 – Jason's Flood – OpenDXL ontology experiences and thoughts

Looking at threat actions and trying to group data together. He is looking at the ontology to make data accessible. Shares his ontology thoughts. Archangel proposal (extensions on top of broker) has been submitted. He is looking at findings (result of queries). Looking at how to use OpenDXL ontology to group results. He looked at NIST's breakdown for cybersecurity events. He wants to propose this work into OpenDXL framework. Anomalies and events data from SIEM is the topic. Pull request has been submitted to OpenDXL.

Bruno and Bill (SCAP) were interested in working with Jason on this project. Configuration and posture assessment would be a focus for the SCAP discussion. Working on the payload definitions for a finding object. Stephen Wood is also interested in SCAP angle.

Jason will send his presentation and I will post it to our Github. I will set up a call in 2 weeks so we can continue the discussion with Jason and discuss how we can align SCAP. We discussed posture collection service.
We discussed perhaps a focus on configuration and vulnerability management as a possible area to focus on.

Topic 2– Endpoint workgroup discussion

Nobody on the call had any input or comments from the previous calls and actions. We do not have a proposal under discussion on how to advance the OpenDXL ontology work for endpoints. Please reach put to Russ Warren if you have any input on how we can move forward with this group. We will need to come up with some ideas on how we can progress in this area.