GridPP Security Status

On behalf of the IRIS Security Team

GridPP52, Ambleside

Since GridPP51

- Threat level still high.
    - This is the minimum, the world isn't getting any less hostile.
- CentOS7 EOL has passed.
- No major incidents at UK Grid sites.
- Ever growing awareness of the importance of Cybersecurity across institutions and infrastructures
    - This is a good thing, but there's a need for it to be nurtured in productive directions.
        - Temper with good Risk Assessment and Management.
        - A need to have pre-prepared "answers" to the the most-likely-to-be-asked questions.

Incidents in the News

- 2023 British Library incident final report
- From last year; HZB attack knocking out light source operations
- Academic DDOS incidents in February
- June's Synnovis attack (the one affecting blood test results)

Many of these are "data theft and ransom" style attacks, but the British library noted extensive "digital vandalism" to their infrastructure.

A reminder of who's who, what's what.

- IRIS Security Team
  - security@iris.ac.uk - with a core backup rota populated by GridPP folks
- EGI CSIRT
  - abuse@egi.eu - the contact point for suspected grid incidents.
  - Joint F2F at Coseners in October
- Software Vulnerability Group (SVG)
  - more on this later.
- AAI Teams and WGs (AuthZ, TTT, GUT)
- Security Operations Centre (SOC) WG
- DRI Cybersecurity

Strong involvement across all these groups.

DRI Cybersecurity Workshops

- The first DRI Cyber Security workshop was hosted at Coseners in April.
  - Organised by David and James
  - Strong involvement from GridPP and IRIS.
- This first meeting focused on Strategy.
  - The next, planned for ~November, will focus on Technical solutions.
- Meet twice a year, with the themes alternating between these two focuses.

OS points

- (Anecdotally) Alma and Rocky appear to be conducting themselves well wr.t. security updates.
  - Alma have made use of the fact they're no longer "downstream" of RedHat to deploy (some) patches (slightly) early.
  - Rocky seem to be keeping up, releasing patches in a timely manner.
    - Issues with errata pages not always documenting patch details
- End of EL7 brought about the end of ARGUS, others.
- No concerns about large amounts of resource still on CentOS7 in the UK.
  - Congrats to everyone on a job well done.

Containerisation and Network Exposure

- Containers have become the de facto distribution system for many products.
- Docker et al are notorious for being "clever" and poking holes in your meticulously crafted host firewall.
- Widely known that Docker daemon and its equivalents should not be exposed to the internet – but many sites are wholly within a DMZ/DTZ - outside of the institution's protections.
    - Need to form new, clear guidance and/or mitigation (like keep your containers up to date).
    - Containerisation isn't the only motivator for this, general good practice to reduce service exposure where you can.

Vulnerabilities

- Still depressingly familiar phrases among the Linux vulnerabilities we see.
  - If we had a pound for every mention of "Use after free".
  - Although we haven't had a netfilter CVE for a while…
  - But optimism there countered by regreSSHion (CVE-**2006**-5051)
  - And the LZ backdoor attempt (CVE-2024-3094), so many lesson to be learned there.
- "CPU architecture" vulnerabilities are still common
  - Hitting AMD as well as Intel (e.g CVE-2023-20569, aka INCEPTION)
  - Extra concerning as we tend to run very old CPUs that might not see a microcode patch to a newly discovered issue.

EGI Software Vulnerability Group (SVG)

- GridPP continues to lead the EGI SVG
- Less changes to report than at GridPP51
  - People seem O.K. with the updated advisory style which we have been using for a year
- Less progress on procedure and getting more people involved than we would have liked
  - Scope depends on participation
  - But we do have one new active member
- In process of better documenting what we do
  - And updating documentation and web pages generally

Some numbers – 27th March to 20th August

- 25 Potential Vulnerabilities reported
- 12 Advisories sent
  - 3 Critical risk
  - 7 High risk
  - 1 Heads Up
  - 1 Alert
- 3 more which were reported and discussed mentioned on EGI CSIRT web page.
  - Decided against sending info to all sites
- Advisories when public now on advisories.egi.eu

SVG Plans

- From the IRIS Workshop – looking at the idea of an IRIS group to share information on vulnerabilities beyond GridPP
  - We are now sending the advisories to a new IRIS-Vulnerabilities list
- Update and revise procedure
- Looking at possibility of making advisories available on-line when AMBER (possibly through confluence)

And…

- If you find a vulnerability (whether one you discover yourself or read about) which you think is relevant/serious in GridPP
    - Report it to Report-vulnerability at egi.eu
    - Someone else may not have found it or reported it.
- If you are interested in being involved in SVG (looking at vulnerabilities, how they affect distributed infrastructures) contact SVG

Security Plans between Now and GridPP53

- Update guidance for networking exposure.
  - Dedicated containerisation best practice docs.
  - Couple with a general improvement of our documentation.
- Be mindful of the continued transition to tokens.
  - Provide support and guidance as needed.
  - Any impact of the loss of ARGUS?
- Continue plans for expanding the capabilities of the Security Team
- An update to IRIS (and by extension GridPP) Security Strategy and Policies
  - Using the NCSC Cyber Assessment Framework (CAF)
  - This will inform future guidance given to sites.
    - See David's update at the July IRIS meeting for more details.

