Endpoint Workgroup Meeting – October 27, 2020
Attendees: Jason Keirstead, Lodrina Cherne, Nalini Kannan

Agenda

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.

Here is the link to the opendxl ontology github showing the actions and notifications we will use as a starting point --> https://opencybersecurityalliance.github.io/opendxl-ontology/
sample event reputation change event --> https://www.opendxl.com/filebase/index.php?file/25-mcafee-threat-intelligence-exchange/#event--mcafee-event-tie-cert-repchange

Any questions or comments, please post on our SLACK channel! https://open-cybersecurity.slack.com/archives/C01CXSADR6U

Topic 1 – Discuss architecture diagram and scoping of our work

Lodrina – got familiar with architecture. Forensics skills at Cyberreason. Updating terminology (ex blacklist). Use actual action (ex blocking list). Example actions may need to be more specific and turn into multiple actions. We should eliminate terms/update terms that are in the example. Bottom left corner (endpoint). Do we have one of each type (ex hosts) and how would it look with more hosts? We may need to update the picture to deal with multiple instances of hosts and endpoints. Questions about the lateral communications and scaling. Posture collection (from SCAP) responds to requests for compliance information and endpoint queries. The actuators come from IACD (services that can actuate commands on the endpoint, ex respond/quarantine a process). EDR is the detection service that is monitoring for IOCs and other endpoint security events and producing findings to share with the fabric. These are logical components.

Our goal is to take these examples and define the top 1-3 use cases that we should align on them and then work the details. Ex Blacklist/whitelist one. Is that one of the most important use cases? What can be done on an endpoint (identify the three most important ones)? Perhaps focus on producing one action per endpoint type (PC, phone,..). There are different types of endpoints. Actions to isolate the endpoint is an example. Atomic data (ex MD5) and relationships (powershell) between items is what we care about. Detections will require this information. EDR box feeds detection box. Detections will be an activity that will follow on.

Look at your product APIs and map to our diagram. Is something missing or contained that does not exist in the product. Let's call those out.

File reputation use case may not be relevant for mobile endpoints. Perhaps we should select a use case that is relevant to all types of endpoints. We can scope (ex non-mobile and file reputation first, then add others later).

URL access/phishing attacks; malicious acts (malware/spyware) are most common in mobile endpoints. Could process detection be a category/use case we can focus on? Would this cover the URL access/phishing case? Perhaps we should start by fleshing out the use case to see if there is any commonality across these. Perhaps we can use extensions to reflect unique properties (windows, mac, phone). Focus on rogue process? How would we communicate that to the fabric?

Should SHA256 or MD5 hashes should be used? We need to see what the maximum compatibility is. Desire is to use the STIX2 cyber-observable ontology wherever possible, use OPEN C2 for communicating actions. STIX2 does have a file object defined. As STIX2 is so flexible, we may want to pick a specific format (ex SHA256) for our definitions.

Action is to look at both use cases and define actions and data for each. Let's also fix the terminology (blacklist) in the ontology documentation.