SACM Vulnerability Assessment Scenario

IETF 95

04/06/2016

Agenda

- Status
- Where and how the solution I-Ds fit in
- Next steps

Status

- The I-D was adopted on 4/1[1]

- Will continue to update as needed, but, don't anticipate any major revisions

- Will serve as our near-term roadmap for developing solution I-Ds to address SACM's needs

[1] http://www.ietf.org/mail-archive/web/sacm/current/msg03862.html

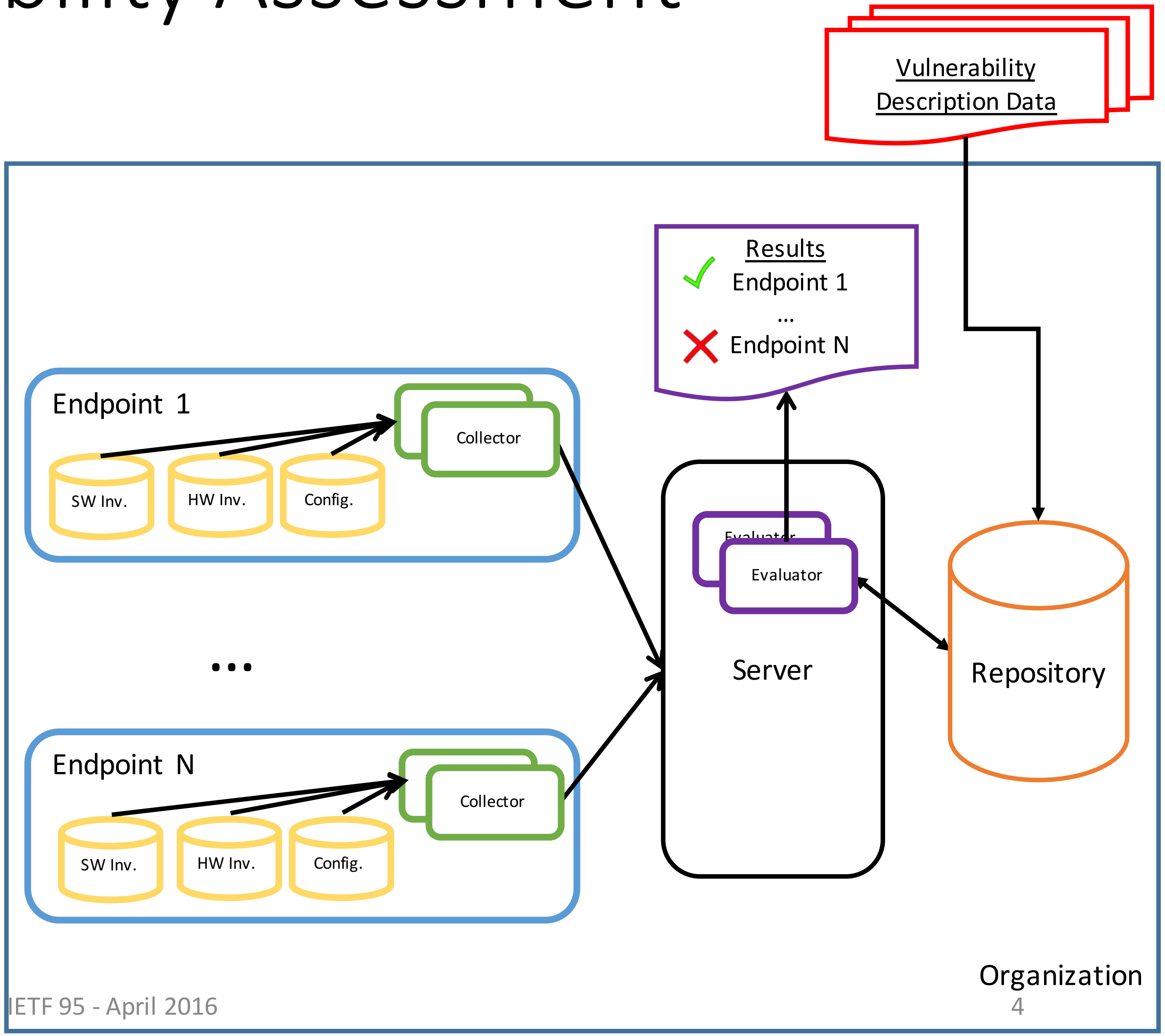
Steps of the Vulnerability Assessment Scenario Process

