Operational Security Update

GridPP53, 11th April 2025

Matt, for the Security Team

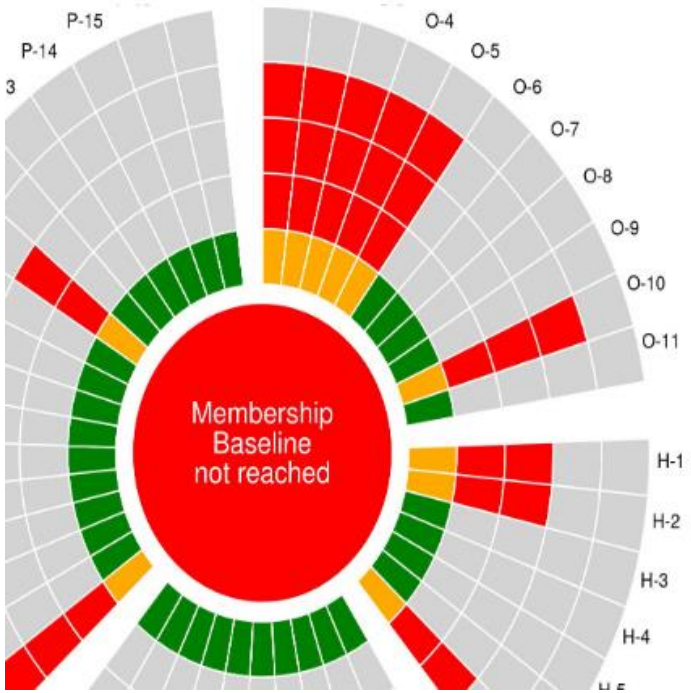
Overview

- Still great need for efforts in this area
  - No sign of this abating.
- Core team: IRIS Security, core group on forming a Duty-Rota
  - Also active in SVG, EGI CSIRT, SOC/TTT/Authz Working Groups

Plans and Challenges

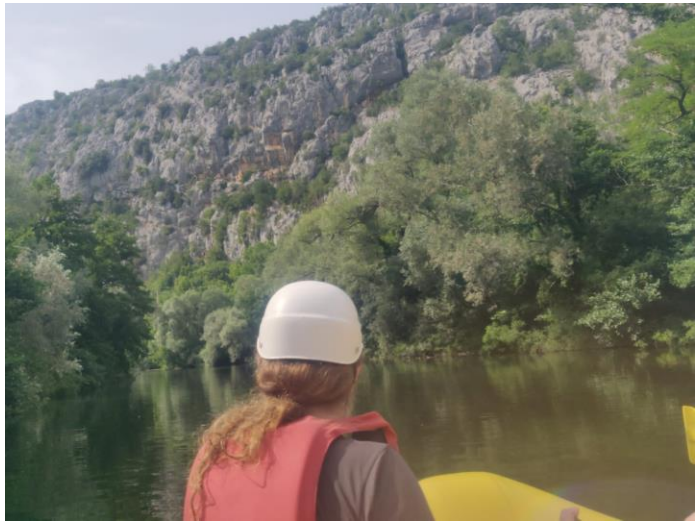
- CSIRTification plans (trailed at the IRIS meeting in December) still going ahead
  - Slower then hoped.
  - Maintaing focus on RFC2350 and SIM3
  - Aiming to have the first stage complete for the summer IRIS meeting.

- Maintaining "situational awareness" of our community and infrastructure, whilst also maintaining visibility within it.
  - Even more challenging across IRIS
- Balance that with not just becoming a source of noise.



Training and Engagement

- CERN Security School - happening this week at Coseners
- Autumn training at CERN
- We think there's appetite for security training, such as we had alongside HEPSYSMAN meetings back-in-day
  - Plenty of material available
  - What would people like to cover?
  - Whilst it would be nice to co-locate with another event it's not a necessity.



Coseners should be around her somewhere...

Vulnerabilities and SVG Activities

- In numbers, since 1st September 2024:
  - 37 reports, 17 advisories; 7 Critical, 3 High, rest alerts/advice
- Spreading the load, onboarded another "vulnerability handler"
- Documenting procedures
- Sharing of information and advisories
  - Are we getting the information to all the right places?
  - And not the wrong ones
- Continuous need to take stock of "what's-running-where" to be able to make informed decisions on relevancy
- Need to improve connections with experts
  - Future scope also depends on expert participation

Threats

- Open source and CI tools constant attack vector
  - Old hat now but the lzma backdoor is still my go-to example of concerns here. (https://en.wikipedia.org/wiki/XZ_Utils_backdoor)
- More recent examples targetting github (like this and this)

- Other threats from more classic "brute forcing an exposed endpoint".
  - Risk that LLMs makes this easier – "revenge of the script kiddie"
- A presentation on incidents dealt with by the EGI CSIRT in 2024

Comms tests and issues

- Email continues to be not as reliable as it used to be.
  - Also a moving target as new "protections" or policies are put in place.
- On the more mundane side tend to have significant bit rot in site (or VO) contact information.
- Comms challenges are here to stay as one of the only arrows in our quiver to deal with these issues.
- Experiments having defined security contacts is a good thing
  - They also had comms challenges.
- SEC01 is still the standard Incident Response procedure.

