Security Incident Handling

NDGF AHM Spring 2025

First aid

- Stop the accident
- Asses
- Call for help
- Perform Aid

Cyber incident response lifecycle

1. (42) DON'T PANIC – Get a cup of favourite hot beverage (and a towel)
2. Triage – capture data,verify, analyse
3. Communicate
4. Acquire and document evidence
5. Contain/mitigate
6. Eradicate
7. Recover
8. Review

Caveats

- Order may be influenced by
  - Skillset
  - Regulation: EU/national laws, institutional rules, federation i.e. wlcg/egi
  - Trust
  - Goal: preserving evidence vs recovery

NDGF specific

- https://wiki.neic.no/int/Security
- documents.egi.eu/public/RetrieveFile?docid=710&version=3&filename=EGI-Procedure-CSIRT-710-V3%20.pdf – see chapter 4

Triage

- Document- log actions and timestamps
- Verify (non invasive)
  - Analyze indicators
  - Correlate
  - Research
- Prioritize

Communicate

- Know who to contact: organization, government, federation
- Clear communication
  - TLP
  - PAP
- NDGF: Chrulle and Ville @ csirt@ndgf.org
  - Ping in rocket
  - No answer in time: Call Chrulle (see the wiki or GocDB for phone no)

DFIR 1

- Prioritize volatile information
  - Memory
  - Disk images
  - Network
- Plan how to get the data
  - Do not trust the system
  - Try to use shared memory or direct to network
  - How are you logging in?
- Gather tools – static binaries are your friends

Contain

- Shut the machine down?
- Block the network?

Eradicate

- Mitigate all vulnerabilities that were exploited
- Remove malware etc.
- Affected accounts? Infrastructure? API(Cloud/AD)?

Recover

- Return to production
  - Consider wiping and reinstalling/recovering from backup
- Confirm
- Implement additional monitoring
  - Did you find C2 servers? Make sure you monitor

Review

- Lessons learned
  - Operational procedures, backups, vulnerability management
  - Incident response
- Report
  - Mgmt
  - GDPR
  - Law inforcement

Bonus 0^{th} step

- Like the 0^{th} law of robotics: the most important

Preparation

Exercise

- Incident response (not RE, DFIR)
- “Simple” incident
- 4 teams (one qemu VM each, one communicator each)
- Pretend VMs are physical machines
- Web app is synthetic, because of time limit.

    Not part of it: gencache.sh

Pool Tarp Federation