VSMI TC Meeting

20 Sept 2022, virtual

ATTENDEES

Azaletskiy, Pavel - VS Optima
Beal, Helen – VSMC
Cullinane, Kelly - Copado
Davis, Robert - Plutora
Finster, Bryan - DoD
Hunt, Christian - CTIN

Joshi, Sunil - IBM
Kanser, Heather - Broadcom
Pereira, Steve - VSMC
Sayers, Yaniv - Micro Focus
Valani, Altaz - Security Compass
Vollmer, Peter - Micro Focus

AGENDA

● Call to order & welcome
● Differential analysis discussion
● New business

NOTES

● Call to order & welcome
● Please log your attendance
● Review of scoring matrix analysis work
  ○ Steve: – Review of CIM and ODI
    Both focused on CRM/customer data - not really analogous to what we are looking at. Only similarity is in connecting tools and sharing with a single vendor.
    ● Cloud Information Model (CIM) - Public review comments on too many fields being mandatory is telling. Shows being too strict had a negative impact
      No flow models here. Looked only at customer activity and not value or work flow
      Failures here are somewhat universal
      Thing they did well – Github repo that still exists. We can emulate this if we get this defined
    ● Open Data Initiative (ODI) - MS version of CIM
      Most of this is not a match. Went away around 2019. Only alive for a year or so. Not a lot of useful information. No active or currently under dev.
    ● Splunk CIM - Active and popular. Still going through it
      Focused on security incidents and data attributes that relate to an active system. This is post build system tracking in a system
    ● Overall, none of the three are applicable, but we can learn from their failures
  ○ Altaz: – Review of IT4IT
- Digital delivery - aiming for value delivery
  Broken down into delivery mechanisms: plan, build, deliver, support
  Data model that exists within IT4IT – brings out where the integrations exist in the domains
  Involved in the planning of IT4IT
  With the matrix - filled out some things. Left not true blank because just because something is not true now, doesn’t mean it can’t/won’t be with extension or revision work
  IT4IT has a data model, but it will take effort to make it map to a value stream schema
  Has all of the attributes. Just becomes a mapping exercise to map it to what we are aiming for.
  Toolchain in IT4IT – it’s not about data access. It is about how pieces relate together to rapidly produce with a product mindsight. Never reach an end state, always improving. Does not address risk.

- Peter: IT4IT
  - Latest version is 3.0 and is under review. Might not yet be published.
  - Plan, build, deliver, run concepts are here – this has the idea of value streams embedded. Question of whether it is the right modeling of value streams
  - Topology is already here – relates some items already – see section 3.7 recap in the spec.

- Helen: Can we see the data model in greater detail?

- Peter: It’s in the appendix
  - [https://pubs.opengroup.org/it4it/3.0/snapshot/index.html](https://pubs.opengroup.org/it4it/3.0/snapshot/index.html) or [https://it4it-forum.projects.opengroup.org/it4it-standard/html/IT4IT-RA.html#_value_stream](https://it4it-forum.projects.opengroup.org/it4it-standard/html/IT4IT-RA.html#_value_stream)
  - Might need to be a member of the open group to access.
  - Lets take defect as an example - has purpose, key attributes, description status, ID type. Very architecture driven.
  - The project has a backlog so it will continue to evolve
  - Model is well managed and maintained in Github

- Altaz
  - Thought is to have a product driven approach. Can expect more improvements.
  - Open Group also has an initiative around digital portfolio - looking to integrate IT4IT and other projects. Keep this in mind for industry context. Could be important for how we operationalize value streams.

- Peter:
  - Will take the action item to reach out and have IT4IT to join a session.

- Altaz: Review of OCSF
  - Focused at a granular level – do you have patches, have you remediated?
  - Touches on discussion we’ve previously had when we talk about operationalized value streams. What do teams or programs need to be focused on?
  - Created by Splunk and IBM. thought was to bring together all schemas for security tools to talk to one another. Currently running. Not sure if it is close to reaching its goals. Picking up speed again after covid.
  - Schema that security tools will adhere to. Open and in Github.
  - Again, just because it’s not currently true doesn’t mean that it can’t.
  - Now part of OASIS – JK is leading
  - We might want him to come speak to us.
- **Kelly:** Will reach out to him and ask.
- **Altaz:** [Has a podcast on some high level – will share this out](#).
- **Helen:**
  Planning for future
  Commitments for all to finish their research by the next meeting
  Considerations for the next step

**ACTION ITEMS**

- Peter to reach out it IT4IT to join a future meeting
- Kelly to reach out to JK to join a future meeting for OCSF
- Complete differential analysis for those who have not done so yet
- All - think about next steps after differential analysis is done
  - Do we:
    - Start outlining our own sepc
    - Think about extensions to other specs to achieve our goals
    - 3rd option?