IRIS Security: Status and Evolution

Matt, for the IRIS Security Team

The Security Landscape

- The Cybersecurity Threat Landscape is a high as ever.
- Cybersecurity is an increasing management concern across institutions and organisations.
- A need to adapt the IRIS Security Team to meet any coming challenges and the expectations of working within the cybersecurity sphere.

Recent and Current Activities

- The Security team is comprised of members from across the IRIS providers.
  - On duty portion from members of the Grid team.
- Engaged with many communities and activities.
  - Completion of CAF at the RAL Tier 1
  - EGI Software Vulnerability Group
  - EGI CSIRT
  - SOC WG, including the development and rollout of pDNSSOC
    - Interest in adopting pDNSSOC at GridPP sites (more next GridPP))
  - DRI Cybersecurity
- Primary engaged in the sharing of information among members.

Recent and Coming Events

- Jisc Security Conference - last week
- European SOC Hackathon - this week!
- DRI Security Breakout at CI:UK – also this week
- TIIME – in Reading
- CERN Security School hosted by STFC at Coseners House
  - 6-12 April, applications hopefully opening before Christmas
  - Previous iteration
- TNC25 - in Brighton

Security Team -> CSIRT (or CSIRTification)

- Over 2025 we plan to evolve the Security Team's into a Professional CSIRT
  - Computer Security Incident Response Team
  - This is planned to be a "**Coordinating** CSIRT"
- This change require (non-exhaustive list):
  - A firm mandate
  - An uplift of capabilities
  - Definition of roles and responsibilities.
  - Professional Recognition of the above

Becoming a CSIRT

- We can't just change our name, print T-Shirts and start poking our noses into security incidents.
  - A set of standards need to be met.

There are resources we can use and processes we can undergo to provide a framework to build our new CSIRT on.

- **RFC2350**, "Expectations for Computer Security Incident Response", from which we write a CSIRT "description document".
- The Open CSIRT Foundation's **SIM3** (Security Incident Management Maturity Model) Self Assessment

RFC2350

A long standing document defining the capabilities and qualities a Security Team needs to have to consider itself a professional CSIRT.

- Some of these are simple, such as defined membership, contact details, documentation location...
- Others are not as easy to defined, such as mandate, service expectations...

The RFC provides an outline template for the CSIRT's description, the process of completing this informs us of our next actions.

RFC2350 CSIRT Description Template

1. Document Information

1.1 Date of Last Update

1.2 Distribution List for Notifications

1.3 Locations where this Document May Be Found

2. Contact Information

2.1 Name of the Team

2.2 Address

2.3 Time Zone

2.4 Telephone Number

2.5 Facsimile Number

2.6 Other Telecommunication

2.7 Electronic Mail Address

2.8 Public Keys and Encryption Information

3. Charter

3.1 Mission Statement

3.2 Constituency

3.3 Sponsorship and/or Affiliation

3.4 Authority

4. Policies

4.1 Types of Incidents and Level of Support

4.2 Co-operation, Interaction and Disclosure of Information

4.3 Communication and Authentication

5. Services

5.1 Incident Response

5.1.1. Incident Triage

SIM3

In many ways we can consider RFC2350 as setting an almost minimal foundation for a new CSIRT.

- A good baseline, describing what we have

The OpenCSIRT Foundation SIM3 assessment tool provides a process to gauge how well "equipped" a budding CSIRT is.

