EGI CSIRT:RFC 2350 3.1. Mission Statement

The mission of EGI-CSIRT is to co-ordinate the resolution of IT security incidents related to their constituency (see 3.2), and to help prevent such incidents from occurring.

- EGEE / EGI
  \(\approx 12\) ROCs \(\rightarrow\) 39 NGIs/471 RCs
- Project wide coordination of operational security activities.
- Interfacing to other (Grid/NREN/VO) CSIRTs
- EGI-CSIRT central tasks, security activities coordination

---

**EGI-CSIRT**

Members: NGI-Security-Officers

- Security-Monitoring Group
- Security-Drills Group
- Incident-Response Task Force
- Vulnerability Assessment
- Training Dissemination
Training and Dissemination
Training and Dissemination

- Defensive
  - You are an admin of a small infrastructure under attack: Solve the incidents, protect your infrastructure
  - 2 Days course with lecture on battlefield forensics / or 0.5 day, offline forensics, analyse an image

- Offensive
  - Kypo [http://www.kypo.cz](http://www.kypo.cz): Framework to simulate IT infrastructures (incl. network) for training purposes (Monday 18. May 13:30, you have not missed it, right?)
  - Mission: Attack this infrastructure with standard methods…
Incident Response in EGI

EGI CSIRTs Incident Response Task Force
Incident Response in EGI

Impossible task:

- 50+ different jurisdictions
- Sites are independent – very little centralized power
- Sites range from big national facilities to small underfunded departmental systems.
- **Since 2014 19+ sites in EGI-FedCloud**
- Sites are usually already in the constituency of some other CSIRT.
Incident Response in EGI

What do we have:

- High level policies give a framework to operate in.
- Last resort – suspension. Follow the rules, or you can’t be in our club.

This worked for the Grid,
Incident Response in EGI

What do we have:

- High level policies give a framework to operate in.
- Last resort – suspension. Follow the rules, or you can’t be in our club.

This worked for the Grid, in the Cloud it gets blurry, here we need a good portion of ”Good will” from the sites. . . :

- to operate within the policies framework
- to pro-actively sharing incident information (or at minimum as the IR policy requires)
Incident Response in EGI

.... blurry: site provides cloud services sharing the same infrastructure resources among diverse communities

http://venom.crowdstrike.com/
Incident Response in EGI

IRTF members serve as EGI Security Officer on duty, on a weekly rota.

- Handle incident reports
- Keep an eye on monitoring
- **Keep things falling between chairs**
Incident Response in EGI

How to monitor the security status of the distributed sites?

Realization: we have an infrastructure to run computation jobs! Use that also for monitoring.

- What to look for? ... Vulnerability Assessment 13:55 - 14:10 Linda Cornwall (STFC) SVG
- How to get Monitoring Data in a usable format, to the right people (ACLs) ...Security Monitoring 14:10 - 14:20 Daniel Kouřil (CESNET)
Incident Response in EGI

- Check for sites running software with CRITICAL vulnerabilities (EGI-SVG assessment).
- This whole exercise is mainly about to prevent local privilege escalation (getting root)....
- (Getting root is also on un-patched systems an extra step, its easier to log in as root right away :) )
Incident Response in EGI

- What happens when we get an incident? (This implies that we get notified about incidents in first place.)
- What *is* an incident?
Incident Response in EGI

- What happens when we get an incident? (This implies that we get notified about incidents in first place.)
- What is an incident?

An [grid] incident is any real or suspected event that poses a real or potential threat to the integrity of [grid] services, resources, infrastructure, or identities.

Anything can be labeled a grid security incident if you feel like it! (This is where you need to be pragmatic...)
The EGI incident response procedure is brief, but establishes a flat structure with maximum info sharing.
Incident Response in EGI

The EGI incident response procedure is brief, but establishes a flat structure with maximum info sharing.

