EGI-CSIRT
Operational Security

Daniel KOURIL, CESNET, EGI-CSIRT
Sven GABRIEL, Nikhef, EGI-CSIRT
Vincent BRILLAULT, CERN, EGI-CSIRT

Activity update

EGI-Engage is co-funded by the Horizon 2020 Framework Programme
of the European Union under grant number 654142

Cloud Incident EGI-20160509 – Lessons Learned

- Forensic investigation done quite quickly,
- Communication to FedCloud sites and configuration service took additional time
- FedCloud sites are exposed to “normal” Internet attacks
- Successful attacker tend to keep working for long time
- New services may easily introduce new threats

FedCloud Incident: EGI-20160509-01

Incident Prevention: VM-Endorsement/Contextualisation

VM-Endorsement

- Concept: Users start from a ”save” image.
- Policy developed, roles defined, etc, see https://documents.egi.eu/public/ShowDocument?docid=771
- Contributions from experts of various sites (incl. FedCloud)
- Discussion on technical issues like: non repudiation of the endorsement process, cryptographic signing of VM images etc.
- This is **expensive!** Multiple experts involved in creating/checking/maintaining Endorsed VM-images.
- This is very useful for a use model where VM end-users can not change the VM (examples: VO crafted WNs)
- It breaks when end-users get root and can install software/change configurations. Example: Contextualisation

VM-Contextualisation

- Concept: Circumvent the limitations the VM-Endorsement imposes on Cloud usage.
- Very easy, cheap, just grab a random fabric management system and create your own grid in FedCloud.
- Problem: No security what so ever (incl. access control, monitoring etc etc.)
- Violates at least the gist of the VM-Endorsement and other EGI security policies

How to proceed

- VM-Endorsement concept makes sense in a certain use model
- FedCloud has not yet described a use model, so we can not create a security model, besides
- . . . something like ”Security groups” as in Amazon’s EC2
- needs a technical discussion with the providers, if this is feasible.
- would provide flexibility for the end users and response possibilities for the (Site-) Security teams.
- a well tested concept.

NGI Argus Servers Monitoring Update

- Hosting change for the nagios server used by EGI CSIRT

→ New certificate used by the argus probe

→ New ACL needed on NGI Argus

- (Please also keep the old one for now)

NGI Argus Servers
New ACL for monitoring

- What?
  - For:

    `CN=secmon.egi.eu, O=Greek Research and Technology Network, L=Athens, ST=Attica, C=GR, DC=tcs, DC=terena,DC=org`

  - Rights:

    `POLICY_READ_LOCAL|POLICY_READ_REMOTE|CONFIGURATION_READ`

- How?

```
pap-admin add-ace "CN=secmon.egi.eu, O=Greek Research and Technology
Network, L=Athens, ST=Attica, C=GR, DC=tcs, DC=terena, DC=org"
"POLICY_READ_LOCAL|POLICY_READ_REMOTE|CONFIGURATION_READ"
```