eduGAIN Security Working Group

Meeting 18. Mar. 2021

Introduction

- The success of an operational security team depends on the acceptance of the participants.
- Key aspects for acceptance:
  - Support of the governing body.
  - Support of the parties involved in security operations.

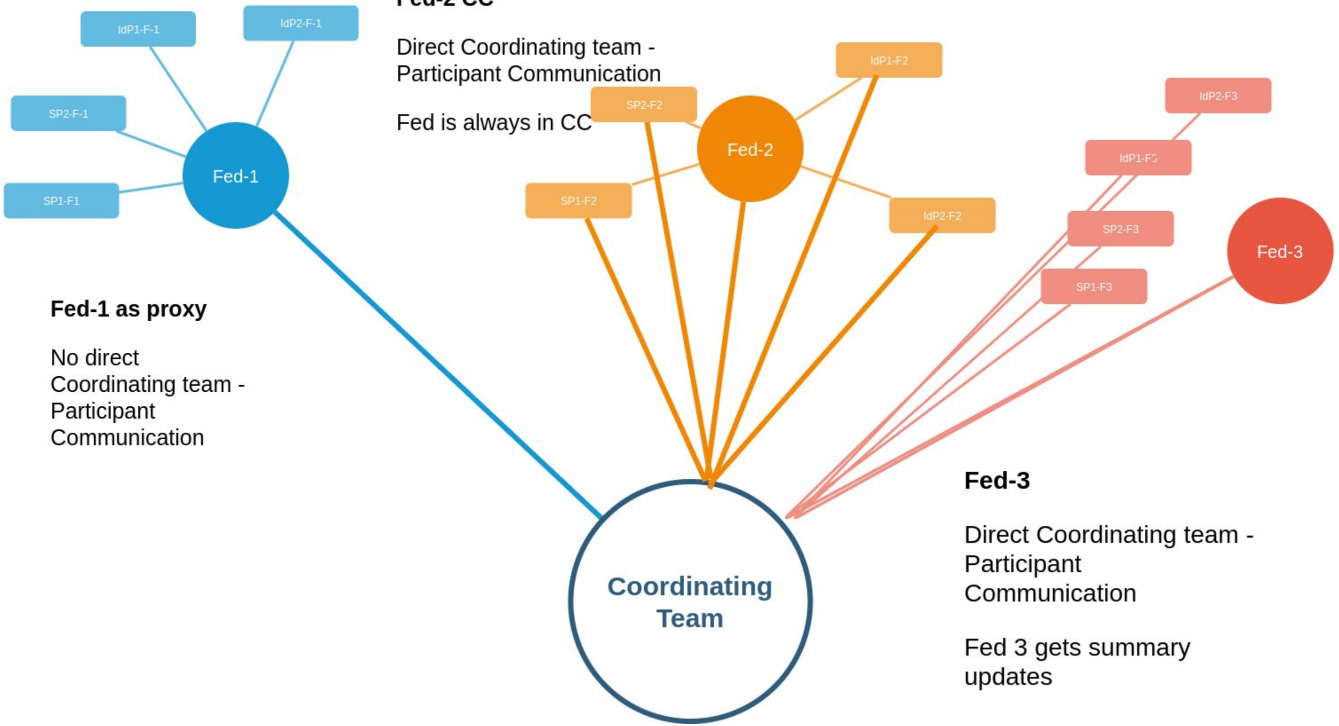
- Support is easier when you are involved in the set-up.

Operational Security in Connected Id Federations

- In Connected Identity Federations incidents are in general not isolated
    - Incident Response has to be coordinated.
    - Coordination requires communication infrastructure.
- Security Operations will affect participants
    - A team conducting security operations needs to be mandated by the governing body.
- Where to start from? Avoid headless chicken approach
    - DNA3.2-Security-Incident-Response-Procedure
    - SIR Handbook
    - Transparency: Who has which role, defines responsibilities
- Coordination of (any) activities begins with communications.

Interfederation Incident Response Coordination

Communication flow options



Fed-2 CC

Direct Coordinating team - Participant Communication

Fed is always in CC

Fed-1 as proxy

No direct Coordinating team - Participant Communication

Fed-3

Direct Coordinating team - Participant Communication

Fed 3 gets summary updates

Communication Flows Pro/Cons

- (Fed-1) All Comms through Federation
  - Pro: Reduces load on coordination team
  - Con: Delays, Point of failure
- (Fed-2) Fed in CC
  - Pro: no delays
  - Con: Channel may get noisy
- (Fed-3) Direct Comm edugain-Sec - Participants
  - Pro: Direct communication quicker, less noise for Fed
  - Con: Fed gets summary updates, may miss developments in Fed
  - Con: edugain Sec Team may need support from Fed

