CC in the Cloud (CCitC) Technical Community – CCUF Workshop Meeting Minutes – Day 2

8:57 AM EST 2023-10-27

Call to Order: 0911
Meeting Lead: Joshua BRICKMAN

Highlights:

~

Old Business:

~

New Business:

- Josh B began with a brief review of yesterday's progress and laid out the brief schedule for the day
- Tyrone presented a brief update on ISO developments.
    o The NWI item that was submitted for CCitC never received any feedback or comments, despite several submissions/requests
    o When CC2022 was delivered, a request was made to merge CCitC work with the new CC updates into ISO, but no response has been received as of yet.
    o A new CC2024 version will likely be released due to several issues with CC2022 and the XML versions of it.
    o Generally, CC part 1 does not address Cloud topics or specific technology types, therefore it is unclear how CCitC work would fit into this or ISO.
    o There's a concern that if CCitC work is not included in the main CC documents, CCitC work will not be part of a freely available publication and therefore our guidance will only be included in the paid version of ISO.
    o With inclusion into ISO, most language around FedRAMP and other standards would largely have to be struck, in favor of ISO being the baseline.
    o Inclusion in ISO does not mean there will be buy-in from Schemes for CCitC.
    o "Patch Management" will be a new piece coming into play which the EUCC will likely require.
    o Discussion around whether targeting inclusion into ISO should be a priority
        ▪ This topic will be monitored and discussed further in the future
- Continued Section-by-Section review of the Guidance document (continuation from yesterday)
    o Reviewed Section "TOE Identification"
        ▪ Section text and Images used are sufficient, no changes required.
    o Reviewed Section "Cloud Equivalence Considerations"
        ▪ Editorial updates made, first two sentences have been struck
        ▪ Discussion around whether multiple cloud listings on a cert would be desired, and ultimately it may come down to a vendor business decision or a scheme decision on whether equivalence may exist if, for example, FedRAMP HIGH or other validation is the same on two different cloud platforms, etc.

- o Reviewed Section "CPU Equivalency"
    - ▪ Brief discussion on the work being done by the CPU Equivalency working group who are actively looking at this topic. This will be revisited in the future to assess whether their work can be leveraged for use in CCitC Guidance
    - ▪ Issue #119 has been created to track developments on this issue.
- o Reviewed Section "Protection Profile Considerations"
    - ▪ Reviewed sub-section "Process to optimize a PP for TOEs in a cloud environment."
    - ▪ Skipping this section and reserving for the editorial breakout group
- o Reviewed Section "Suggested inputs to a Security Problem Definition for Cloud evaluations"
    - ▪ Tyrone discussed this section and that with review of several other PP's to see which SPD components were similar and which had unique components, which could apply to Cloud deployments. Do they have assumptions and security objectives that we could incorporate into PP's that include cloud deployments.
    - ▪ These are just examples and not by any means a definitive list and can be further expanded for the requirements of specific PP's
- o Reviewed Section "Guidance Documentation"
    - ▪ Discussion around the "implicitly satisfied" language in the MDM PP
    - ▪ No editorial changes needed for this section
- o Reviewed Section "Guidance for Establishing Test Environments on Cloud Infrastructure"
    - ▪ Related to Issue #74
    - ▪ Some editorial changes made to exclude references to "raises some initial concerns"
- o Reviewed section "Vulnerability Assessment Methodology"
    - ▪ Discussion around TOE boundaries and whether the OE may or may not be included in the scope of the AVA.
    - ▪ No editorial changes made to this section

Break @ 10:56

Reconvene @ 11:13

- Breakout sessions have begun. Main room is for overall Guidance doc editorial updates.
    - o Conducted a section-by-section walkthrough to correct any grammatical, or editorial issues.
    - o Various sections updated, see GitHub tracking for exact modifications.

Break for Lunch @ 12:50

Reconvene @ 1:48pm

- Breakout sessions resumed. Main Room continued with editorial review of the Guidance Document.
  o Various sections updated, see GitHub tracking for exact modifications.

Break @ 3:15pm

Reconvene @ 3:30pm

- All breakout groups reconvene back into Main room
- Justin F presented the work conducted by the second breakout group
  o Review and modify the section "Process to optimize a PP for TOEs in a Cloud Environment" In the CCitC Guidance Document.
  o Using the content of the "General Derivation Procedures" document, explicit steps were created for incorporation into the Guidance document.
  o Marked up Derivation Procedures document to be posted to GitHub
- Brandon H presented the editorial work conducted by the first breakout group
  o "Preface" section, significantly revamped
  o "Relationships Between the TOE, TOE Platform, and Trusted Platform" Section significantly updated
  o Minor editorial updates made throughout the document
  o "CCiTC" changed to "CCitC"

Questions/Follow-ups:

~

End of Meeting – Adjourned 4:40pm EST