Changing landscape

- To be trailled later by Tim, there's a drift away from the straightforward DMZ/DTZ
  - Although always firewall everything anyway.
- Institutes rolling out (insisting on deploying) IDS, monitoring or other corperate solutions.
  - Tanium is a common example
  - Evidence of "slippery scope slope"
- Investment in cybersecurity – get to know your local team!
  - And make sure you have their contact details to hand in your hard-copied emergency contact and information pack.
    - You do have one of these, right?

Various types of SOC

- Continued work within SOC WG.
  - Presentation at ISGC
  - Hackathons
  - Training (CERN School module)

- Deployment of SOC at RAL
- Lightweight/easier to deploy alternatives, such as pDNSSOC, PocketSOC
- Information sharing with MISP
- Ways of alerting on IOCs* within a site's "regular" monitoring

*Indicator(s) of Compromise

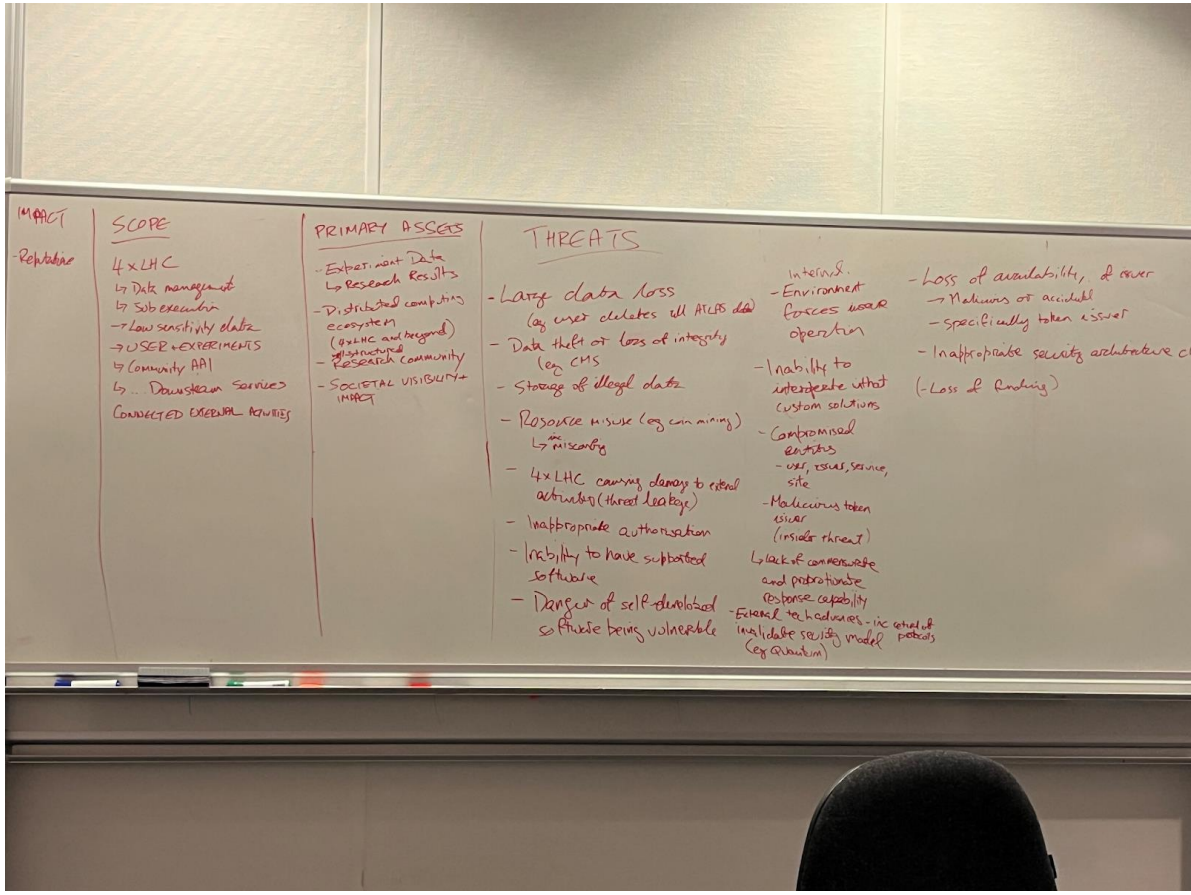
Certificates and Tokens

- TCS shake up from last year worrying
  - Motivation not to move away from escience certs to a commercial solution
  - Alternatives?
- Wide move to shorter lived certificates.
  - Require automated renewal processes
- Many aspects of Tokens still a work in progress
  - Still operational questions
  - Work on best practice
  - TTT
- A little too regular issue comes from tokens are easy expose.
- Debate over lifetime, scope
- Technical issues with accounting
- Revocation question?
  - Some kind of Argus like service for tokens? TRLs?

Still very much in a transitional phase

Assessing Risks

- Risk Assessment is an essential area
- Need to update the WLCG Security Risk Assessment, in part to reflect the move to tokens from x509
  - Suggesting of an accompanying code review of token components
- At TIIME last week work on a high level risk assessment for token based infrastructures was started.
  - Primary assets indentified, sorting through threats and risks.



Summary

- "CSIRTification"
- Training
- Threat awareness, Information dissemination and "contactability"
- SOCs
- Certificate and Token Evolution
- Risk Assessment

Luna's relaxed as all her systems are secured.