Incident Response Task Force

Leif Nixon

September 18, 2013

Incident Response Task Force

IRTF helps sites to deal with incidents that pose a threat to the EGI infrastructure.

- Incident prevention
- Incident response
- Forensics
- Coordination and communication with other players
- Outlook

Incident causes

EGI-20110809-01	NO	stolen ssh credentials
EGI-20110713-01	CA	stolen ssh credentials
EGI-20110418-01	IN	stolen ssh credentials
EGI-20110301-01	FR	bruteforce ssh
EGI-20110121	ES	web server misconfig
EGI-20111201-01	PK	bruteforce ssh
EGI-20101018-01	IT	bruteforce ssh
EGI-20100929-01	FI, DK	stolen ssh credentials
EGI-20100722	IT	bruteforce ssh
EGI-20100707-01	CERN, CA	stolen ssh credentials/ remote vulns in CMSes
EGEE-20091204	CH, DK, PL, DE, NL, BE...	stolen ssh credentials/ remote X keyboard sniffing
GRID-SEC-001	Most of known world	stolen ssh credentials

Underlying theme

Initial intrusion through stolen credentials

Privilege escalation through unpatched known vulnerabilities

Underlying theme

Initial intrusion through stolen credentials

Privilege escalation through unpatched known vulnerabilities

There is nothing EGI specific here

Prepare to be rooted

Security training – experience incidents first-hand; train incident response and forensics in a realistic setting.

Prepare to be rooted

Security training – experience incidents first-hand; train incident response and forensics in a realistic setting.

Upcoming training: Learn how to secure your systems.

Prepare to be rooted

Security training – experience incidents first-hand; train incident response and forensics in a realistic setting.

Upcoming training: Learn how to secure your systems.

There is nothing EGI specific here

Factorize

Research eInfrastructures are facing similar threats and problems

$\Downarrow$

Build joint security groups

See e.g. CTSC – NSF-funded Center for Trustworthy Scientific Cyberinfrastructure (`http://trustedci.org`)

Same discussion in the Nordics: establish a central body supplying projects and infrastructures with security services and expertise.

Next step

EGI/PRACE/EUDAT Joint training and workshop in Linköping 7–9 October.

`http://www.nsc.liu.se/joint-sec-training`