CSIRT WEBPAGE

Status update

Ian Neilson, Barbara Krasovec

Let’s see what we have

- Obviously work in progress…

- http://csirt.splet.arnes.si

EGI CSIRT

The EGI Computer Security Incident Response Team

Report an incident | Report a vulnerability | Forensics Howto

EGI CSIRT coordinates operational security activities within the EGI Infrastructure helping to deliver a secure and stable infrastructure and giving scientists and researchers the protection and confidence they require to safely and effectively carry out their research.

EGI CSIRT is a Certified member of TF-CSIRT Trusted Introducer Service and maintains links to security teams in peer infrastructures, National Grid Infrastructures (NGIs) and National

- Incident response, forensics and containment support, reporting and information exchange.

REPORT AN INCIDENT

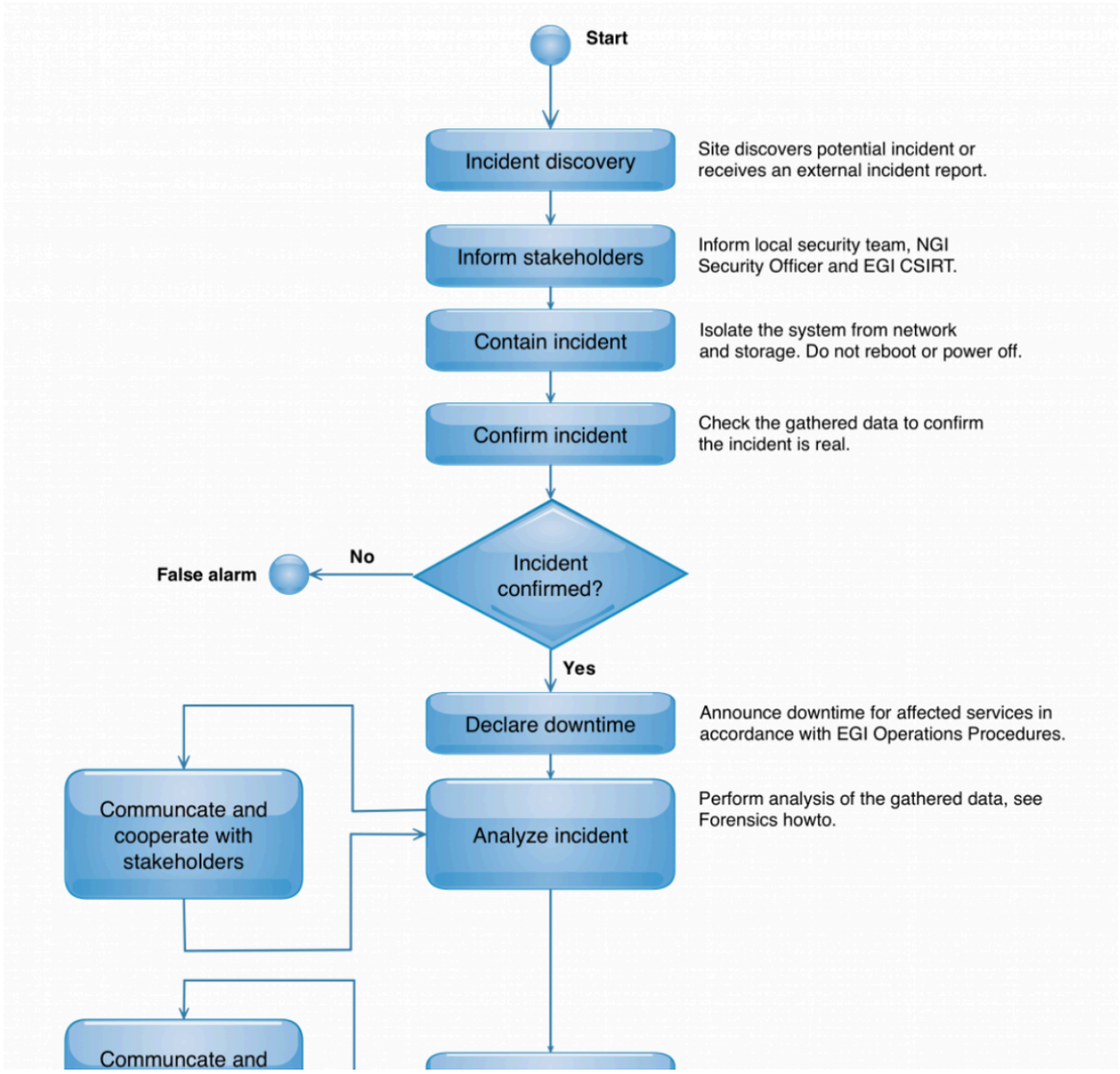
If you suspect you have information about a security incident affecting the EGI Infrastructure

The EGI Computer Security and Incident Response Team (EGI-CSIRT) provides operational security for the EGI Infrastructure. This includes responding to computer security incidents affecting the infrastructure, which is carried out by co-ordinating the incident handling activities in the NGIs/EIROs, RCs, VOs, and where applicable interacting with partner Infrastructures CSIRTs and CSIRT communities with which EGI-CSIRT has a trust relationship. If needed RCs are provided with expert level forensics support for the incident resolution. EGI-CSIRT also provides preventive and educational services such as security monitoring, vulnerability assessment, advisories to mitigate risks due to vulnerabilities,and security training.To improve collaboration in the field of IT-Security EGI-CSIRT actively reaches out to CSIRT communities and is an active member of TI TF CSIRT.

Please follow the EGI Security Incident Handling Procedure to report a security incident to **abuse at egi.eu** (PGP key).

Sites must report an incident or possible incident **within 4 hours** after the suspected incident has been discovered.

