20220203 - eduGAIN Security Working Group meeting

Attendees: Casper Dreef, Davide Vaghetti, Sven Gabriel, Wolfgang Pempe, Russell Ianniello, Bjorn Mattsson, Pal Axelsson, Daniel Kouril, Nicole Harris

Notes:

Security Team to act as a SOC for alerts distribution. Work with the community to set up this service. Security Team to coordinate: monitor threats, set up communication channels.

Sven: In addition, the SecTeam has experience with vulnerability management (monitoring).

Wolfgang: Some NRENs already have CERTs and SOCs. Very useful to establish coordinated communication channels to prevent duplication of the work and simplify collaboration.

Davide: Specify the targets audience. FedOps vs security contact.

Björn: Good idea to communicate with FedOps. They already have the contact details of their entities.

Sven: Would need technical experts to play an advisory role. Challenging to collect the technical knowledge.

Davide: Scope to distribute information across the eduGAIN membership.

Björn: Create contact list with software specific technical experts?

Nicole: Does any of our tooling do any of this? Do we know what tools are being used? What is the workflow and where do you start.

Björn: I would start with: "do we know if System X is affected?". And then "do we know who else is this system?"

Davide: Start with the most common used systems.

Sven: Take a step back: what do we want to do in vulnerability management. We could provide information and advice on whether entities need to take action or not.

First: what is our scope (technologies used)?

Daniel: Decide on what to do in what order. Determine the primary needs. What are the expectations of the community.

Davide: Provide a list of options to the WG.

Björn: General mailing list. Breaking down into software specific lists.

Nicole: Point out to already existing lists and communities.

Participate in CLAW as eduGAIN

Nicole: We could advertise the event to the membership, include the federation into the scenario?

Sven: Who would participate? The Fed operators?

Davide: Depends on site of the event.

Nicole: Main event is that the network goes down. Might be worth looking at previous scenarios, training materials and toolset. Repurpose it for federation specific use. The 2021 scenario could be very useful.

eduGAIN CSIRT - RFC and ToR vote