When a security incident potentially affecting grid users, services or operations is suspected, the following procedure MUST be followed:

1. Immediately inform your local security team, your NGI Security Officer and the EGI CSIRT via abuse .at. egi.eu. This step MUST be completed within 4 hours after the suspected incident has been discovered. You are encouraged to use the templates in Appendix B.
Incident Response in EGI

Each incident is assigned an IRTF member as incident coordinator (usually Security-Officer-on-Duty), who

- issues a heads-up warning to all sites (is the currently available information in goc-db sufficient for cloud incidents)
- works with the victim site to investigate the incident, possibly issuing additional all-sites broadcasts as new information is discovered
- coordinates the incident with other players (VOs, CAs, other CSIRTs, law enforcement...) this list is incomplete for cloud incidents.
- makes sure a closure report is sent to all sites
Incident Response in EGI

Incident Response Procedure:


- communication templates
- target times / what to investigate
- forensics
### Incident Response in EGI

<table>
<thead>
<tr>
<th>Incident ID</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>EGI-20110418-01</td>
<td>stolen ssh credentials</td>
</tr>
<tr>
<td>EGI-20110301-01</td>
<td>bruteforce ssh</td>
</tr>
<tr>
<td>EGI-20110121</td>
<td>web server misconfig</td>
</tr>
<tr>
<td>EGI-20111201-01</td>
<td>bruteforce ssh</td>
</tr>
<tr>
<td>EGI-20101018-01</td>
<td>bruteforce ssh</td>
</tr>
<tr>
<td>EGI-20100929-01</td>
<td>stolen ssh credentials</td>
</tr>
<tr>
<td>EGI-20100722</td>
<td>bruteforce ssh</td>
</tr>
<tr>
<td>EGI-20100707-01</td>
<td>stolen ssh credentials/remote vulns in CMSes</td>
</tr>
<tr>
<td>EGEE-20091204</td>
<td>stolen ssh credentials/X keyboard sniffing</td>
</tr>
<tr>
<td>GRID-SEC-001</td>
<td>stolen ssh credentials</td>
</tr>
</tbody>
</table>
Incident Response in EGI

- Large majority of incidents due to stolen or weak ssh credentials
- We have no power to force sites to deploy e.g. two factor auth
- (In fact its already difficult to get a good ssh config and reasonably secure passwords in place everywhere.)
- We do try to motivate sites to install important security patches, partly to offset the potential damage from user level intrusions
Incident Response in EGI

We have our IR toolsets ready... for the Grid

- We can centrally suspend a DN.
- In case of a compromised DN we can filter for a list of potentially affected sites.
- We can suspend bad sites from the infrastructure.
Incident Response in EGI

Will This work for... incidents on academic cloud infrastructures:

- Appliance analyzed: weak root password "...." in VM image, ssh root login permitted, 8 VM instances running same appliance found.
- A VM had REDIS running without any firewall so accessible to anyone detected by the NREN.
- running an insecure Tomcat (weak password) tried to access what seemed to be a controller node of a bot net.
- DoS attack starting from the compromised machine has been detected by our ... NREN.
- DDos from 2 COMPs workers created from the Image for COMPSs-PMES Debian/7/KVM detected by our ... NREN.
- EGI-CSIRT would benefit form getting notified about all Cloud Incidents (not limited to FedCloud).
Incident Response in EGI

Will this be enough for the FedCloud?

- We have to protect the infrastructure from under-performing RCs/Endorsers/rogue VMs/Users....
- Are all certified FedCloud sites really ready to operate this infrastructure.
- Are the responsibilities in IR (reporting, containment, forensics) on VMs clear?
- Can we centrally suspend a users credentials in Fedcloud?
- Can we centrally operate on running VMs?

Check: 20-May-2015 13:30 Security for cloud federations
Boris Parak: VM and User Management in Incident Response
Incident Response in EGI

Additional tools

- Remote Forensics Infrastructure?
- Check/Ensure quality of endorsed VMs.
- Revoke Endorsement (who endorsed a VM? ... etc)
  Communication endpoints are not complete any more.
- A FedCloud tech expert needed in IRTF (attend/report weekly meetings)
Incident Response in EGI

Attackers almost always go for the lowest hanging fruits,... what are the major players in cloud-provisioning are doing about security?

Where do we stand with our FedCloud security compared to these.
Finally, we try to be good community members and maintain good relations with neighbouring CSIRTs at all levels.

Want to report an incident, ... send a mail to abuse .at. egi.eu
Collaborating security teams

EGI-CSIRT

- NREN + NGI CERT
- NGI CERT
- NREN CERT
- IRTF

Peer Infrastructures

NGI

NGI

NREN CERT

100+ Teams
Academia,
Gov, Industry,
ISP, Mil,
Finance

Non public
Communication
channels

ad-hoc collaboration

Strong cooperation
Incident Response in EGI

- candidate (12)
- listed (119) (2009)
- accredited (97) (2012)
- certified (8) (2014)

Ready for an interactive self assessment? check: https://check.ncsc.nl/questionnaire/
Thank you for your attention!