operationalizing-be

Background

Adopting Baseline Expectations (BE) marked a milestone in furthering trust and assurance across the InCommon Federation. For the first time, organizations within InCommon were able and expected to self-assert trustworthy operational practices for their federated entities, both identity providers (IdPs) and Service Providers (SPs). Nonetheless, assertions of this sort, however accurate and well-meaning when they are made, are prone to become stale via a number of mechanisms:

- Practices that are trustworthy at one time become deprecated as technology progresses. For example, ciphers that are considered secure today may be considered insecure next year.
- Organizations evolve and shift their practices over time. For example, work that was done on premises may be outsourced in order to save costs.
- Institutional knowledge as to how particular practices match the assertion or even that such assertions have been made may be lost due to personnel turnover.

Consequently, the InCommon Federation Community Trust and Assurance Board (CTAB) has recognized that InCommon has an interest in monitoring the degree to which the self-assertion of BEs drift over time and in aiding organizations in maintaining the accuracy of their assertions. However, the methodologies and apparatus for querying organizations and measuring assertions has to be developed *in toto*. As a result, CTAB, in consult with InCommon's Operations has developed guidelines and general methodologies for help InCommon participants maintain adherence with Baseline Expectations.

Implementation

Phase 1 - Rollout Data Collection Infrastructure

When

From November 8 to November 24, 2023

What is Happening?

InCommon Operations will introduce several data integrity detection features designed to help us detect out-of-date metadata information registered with InCommon. These include:

- contact email addresses - site admin emails as well as emails registered in the admin, technical, and security contact fields in your entity metadata
- privacy statement URL, logo URL, and Error URL - where as we previously only validated these fields during metadata submission, we can now periodically check the URLs to detect broken links

In addition, we have updated the TLS scanning process to let the Site Administrators schedule on-demand scans of their entities from Federation Manager.

We are also introducing a number of user interface improvements in Federation Manager to help Site Administrators better manage their organizations Baseline Expectations adherence.

Visit this useful guide published by the InCommon Operations team to dive deeper into what's changing.

What do I need to do?

Site Administrators: you will see an updated user interface in FM starting in mid November. The "View/Edit Entity" view adds a "Metadata Health" tab containing the latest status check results. This is also where you'll be able to initiate a TLS scan for that entity. Be sure to take a look when it becomes available.

In early November, we will send out a broadcast email ping to all metadata contacts. Since we have not historically reached out directly to these contacts, you may receive questions about that email. We are sending it to establish a baseline of where we are (i.e, how many emails are bouncing) This information will also populate the Metadata Health tab mentioned above to let you know if any emails needs updating.

Metadata Contacts: you will receive an "InCommon metadata health check" email in early November. If you are the contact for one or more InCommon-registered entities, there is no action on your part. If you are not a contact for any service, please reply to that message and let us know.

Phase 2 - Implement CTAB Recommendations to Operationalize Baseline Expectations

When

Throughout 2024

What is happening?

Once the first set of data collection infrastructure is in place, we continue on to implement the full set of recommendations made by CTAB in its Operationalizing Baseline Expectations Report. Most of these involve process changes on the InCommon Operations side to schedule regularly occurring metadata health validation, for example, a semi-annual check for URLs and email address. It also will introduce an annual attestation feature to affirm each service registered in InCommon continue to adhere to Baseline Expectations statements.

We will share more details as this next phase unfolds in early 2024.