Collaborative Security

David Crooks

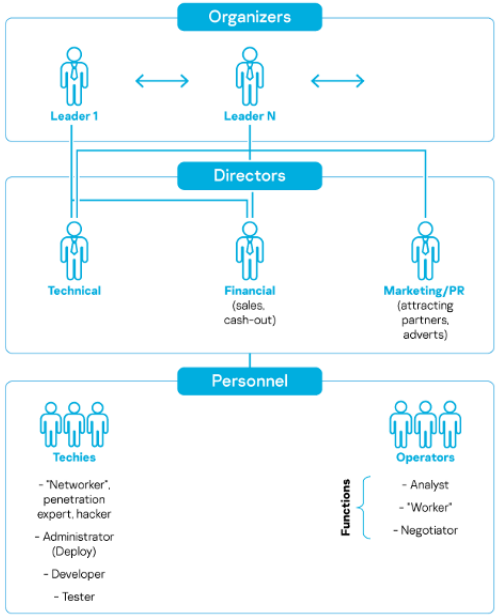
EGI CSIRT

david.crooks@stfc.ac.uk

Landscape

Landscape: the world has changed

- In the past, biggest risk for academic security
  - Relatively simple, untargeted attacks
  - Belief that research computing was major risk
- This is no longer the case
  - Determined, well-resourced attackers
    - **9-5 jobs** working on malware services
  - Phishing and identity theft are major risk
    - Research computing security can be **major asset**
- Big business: we are targets



kaspersky

https://securelist.com/russian-speaking-cybercrime-evolution-2016-2021/104656/

Impact

- In our community (research and education) we are faced by determined attackers
- The impact of successful attacks can be **catastrophic**
- **Months** of site/facility downtime
- **Major** reputational and financial damage

The approach

- We **must** collaborate
- Threat intelligence
- Facility capabilities

Threat intelligence

- Threat intelligence is the collection of indicators that can identify a particular attack

- We **must** actively share this within the EGI infrastructure

Threat intelligence

- EGI CSIRT is developing procedures to use the MISP platform to share this intelligence
  - In addition to existing emails to site-security-contacts

- API allows systematic integration with existing tools
- Live update of incident indicators of compromise
- Opportunity for facilities to augment in real time

Facility capabilities

- We have an active source of intelligence
  - what next?

- We need to understand what is happening in our networks

Large facilities

- For large facilities (>~100Gb/s and above)
  - **HTC**, **HPC** and **Cloud** facilities
- Fine-grained deep packet inspection at facility/organization perimeter
- Capabilities most impactful at highest level possible in organization
  - Requires strategic approach with upper management

Small facilities

- For small facilities, two approaches
  - **HTC**, **HPC** and **Cloud** facilities
  - Fine-grained deep packet inspection at facility/organization perimeter
- Virtual deep packet inspection monitoring nodes
  - Suitable for ~< 10Gb/s throughput
- Passive DNS
  - Work ongoing to gather passive DNS information which can be analysed at central nodes
  - Led by Romain Wartel (WLCG Security Officer): welcome contributors

What's next?

- EGI CSIRT is developing procedures to share threat intelligence
- Identify large facilities that would benefit from organizational level monitoring
- Develop (virtual) sensors suitable for smaller sites
- Step change in our network visibility, coordinated through existing security team

Contacts

- If you would like to **participate** in this work or
- If you have **existing** monitoring capabilities and would already like to integrate threat intelligence

- **Please get in touch!**
  - david.crooks@stfc.ac.uk

Questions?