InCommon Conducting Proof of Concept for Federated Incident Response

InCommon is conducting a proof of concept for SIRTFI (Security Incident Response Trust Framework for Federated Identity). This is the first step toward supporting a global incident response system for research and education trust federations.

With the ever-increasing and evolving cybersecurity threats, and our increasingly interconnectedness through eduGAIN, federation operators need a way to quickly collaborate in the face of a security incident. One compromised account at an institution can provide access to a multitude of service around the world. SIRTFI provides a framework for an effective coordinated response in the event of an incident.

SIRTFI stipulates preventative measures and identifies organizations that are capable of participating in a coordinated incident response. Federation participants that comply with SIRTFI are marked in the federation’s metadata, raising the bar in operational security across the federation. A very good explanation is available at https://refeds.org/wp-content/uploads/2016/02/Why_Sirtfi.pdf .

InCommon’s proof of concept involves three participants (University of Chicago, LIGO, and the National Center for Supercomputing Applications) that agree to the SIRTFI framework and have the entity attribute added to their metadata. But there are also more than 100 identity providers from other federations with the SIRTFI attribute, and InCommon participants will also see these in metadata.

Once the proof of concept has been evaluated, we anticipate encouraging all InCommon participants to adopt the SIRTFI framework. In the future, we expect this will become a requirement for federation participation.

What can you do right now? One SIRTFI requirement is to have security contacts in metadata. It is a simple process, with your site administrator logging into the Federation manager and adding a security contact. This is useful information to include, independent of the adoption of SIRTFI.