IETF SACM Virtual Interim – March 9, 2016

Chair Slides

Requirements Draft Update

- No objections to addressing issue #97 as suggested by the issue
- Issue #67: Henk suggested that we address issues where we use terminology in a different context from where it was intended; Lisa proposed to Close this issue in the requirements draft and highlight contextual issues in the terminology draft (with a new issue). No one objected.

Endpoint Compliance Profile

- Question about needing to look at configuration information in addition to software inventory information. Danny: In addition to the current SWID-based ECP specifications, we want to look at using OVAL to assess configuration information. We need to create (or refine) data models to address these needs.

SWID Messages

- Dan: Would adoption mean merging this draft into another WG document?
    - Danny: This is a solutions draft on top of NEA, so keeping it separate is useful.
- Henk: Can you visualize how this draft fits into the SACM architecture?
    - Danny: We will do that.
    - Jess: To do that, we will need to sort out the role of an internal collector first.
    - Henk agreed with Jess.
- Karen: We need to discuss who will review this and all the other solutions drafts.

Information Model Update

- Ira: Did the datatypes you presented represent all the datatypes from IPFIX?
    - Danny: no I left some out to save space on the slides
    - Ira: Suggestion: Use URI, array, and map datatypes since these are constructs in JSON and CBOR.
    - Danny: Suggested posting these suggestions to the list.
- Lisa: What would these attributes be, what would the workflow be like if you move these to an attribute store?
    - Henk: We may need to classify first. Identify first, then associate collection and evaluation related attributes. Other processes can be about re-identifying and correlating. It is important that we allow solutions to scale.
    - Lisa: What SACM component would do this? It would be helpful to have a diagram showing this.

OVAL

- Dave and Danny: Briefly discussed that data published to a CMDB could be statically configured on the endpoint or could be initiated by a request to the endpoint to publish.
- David Ries: Clarified that logic and what data to collect needs to be associated.
    - David Waltermire: Discussed the need to separate collection and evaluation from the perspective of exchange.

Chair Discussion

- Adoption call on vuln assessment scenario between interim and IETF 95
- Dave W. Suggest we use the vulnerability assessment scenario to inform a small set of drafts (2-4) to work on. Adam agreed.
- Karen: Depending on adoption call, Consider focusing IETF-95 discussion on what drafts are needed to address the vuln scenario.
- Karen, Danny, Jess: Focus reviews on ECP and SWID messages.
- Danny: Present at the opsec meeting
- Karen and Adam: Will work out request for reviews after the meeting.