# Information Model Update

SACM WG Virtual Interim Meeting

09/13/2016

# Agenda

- Open issues
- Next steps
- Status

# DM-001: IM/DM requirements issue (1)

- DM-001 currently states that a data model MUST contain a data model element for every SACM Information Model element
- At the IETF 96 Meeting[1][2][3], there was consensus not to reopen the Requirements I-D[4] for editing, but, we could revise DM-001
- Revised text for this requirement was discussed on the list[5]
  - The term "element" was preferred over "artifact"

1. https://www.ietf.org/proceedings/96/slides/slides-96-sacm-2.pdf
2. https://www.ietf.org/proceedings/96/slides/slides-96-sacm-5.pdf
3. https://www.ietf.org/proceedings/96/minutes/minutes-96-sacm
4. https://datatracker.ietf.org/doc/draft-ietf-sacm-requirements
5. https://www.ietf.org/mail-archive/web/sacm/current/msg04345.html

# DM-001: IM/DM requirements issue (2)

- Each data model element that is derived from the SACM Information Model MUST be associated with at least one SACM Information Model element and MAY be associated with more than one SACM Information Model element.

- A SACM data model MAY include additional data model elements that are not associated with any SACM Information Model elements. For example, two SACM Information Model elements ~~from the SACM Information Model~~ could be mapped to a single SACM data model element. As another example, a SACM data model element does not need to directly correspond to any ~~item in the~~ SACM Information Model element.

# A few non-critical IE-related topics

- The IM is now 153 pages and growing (without IEs it’s 32 pages)
  - May want to consider moving some (or all) IEs into separate I-Ds

- When adding IEs we noticed some shared the same enumeration of values
  - For now, we just duplicated the enumerations in each IE
  - Do we want to define generic IE enumerations and use them as IE datatypes?

# Next steps

- We have a complete IM with lots of IEs and need WG review ☺
  - Does the text for guidance and evaluation results seem reasonable?
  - Which IEs are critical? Which IEs are non-essential? Where are the gaps?
  - Are we missing any key IANA, security, operational, or privacy considerations?
  - Any other feedback is welcome

- Close out the DM-001 issue and submit a pull request to the Requirements I-D

- Beyond incorporating WG feedback, we plan to shift focus to data model development and gaining experience using the IM

# Status

- Made various updates to the IPFIX syntax based on discussions at the IETF 96 Meeting
  - Introduced an enumeration datatype for IEs
  - Added a structure property to the IE specification template to define list and enumeration IEs
  - Defined a naming convention for IEs
- Defined identity, guidance (collection, evaluation, classification, storage), and evaluation results
- Included additional IEs related to software, configuration, and the Vulnerability Assessment Scenario I-D[1]
- Added text for IANA, security, operational, and privacy considerations sections
- Performed various other editorial changes and clean-up

1. https://datatracker.ietf.org/doc/draft-ietf-sacm-vuln-scenario/