Comm Flows

What to implement depends on Federation, how the federation implements its role in Incident Response

- Discourage Fed-1 example.
- Fed-2 Setup is probably more robust
- Fed-3 Not ideal, in particular when a more active role from the Fed needs to be taken

Communications / mandate

- Communications should not come out of the blue
- In a crisis situation you not want to spend time on explaining who you are and why you do it.
- Have your paperwork done, in case refer to it.
- This gets more important the more distributed the participants are.
- Lets start with a mandate

Mandate, example:

The eduGAIN Security Team is a central contact and support point for security incidents, and coordinates the investigation and resolution of suspected security incidents that affect Federation Operators and Federation Participants. This includes notifying Federation Participants and Federation Operators or any other relevant entity about attacks potentially affecting them.

The eduGAIN Security Team is authorized by the eduGAIN SC to set up and test a communication infrastructure to fulfil its incident coordination task

How to get there, Action Plan

Mandate for the edugain security team:

M1: In collaboration with esWG, define the base mandate of the eduGAIN security team. This mandate shall then be updated as other action points from this plan are being completed.

Target time: Q2 2021

Towards security communication infrastructure

- CI1: In collaboration with ewSG, create the security communications infrastructure that will allow for the implementation of the Incident Response Procedure
- CI2: Provide test framework to challenge the Comm Infra on the different levels. Support Federations for inner Federation challenges. In collaboration with ewSG define the communication challenge, and approve it by eSG.
- CI3: Pending on CI2 approval, run the communication challenges.

  Target time: Q3/4 2021

Towards a formal security team

In collaboration with esWG follow standard procedures to set up a security team:

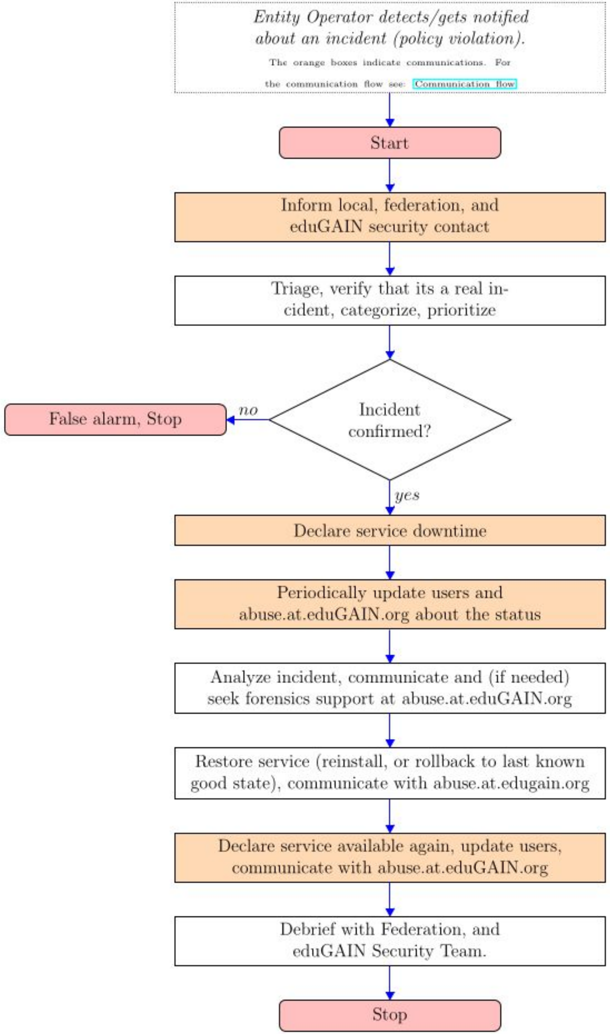
- describe team, constituency, provided services
  - develop a Terms of Reference for the security Team which will be approved by eSG.
- develop incident response procedure (also) to be followed by participants.
- develop a set of security policies that support the flow of concerted actions described in the procedure.

  These documents need to be approved by the governing body.

Questions?

Reserve stuff

IR Flowchart



Entity Operator detects/gets notified about an incident (policy violation).

The orange boxes indicate communications. For the communication flow see: Communication flow

Start

Inform local, federation, and eduGAIN security contact

Triage, verify that its a real incident, categorize, prioritize

Incident confirmed?

False alarm, Stop

Declare service downtime

Periodically update users and abuse.at.eduGAIN.org about the status

Analyze incident, communicate and (if needed) seek forensics support at abuse.at.eduGAIN.org

Restore service (reinstall, or rollback to last known good state), communicate with abuse.at.edugain.org

Declare service available again, update users, communicate with abuse.at.eduGAIN.org

Debrief with Federation, and eduGAIN Security Team.

Stop