2020-Sept-1 CTAB Public Minutes - off week call

CTAB call of September 1, 2020

This was an off-week CTAB call to finish reviewing comments and editing the Baseline Expectations v2 Implementation Guidance and Best Practices document

Attending

- David Bantz, University of Alaska (chair)
- Brett Bieber, University of Nebraska
- Pål Axelsson, SUNET
- Tom Barton, University Chicago and Internet2, ex-officio
- Richard Frovarp, North Dakota State
- Jon Miner, University of Wisc - Madison
- Marc Wallman, North Dakota State University, InCommon Steering Rep, ex-officio
- Robert Zybeck, Portland Community College
- Johnny Lasker, Internet2
- Ann West, Internet2
- Albert Wu, Internet2
- Emily Eisbruch, Internet2
- Dean Woodbeck

Regrets

- Mary Catherine Martinez, InnoSoft (vice chair)
- Rachana Ananthakrishnan, Globus, University of Chicago
- John Pfeifer, University of Maryland
- Eric Goodman, UCOP - TAC Representative to CTAB
- Ercan Elibol, Florida Polytech Institute
- Chris Hable, University of Michigan
- Chris Whalen, Research Data and Communication Technologies
- Jule Ziegler, Leibniz Supercomputing Centre

Discussion

Intellectual Property reminder

BE2 Implementation Guidance & Best Practices

- Albert implemented the suggestions to the document made on the last call, including
    - improved statement numbering
    - There are now subsection markings and references to the SAML2 profile

- **Secure endpoints section**
    - Moved the OWASP reference to the footnote
    - Changed “should” to “shall”
    - The 90 day countdown period was clarified
    - annual testing by the federation operator: “The Federation Operator SHALL test each registered entity at least every 365 days. It SHOULD test when a significant change event occurs (e.g., changes in the entity’s metadata, SSL Lab changing the grading criteria, etc.)”
- **SIRTFI section**
    - Clarified the statement about SIRTFI as applied to federated single sign on
    - Added text that indicates that checking box about complying with SIRTFI acknowledges responsibility
- Albert will work on wording around informing the exec
- Wording around Health Check reports has been clarified
- **Error URL section:** A title was changed in one place

BEV2 Implementation Planning

-
    - Package I: Pre-requisite changes required for Participant Implementation
    - Package II: Additional Features / Refinements
- **Package 1**
- Focus on things the Federation operator must put in place
- Federation operator health check reports

- Federation Operator starts warnings to entities that don't meet Baseline

- **Package 2**
- Do automated scanning at scale
- Will look at endpoints, will also look at contacts

- Plan is to use QUALYS for scanning
- Need to modify backend infrastructure to mark last scan date
- Trigger scans based on
    - If entity not scanned within a year
    - If entity has been updated for certain data elements, especially endpoints updates
    - If SSL Labs has significant changes in grading criteria
    - Possibly other trigger points for a scan, such as a change to the Site Admin
- Will relax the requirement for the privacy, logo and error URLs in metadata to have 200 response code, certain other redirects will be allowed

- Future: stop the ability to register metadata that does not meet baseline
- notify and eventually, if required, remove those entities that do not meet BE
- For health checks, the goal is to create a database that can be queried, to make the process more dynamic and flexible

- Opportunity to decide carrot or stick, for health checks
- During implementation we may send targeted emails for those not in compliance
- Nice to acknowledge those in compliance, but don't want to imply they will be in compliance in future, as things can change
- There is a RACI chart, geared towards internal use, but CTAB is represented generally. CTAB is accountable for making sure BE2 is done
- Begin next week and complete before end of 2021.
- Transition date goal around July 1, 2021
- Due to pandemic, schools may be occupied with other matters
- Similar to schedule for BEv1
- If not for pandemic, possibly BEv2 would have been scheduled at slightly faster pace

Communications and Outreach

- Dean suggests we consolidate communications on a regular cadence, about every other month
- In parallel with some targeted outreach to those not in compliance
- Planning for some office hours, depending on the need

- An important milestone is online CAMP and ACAMP, November 16-20, 2020
- https://incommon.org/academy/camp-meetings/2020-virtual-camp-and-advance-camp/
- After that start the implementation phase
- Have FAQs and other materials ready at that point
- **Impact analysis**: community may not be informed about how much of a lift
- Have some of the reporting prior to finalizing
- Updating the data we have
- QUALYS SSL lab scans, we have initial report from many months ago
- Albert: we are working on the impact analysis
- We expect there may be significant lift around Error URL
- Scanning has been tricky because it takes so long to scan
- Hope to do the one time scan using QUALYS SSL
- It was noted that InCommon Steering will also be interested in seeing an impact statement

Next Steps:

- Albert will finalize the implementation doc
- Feel free to send additional comments.
- To start the Trust and Identity **consultation**, we must officially announce the opening of consultation,
- Could launch consultation on Sept 8.
  Trust and Identity Consultations

Next CTAB Call: Tuesday, Sept. 8, 2020, day after Labor Day