Security Groups progress and plans in the changing EGI environment

Security Operations

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

EGI-CSIRT
Cloud Security

Sven Gabriel

EGI CSIRT FedCloud collaboration, a timeline

- EGI Federated Clouds F2F meeting 13/14 Jan 2014, Oxord, UK
  - Get started / FedCloud Use/Security Model ?
- EGI Conference on Challenges and Solutions for Big Data Processing on Cloud, 24 – 26 September 2014
  - Results / Evaluation CRP Questionnaires
- EGI Federated Cloud - Face to Face workshop, 19 – 21 Jan. 2015 Amsterdam
  - Use/(Security) Model presented by FedCloud
  - EGI-20141024-01 FedCloud incident at CESNET
- Advancing the EGI Security infrastructure, 18 – 22 May 2015 EGI-TF Lisbon
  - NGI-CZ - CESNET-MetaCloud EGI-20150514

Cloud Security / Pass Security Tests vs Secure your Infra

- Certification of CRPs, really ?
- VM Endorsement, of course, where do I have to click.
- Will checks/tests help in the certification process?
- VW Case, Golden WNs, tweaking security probes: check successfully passed, but . . .

Cloud Security

- Let FedCloud find out what there users want.
- Support FedCloud in distilling what there users need.
- Support FedCloud in building an Infra that can serve this purpose.
- There are similarities in building security in FedCloud with: https://youtu.be/LVJ0edTBogU
- although its fun . . . we probably should use a different approach.

Incident Response

Vincent Brillault

IRTF operation May-Oct. 2015

- Rewriting vulnerability handling policy (SEC03)
- 137 critical vulnerability cases (libuser: 103)
- 5 site suspension (vulnerability: 3)
- 3 security incidents

IRTF incident: EGI-20150515-01

- VMI/VA with weak root SSH credentials
- 2 instances in 2 different sites compromised
- Demonstrated weaknesses in FedCloud:
  - EGI CSIRT cannot disable VMI/VAs
  - Hard to locate running instances and check/stop them

IRTF incident: EGI-20150611-01

- Exposed non-patched Elasticsearch servers compromised
- 2 instances in 2 different sites compromised
- Issues with new/hyped technology?
  - Using *standard* technology: exposed to *standard* hacks
  - No experts/not supported by EGI SVG, no monitoring

IRTF incident: EGI-20150925

- Root compromise, SSH trojan
- Multiple server in 1 decommissioned site, 3 other
- Credentials to 2 other sites exposed (not exploited)
- Grid certificates exposed (not exploited)
- Important to collaborate outside EGI:
  - What about *decommissioned* UIs ?
  - Shared users: can easily expand (didn't start at site)

IRTF future

- Policy refreshing:
  - SEC01 : Rewrite in Wiki format, update for cloud
  - SEC03 : What about vulnerabilities in VAs?
- FedCloud security: better tools needed (instance identification, instance/user *suspension*)
- Increase collaboration with VOs (Cloud *Sites* admins)

Security Monitoring

Daniel Kouril

Overview of security monitoring in EGI

- Detection of security weaknesses
- Improvement of incident response
- Integral part of EGI CSIRT activities
  - Regular monitoring of infrastructure
  - Certification of sites
- Several key services involved
  - Pakiti
  - Nagios (secmon)
  - Security dashboard

Activities

- Regular activities
  - Operations of tools
  - Certification of sites
  - Support of user, EGI CSIRT, . . .
- Development
  - Improvements to tools
  - Improvements to presentation layer (security dashboard)
  - Focus on clouds
- Plans
  - Metrics, reporting, less manual work
  - FedCloud VA assessment

Security assessment of cloud VA's

- Automated framework to detect common flows
- External and internal checks
- Discussions about integration with AppDB
- Pilot implementation being finished at CESNET
  - https://github.com/CESNET/secant