Endpoint Workgroup Meeting – October 6, 2020
Attendees: Jason Keirstead, Bill Munyan, Darren Thomas, Charles Schmidt, Lodrina Cherne, Shawn Wells, Michael Haines, Chris Kachigian, Saravanan Thiyagarajan, Chris Smith, Steven Wood, Doug Austin

## Agenda

Discuss group objectives and identify background material
Level set for the group
    Discuss current draft architecture
    Discuss OpenDXL and OpenDXL Ontology
        Review and Discuss an example of what we would like to produce from this workgroup
Identify next steps

## Topic 1 – Discuss group objectives and identify background material

We reviewed the group objectives and timelines. We will use the OCA Documentation Github to capture meeting minutes and group activities. To start off, we would like to define key use cases and identify formats for the Actions and Responses for common actions. Later in the agenda we covered an example, file reputation event.

We discussed two high level examples of the work groups goals:

1. The endpoint detecting a deviant process execution as an example. Once this is discovered by the endpoint, how should this event be reported to the other security components?
2. The endpoint discovers a file reputation change. How should this be communicated and how would the security components respond to it.

The desired output for this work group would be to identify common actions and define the data formats that we can standardize on to enable security components to more effectively communicate with each other and improve on today's approach of point-to-point (product to product) communications. By achieving this objective, OCA can foster intercommunications across multiple security components and increase the effectiveness of security operations.

## Topic 2 – Discuss current draft architecture

For our current architect diagram, we discussed the need to update it for SCAP V2. Members of the work group are welcome to update and edit our current diagram. We can discuss these updates in our next work group call. We also plan to restart the architecture work group in the next 2 weeks. If you are not currently on this work group and are interested in joining, please send an email or slack to Russell.warren@us.ibm.com and I will add you to our group. The previous architecture meeting notes and documentation are located on our Documentation

Github (https://github.com/opencybersecurityalliance/documentation/wiki).

## Topic 3 – Discuss OpenDXL and OpenDXL

An OpenDXL Ontology overview was reviewed to level set the group on its goals and objectives. We will be using examples from the OpenDXL project to help guide us and provide a starting point for the development of our OCA actions and message formats.

## Topic 4 – Review and Discuss an example of what we would like to produce from this workgroup

There is a Web site that contains examples of actions and notifications (opendxl.com/filebase). We reviewed the McAfee Threat Intelligence Exchange (TIE) to show an example of how file reputation events are communicated.

## Topic 4 – Next Steps

Please review the TIE examples on the file reputation event. Provide input on what the action and message formats should look like for this event. We want to focus on the base case (not all the message content needs to be covered but the main content should be to enable us to facilitate interoperation across multiple security components.

- For those with SCAP V2 background, try and ensure our architecture diagram is up to date and positions the SCAP components (Policy, SACM, etc.). Take a look at the example message formats for the reputation event and consider the SCAP components and their communication needs and propose message content/formats that would be able to receive and process the file reputation event message.
- For those with endpoint, SOAR, SIEM and other security component knowledge, consider these components and their communication needs and propose message content/formats that would be able to receive and process the file reputation event message.
- For all others, review our architecture diagram and proposed suggested updates we can make that would enable a clearer picture of how we approach interoperation. Review the message formats for the reputation event and proposed extensions/updates that would provide better information exchange across the security components.

Thank you all for participating in the call. Here is a link to the replay https://ibm.webex.com/recordingservice/sites/ibm/recording/play/a8bf593724c8469081de50536308f0e6 password: Pun3ppai