EGI CSIRT SSC
or
Distributed Incident Response

Agenda

1. What to expect in the exercise
2. What are the goals?
3. What are the channels?
4. What should sites do/not do?
5. What are the arrangements if this happens during GridPP?
6. What will the Security team do?

What to expect

- The structure of this exercise is similar to before:
- Activity will increase in participating sites until enough (read: more than 1) report it to the CSIRT, at which point the exercise proper begins
- The EGI CSIRT Security Officer on Duty will then coordinate the overall incident, supported in the UK by the GridPP/IRIS Security Team

What are the goals

- The **key** goals of this exercise for all participating sites are

  1. initial feedback: 4 working hours
  2. found malicious job/processes/stop them: 4 working hours
  3. ban problematic certificate: 4 working hours
  4. contain the malicious binary and sent it to the incident-coordinator: 24h

- See https://confluence.egi.eu/display/EGIBG/Security+challenges

What are the goals

- The **optional** goals of this exercise for all participating sites are to perform forensics beyond these goals. This will be tracked in a CTF format where sites should form a team per site if they wish to be involved.
- I encourage people to get involved, but this is optional, we do not expect everyone to have deep forensics capabilities
- But this could help if this is something you want to develop
  - And helps us (EGI CSIRT) know where the forensics capabilities are

- See https://confluence.egi.eu/display/EGIBG/Security+challenges

What are the channels

- Contact from the CSIRT will be via email to site-security-contacts and/or the raising of individual tickets, which will be sent to the contact identified in GOC DB
  - We have recently tested that everyone should receive tickets
- For GridPP internal discussion:
  - security-discussion@jiscmail.ac.uk is already in place and is available for discussion **as long as** you also respond to the CSIRT directly
  - GridPP Mattermost Security channel: we are adding people now, but can always add people as we move forward
- I intend that these channels will remain in place for this purpose after the exercise.

What should sites do?

- If you see something suspicious (this is always true!) contact abuse@egi.eu and cc security@iris.ac.uk
  - This exercise is self contained so we will not be including other parties. If you want to inform your local security of an exercise, please do so **marking it as an exercise**, or mark up in comms with the CSIRT that you would have done this

- If you want to share something on one of the security channels please do so, **after** doing the above

- The Security Team will monitor the security channels and encourage people to make sure they have talked to the CSIRT

What should sites do/not do?

- Do **not** discuss security matters on TB-SUPPORT. It has public archives and is not an appropriate place to discuss security.

- Do **not** block an entire VO **during the exercise**
  - if you feel the urge to do so, mark up in an email to the CSIRT that you would have taken this step

- Use the GridPP Security channel for live chat; it's not a good place to record information

- Contact with the VO is the role of EGI CSIRT; I expect sites to communicate directly with them, not with the VO
  - Otherwise we could end up with hundreds of sites contacting the VO and comms would be a mess

What are the arrangements during GridPP?

- For Tuesday/Wednesday morning/Thursday we have an extra room (The Quiet room I think) which will be available as an incident room to gather and compare notes
- Wednesday afternoon this will be used as an overflow from the main meeting

What will the GridPP Security Team do?

- Monitor communications; prompt sites if we don't hear from you following a ticket
- Monitor security-discussion/GridPP Security and help coordinate information
- Monitor TB-SUPPORT and politely redirect people ☺
- During GridPP, arrange status/catchup meetings in the incident room as appropriate; this could also be used by those involved with forensics
  - While the CTF does have a scoreboard, I'm extremely fine with helping each other out
- These arrangements will probably be announced on the Mattermost channel

Final thoughts

- These exercises will involve some stress given the type of exercise and the fact that there are time constraints
- BUT the key elements are around communicating with the CSIRT when prompted; lean on them and the Security Team and other sites
- Some things will go well, others will identify areas needing development; this is to be expected