Follow this procedure to handle the incident at your site:



Name

Email Address

Message

2 + 11 =

Submit

Presentations and reports

Venom Rootkit

End of Year Report

Forensics howto

Report an incident template

Presentations on conferences

EGI CSIRT Contact Information

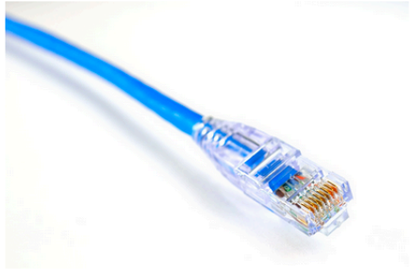
- abuse 'at' egi.eu : to **report security incident and/or abuse**
- csirt 'at' egi.eu (alias for csirt 'at' mailman.egi.eu): **EGI CSIRT main contact point**
- irtf 'at' mailman.egi.eu: **Incident Response Task Force operational actions**
- ngi-security-contacts 'at' mailman.egi.eu: Alias for all NGI security officers and their backups
- site-security-contacts 'at' mailman.egi.eu: Alias for all EGI site CSIRTs

EGI SVG Contact Information

- report-vulnerability (at) egi.eu: to **report a Software Vulnerability**
- svg-discuss 'at' mailman.egi.eu: The EGI Software Vulnerability Group discussion list
- svg-rat 'at' mailman.egi.eu: The Risk Assessment Team for the EGI Software Vulnerability Group

EGI SPG Contact Information

- spg-discuss 'at' mailman.egi.eu: Security Policy Group (SPG) discussions



EGI CSIRT team coordinates operational security activities within the EGI Infrastructure helping to deliver a secure and stable infrastructure and giving scientists and researchers the protection and confidence they require to safely and effectively carry out their research. The EGI CSIRT team is organized in the following groups:

Incident Response Task Force (IRTF)

Handle day to day operational security issues and coordinate Computer-Security-Incident-Response across the EGI infrastructure.

Security Drills Group (SDG)

The objectives of the Security-Drills are twofold. One aspect is to get an overview of the incident response capabilities of the sites participating in EGI and improve the collaboration among the distributed teams. The second is to improve the Security-Incident-Handling capabilities of the EGI-CSIRT itself. Here we continuously have to revisit our procedures and check whether our tracing of the security activities is sufficiently monitored and recorded.

Training and Dissemination Group (TDG)

Raise security awareness and improve security for system administrators by providing security training and best practice.

Security Monitoring Group (SMG)

Develop, deploy and maintain security monitoring tools.

Forensics HowTo

How to start?

DO NOT:

- restart the system
- kill the processes
- delete malicious files

MAKE SURE THE SYSTEM WAS HACKED:

- check system logs
- check commands history
- check login history
- check monitoring graphs for any abnormalities
- check running processes: top, ps, netstat, lsof
- If you connect to the system remotely, e.g. ssh, avoid using credentials that can be reused on other systems and consider them lost: change them as soon a possible
- Don't store data on the harddrive:
  - Set HISTFILE to /dev/null
  - Store temporary files in a filesystem backed by a tmpfs (in RAM), remotely or on a USB drive.

OK, SYSTEM WAS COMPROMISED. HOW TO CONTINUE?

Isolate the system

- unplug the network cable or apply the necessary firewall rules
- if it is a virtual machine, create a snapshot

First analysis

- How did the intruder get it?
- When did that happen?
- What kind of activity was performed on the server? (what was changed, installed, what kind of processes are running)

Content of the current webpage (public wiki)

1 EGI CSIRT Mission
2 Contacts
3 Incident Response
    3.1 Incident Response Task Force (IRTF)
    3.2 Incident Response in virtualized environments
    3.3 Communications: How To Report a Security Incident
    3.4 Incident Containment
    3.5 Forensics
4 EGI CSIRT Operation Policies and Procedures
    4.1 Central-emergency-suspension
5 EGI Advisories and Alerts
6 EGI CSIRT Members
7 RFC-2350

Pages on the new web

- Mission
- Activities
- Report an incident: flowchart for the
- Report a vulnerability
- Forensics howto: just basics
- Materials: reports and presentations
- Contacts

What do we want to move to the new web?

- Presentation of CSIRT and its mission
- Report an incident
- Report a vulnerability
- Contacts
- Reports and papers
- **Presentation of CSIRT groups? IRTF, SMG, SDG, TDG** (see: https://wiki.egi.eu/wiki/EGI_CSIRT:Activities)
- **Do we want to put tutorials, howtos, forensics … on the web?**
- **Do we want to put procedures and policy documents on the web?**

Suggestions

- We keep the detailed instructions, documents, tutorials and howtos on the wiki.

- We provide a template for reporting an incident to download and explain the procedure. Not the email template as we planned before..

- We provide an email contact or email form for reporting a vulnerability.

- We put links to presentations and reports in the materials section..

- We keep advisories on the wiki.

Questions

- Do we present other groups too? What do we want to say about SVG and SPG? Just links to their web?
- Do we publish links to useful sites, such as Pakiti, Operations Dashboard, Argo etc?
- Do we publish any “best practices” examples?
- Do we provide information about certification and suspension of the site? At least a link to the wiki?

Any suggestions on the layout / design?

- We will ask Sara for suggestions and some relevant images..

- Any preferences on the colours, position of the menu or something like that?

Any other suggestions on the content?

- Do we want to use some fancy buzzwords?
- Do we want to mention any services, tools, organizations? Federated Cloud, EUGridPMA locator, link to VO lists, working hours and so on?
- Do we want to put links to security teams SPG, SVG, SCG …?

Not to forget..

- The site is supposed to be ready **by the end of June**, so we only have a month left to finish it.

- What kind of domain are we going to use?

That’s all..

Comments?