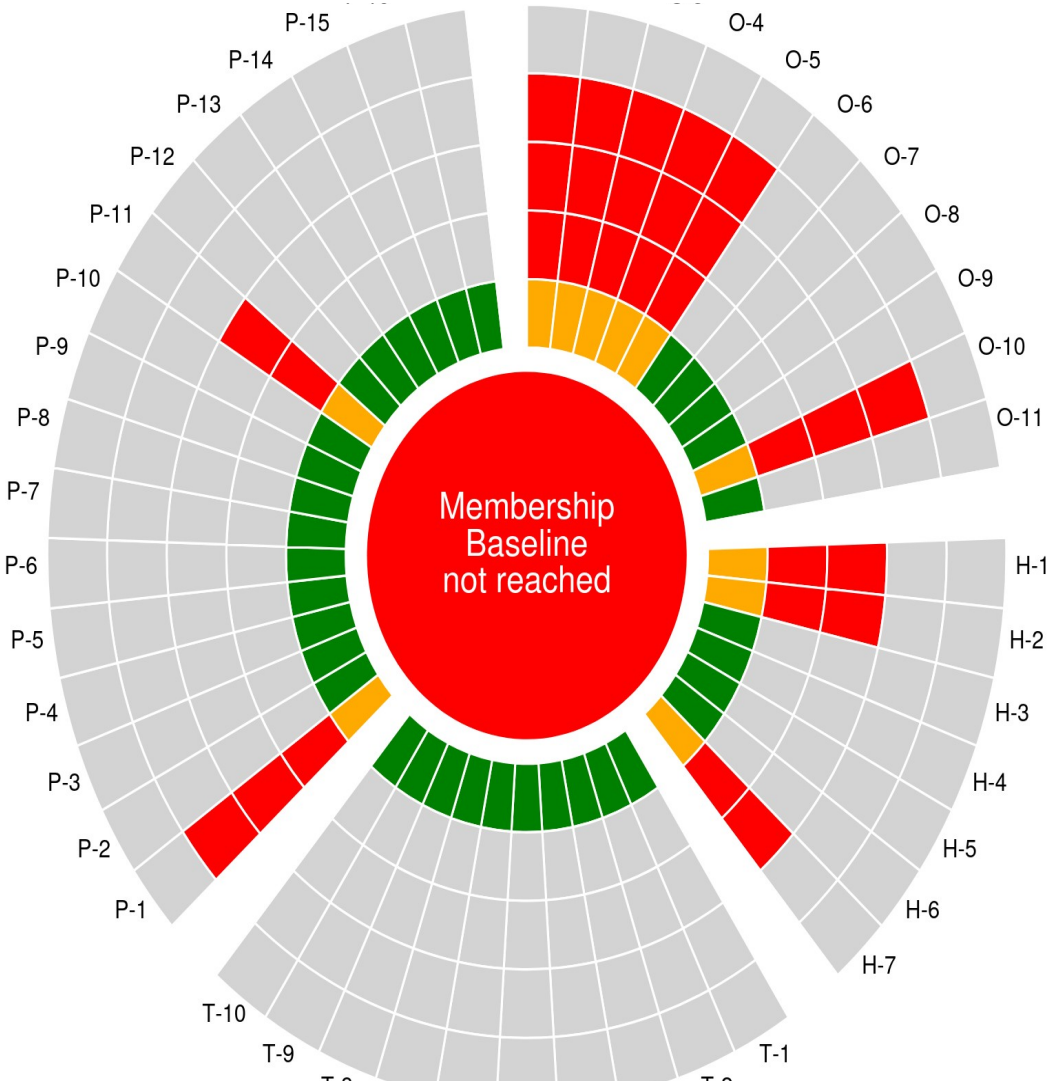
The model is built around four pillars:

- Prevention
- Detection
- Resolution
- Quality control & feedback

Within four independent assessment quadrants:

- O - Organisation
- H - Human
- T - Tools
- P – Processes

Assessments are rated from 0-4.



SIM3 Quadrants

Organisational:

Examples – Mandate, Constituency, Public Media Policy.

Tools:

Examples: Information Source Lists, Resilient Comms and Infrastructure

Human:

Examples – Staff Ethics, Resiliency, Development

Processes:

Examples: Escalation procedures, Incident Prevention/Detection/Response, Auditing.

Plans and Outcomes.

- Process over the start of 2025 where we look at the requirements and identify where we fall short, and what we need to do.
- Then backport these needs.
- Identifying and providing the training for the members of the new CSIRT.
  - The recommendation is at least 3 individuals, although not 3 FTEs.
- Once the team is assembled and equipped, a process of gaining recognition of the team as a full fledged, professional CSIRT

Wrap Up

- To realistically meet the needs to respond to a cybersecurity incident affecting the IRIS community the Security Team needs to evolve its capabilities.
- We have the processes we need to undergo in order to identify our needs for achieving this evolution.
- More next IRIS meeting!