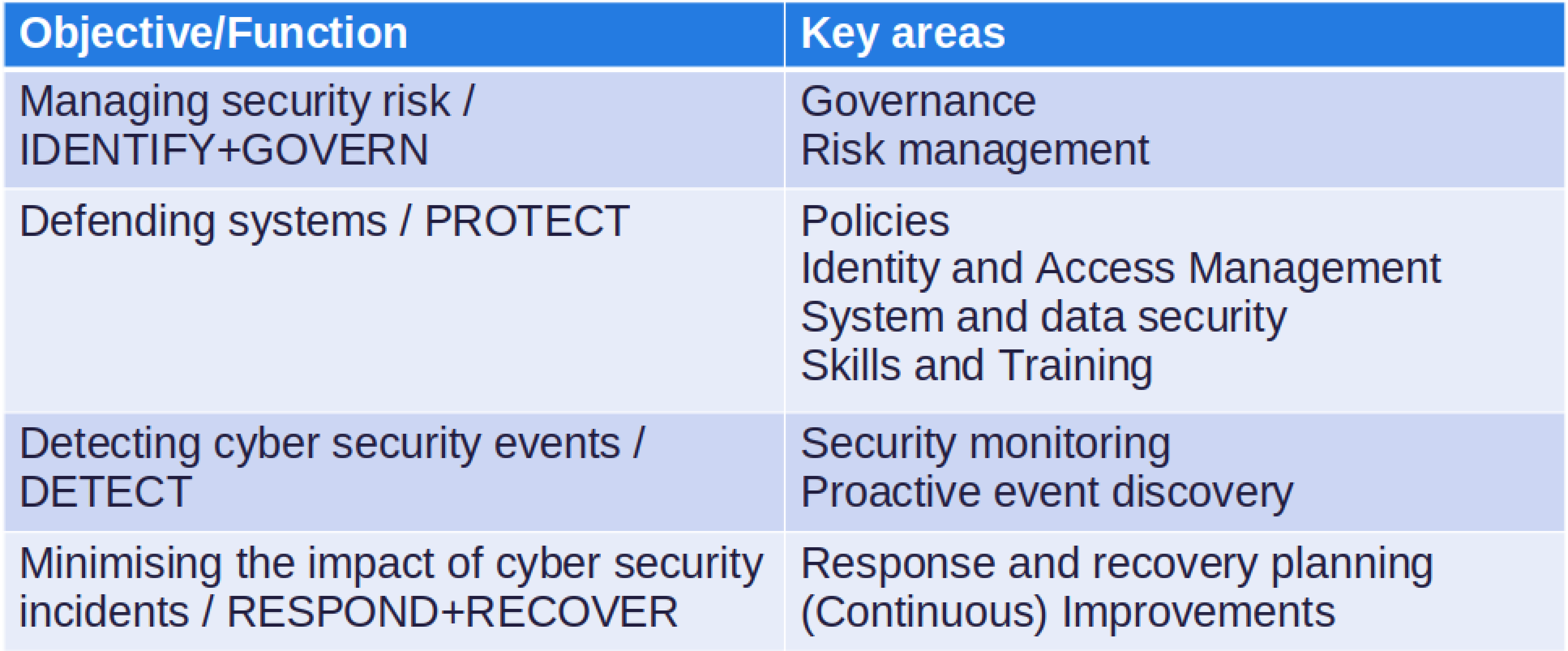
Inventory and Assessment

- Part of forming any Cybersecurity strategy is Assessing Risks, and the start of that process involves taking Inventory.
- Need to "take stock" in the UK of sites and their infrastructure.
  - What's running where.
  - Much of this information is in the gocdb, but not all.
    - There's a side conversation to be had with the gocdb devs about adding in extra information, for example batch system type.
    - But not all information will find a good fit for a database.
- This is part of a larger push within IRIS (and beyond) - although we are in a good position.

FIN

- Any questions?

Bonus Slide: CAF objectives



Objective/Function	Key areas
Managing security risk / IDENTIFY+GOVERN	Governance Risk management
Defending systems / PROTECT	Policies Identity and Access Management System and data security Skills and Training
Detecting cyber security events / DETECT	Security monitoring Proactive event discovery
Minimising the impact of cyber security incidents / RESPOND+RECOVER	Response and recovery planning (Continuous) Improvements