- Identification and initial data collection

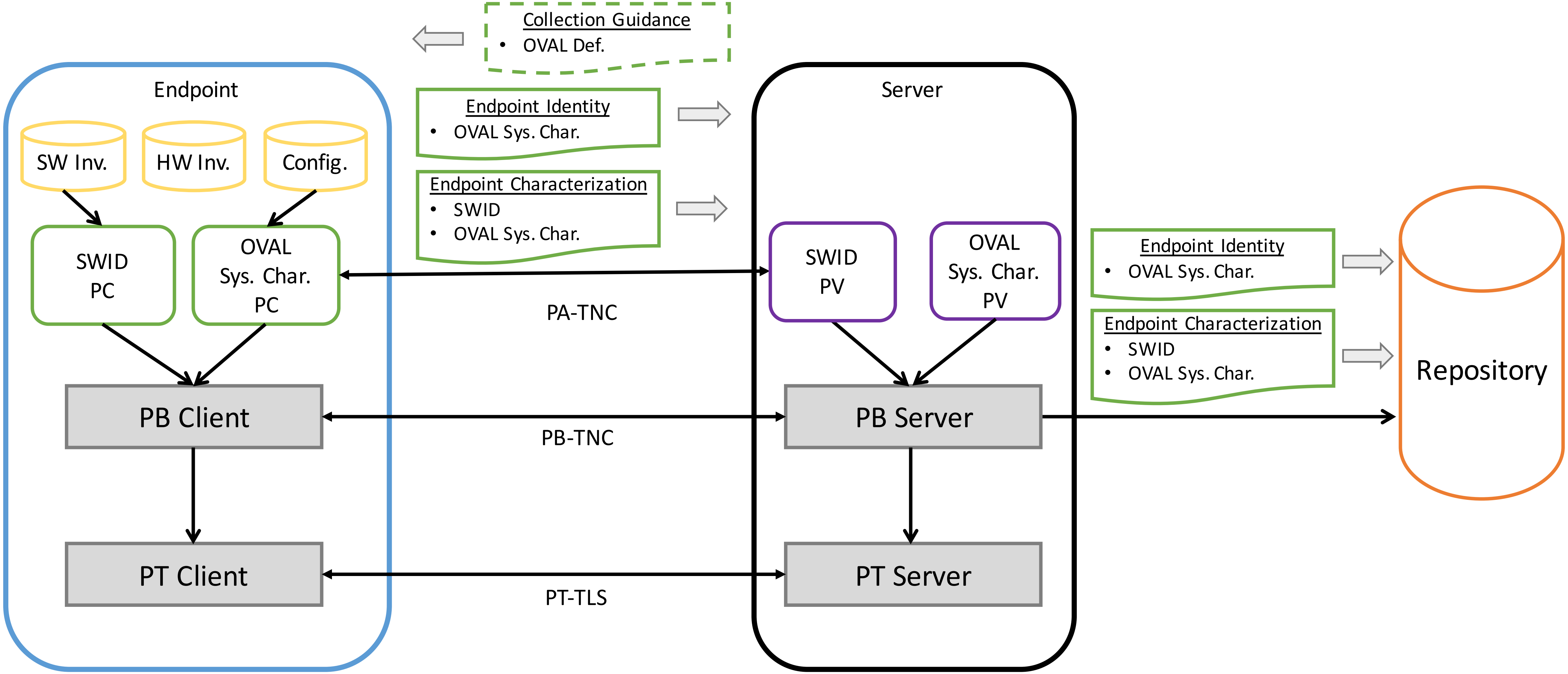
- Vulnerability description data

- Endpoint applicability and assessment

- Assessment results



Identification and initial data collection



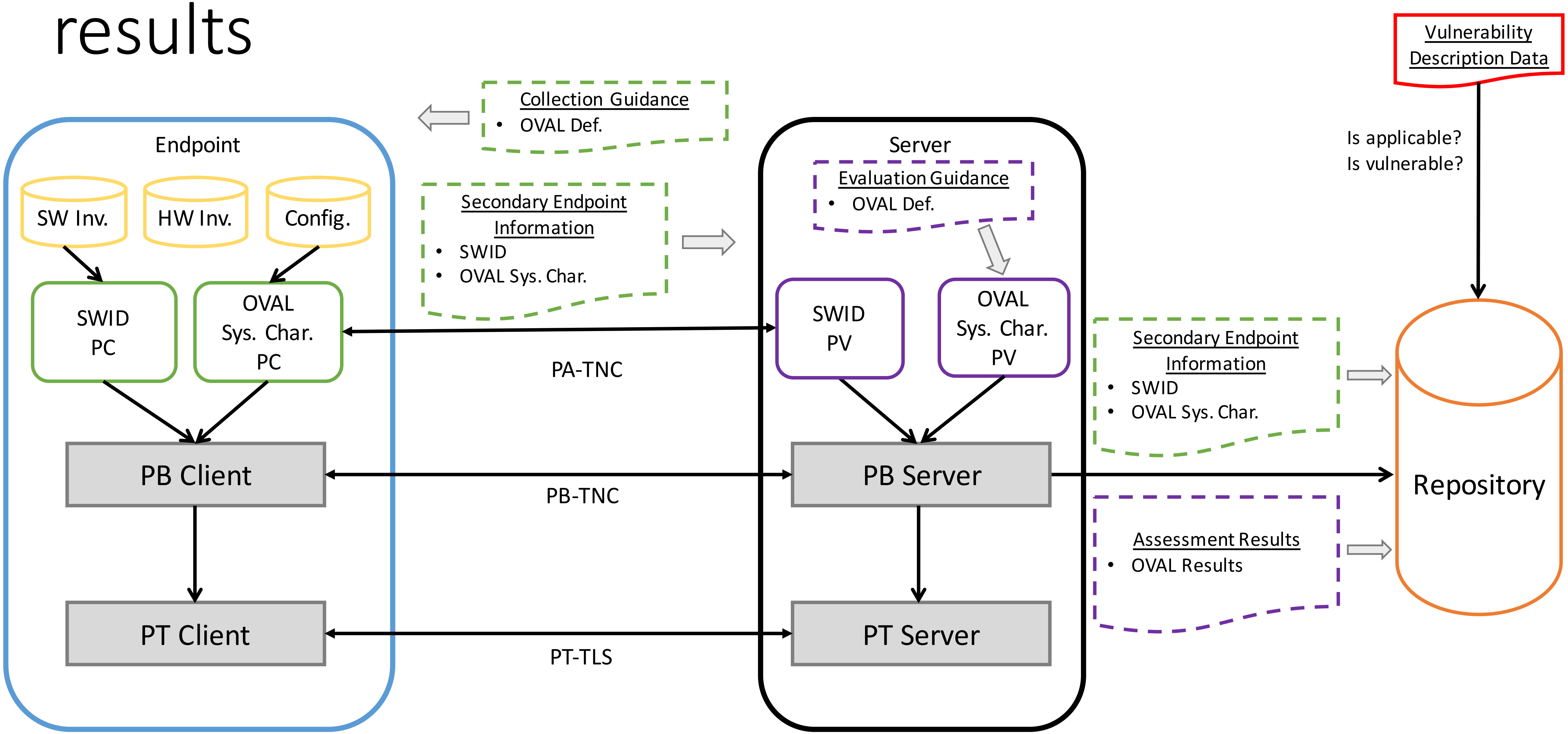
*Please note where OVAL is mentioned that I really mean the next-generation data models based on OVAL :).

Vulnerability description data

- An organization collects/receives this data from numerous sources and converts it to a form that can be used to assess endpoints on a network

- There are currently no solution I-Ds in SACM to support this

Endpoint applicability, assessment, and results



*Please note where OVAL is mentioned that I really mean the next-generation data models based on OVAL :).

Next steps

- Tie up loose ends on the I-D
  - Incorporate feedback from the OPSEC WG session[1]
  - Remove the TODO from the security considerations[2]
  - Integrate definitions into the Terminology I-D[3]
  - Capture information needs in the IM[4]

- Continue to develop solution I-Ds that satisfy the steps of the Vulnerability Assessment Scenario

[1] https://datatracker.ietf.org/meeting/95/agenda/opsec/
[2] http://www.ietf.org/mail-archive/web/sacm/current/msg03893.html
[3] http://www.ietf.org/mail-archive/web/sacm/current/msg03589.html
[4] https://datatracker.ietf.org/doc/draft-ietf-sacm-information-model/