## Wednesday, September 27, 2017

**Presentation**

**Participants:** Dave Kemp, Jyoti Verma, Lisa Mathews, Allan Thomson, Dave Lemire, Phillip Royer, Alex Everett, Danny Martinez

|  |  |  |  |
| --- | --- | --- | --- |
|  |  |  |  |

**Notes:**

Dave Kemp presented the Actuator Profile roadmap.  Mr. Kemp highlighted that there are multiple models and the subcommittee is still refining.  Different ‘categories’ or ‘taxonomies’ have been considered such as ‘device centric’, ‘functional actuators’, or possibly hybrid approaches. The presentation defined two very high level categories of actuators; ‘Acting’ and ‘Sensing/ analytics’

Philip Royer discussed his effort to create an early draft of an ‘endpoint’ actuator profile.  He is capturing the command set from seven endpoint security products and mapping to OpenC2.  He will identify which actions, specifiers and any deficiencies in the OpenC2 action list.

The categorization and the appropriate level of granularity for the actuator profiles was discussed at great length.  Some of the major points identified include:

* A single product may do multiple functions (need multiple profiles)
* Other ‘categories’
  + STIX uses ‘Personas’
  + ‘monitor’ vs ‘change state’
  + Value in defining in terms of ‘product class’
    - Facilitates vendor adoption
    - Permits companies to ‘see themselves’ in one or more of the products
  + Tradeoff is between increasing number of profiles required (if functional centric) vs increasing overlap between profiles (if product centric)
* Is a clustering issue.
  + Survey different products and write profiles IAW how they are clustered
  + Challenge is to identify the appropriate clusters
* Hybrid approach
  + Both lists [device centric vs functional actuator] have value
    - Each list has a distinct purpose
    - Do not need to ‘merge’ the lists

The STIX approach was presented by Allan Thompson and discussed at great length

* STIX defines ‘Personas’
* Tests were defined
* A matrix consisting of a test, applicable personas is provided
  + A product of a particular persona reviews the list and executes the test if it applies to the persona
  + Common tests apply to multiple personas
* Discussion/ Questions
  + If there are multiple products with ‘partial’ functionality, how does one define ‘Mandatory to implement’ vs ‘optional’?
    - Agreed, that justifies the ‘profile’ approach
  + Tradeoff identified:
    - Avoid excessive number of profiles
    - Avoid profiles with a low ratio of ‘mandatory’ vs ‘optional’ to implement
  + A lot of correlation, OpenC2 needs to identify which set of ‘personas’ are needed
    - The ‘list’ of personas will come from the marketplace
  + Similarities (between OpenC2 and STIX personas) but not exact. Coupling of actions with actuators adds nuances to the meaning [of the action]
  + Need to define [profiles] in a manner that vendors are comfortable mapping their products to
    - Broad device centric products make more sense to real world products
  + Consider define in terms of ‘products categories’ but test in terms of ‘functional categories’

**Actions:**

All;  Review product categories and functional categories

Philip Royer to present a draft ‘endpoint profile’ at the October 11, 2017 AP SC meeting

Joe Brule to create a directory on googledocs for the endpoint actuator profile

Jyoti Verma to provide Gartner’s list of ‘product classes’