Incident Response Policies and Procedures

Carlos Fuentes carlos.fuentes@rediris.es
IRIS-CERT, RedIRIS
SWE Security Contact

How to achieve consistent, effective response

- **Security Policy**
  - Define what is required/allowed/acceptable
  - Define responsibilities and authorities
- **Security Plan**
  - What is provided, who receives it and who provides it
- **Incident Response Policy/Plan**
  - Documented steps to keep control of incident
  - What will we respond to and when. How will we respond
  - RFC2350 - format for part of Incident Response Plan
- **These must link together**

How to achieve consistent, effective response

- **Aims: ensure consistency, reduce stress**
  - Mid-incident is a bad time to make decisions!
    - Much easier to read a document you wrote earlier
  - Make as many decisions as possible beforehand
    - Incidents differ in details; often same stages apply
  - Be sure your team has read the IH procedure
    - Don’t disturb me when I am on the beach, please read the doc!!!
- **If possible try out plans as exercises**
  - Modify procedures as you learn from experience
  - Security Service Challenge
    - https://twiki.cern.ch/twiki/bin/view/LCG/LCGSecurityChallenge

Procedures and policies are alive, keep them going/reading on

https://edms.cern.ch/document/867454

How to achieve consistent, effective response

Document, or at least think about, what you will do at each stage:

1. Receiving and Assessment (triage)
2. Progress Recording
3. Identification and Analysis
4. Notification - initial and once more information is available
5. Escalation - by incident type or service levels
6. Containment
7. Evidence collection
8. Removal and Recovery

Incident response policy

- **Grid participants are bound to (at least) two different incident response policies:**
  - Local incident response policy
  - "LCG/EGEE Incident Handling and Response Guide" (JSPG) Base on the Open Science Grid, Approved by WLCG Management Board on 28th November 2005:
    - http://cern.ch/proj-lcg-security-docs/LCG_Incident_Response.asp
  - May apply the NREN security policy (are you directly connected to the NREN?)

Incident response guide for LCG/EGEE

- **Reporting and Responding**
  - MUST report incidents related to GRID infrastructure
  - MUST respond incidents when you are involved
- **Handling of Sensitive Data**
  - Incident Information
  - Preservation of supporting data and evidence collection
- **Organization Structure**
  - Security Contacts
  - Defined Response technical experts and response team leader
  - Grid operations center

Incident response guide for LCG/EGEE

Incident Handling Process:

1. **Discovery and reporting**
   - Member: Report to your local security contact and your ROC Security Contact
   - No Member: Report to project-egee/lcg-security-csirts@cern.ch
   - Template for reporting should be followed:
     - Name, Phone, E-mail, Grid VO, ….
2. **Initial Analysis and classification**
   - Classification of incident: High, Medium, Low
   - Depending on the severity, risk, different actors should be required
3. **Containment**
   1. Preventing further spread of the attack through local services or resources
   2. Preventing further attacks from external grid services or resources
   3. Protecting the grid from attacks sourced at a different site
4. **Notification and escalation**
5. **Analysis and response**
   1. Resource tracking
   2. Evidence collection
   3. Removal and recovery
6. **Post-incident analysis**

Incident response procedure for grid hosts

- This procedure is provided for guidance only and is aimed at minimising the impact of security incidents, by encouraging post-mortem analysis and promoting cooperation between the sites. It is based on the EGEE Incident Response policy (available at https://edms.cern.ch/file/428035/LAST_RELEASED/Incident_response_Guide.pdf) and is intended for Grid site security contacts and site administrators.
- A security incident is the act of violating an explicit or implied security policy (ex: your local security policy, EGEE Acceptable Use Policy - https://edms.cern.ch/document/428036/3). When a security incident is suspected, the following procedure should be used:

Incident response procedure for grid hosts

1. Contact immediately your local security team and your ROC Security Contact
2.
3.

How to report:

- Message
- To: Your local site and your ROC Security Contact
- If not available to : project-egee-security-csirts@cern.ch
- Logs/information/evidences you did gather
- Actions you did take before sending the message¡

Incident response procedure for grid host

4. **If appropriate:**
   - Report a downtime for the affected hosts on the GOCDB
   - Send an EGEE broadcast announcing the downtime for the affected hosts

   Use “Security operations in progress” as the reason with no additional detail both for the broadcast and the GOCDB.
5. **Perform appropiate forensics and take necessary corrective actions**
   - If needed, seek for help from your local security team or from your ROC Security Contact or from project-security-support@cern.ch
   - If relevant, send additional reports containing suspicious patterns, files or evidence that may be of use to other Grid participants to project-egee-security-contacts@cern.ch. NEVER send potentially sensitive information (hosts, IP addresses, usernames) without clearance from your local security team and/or your ROC Security Contact.

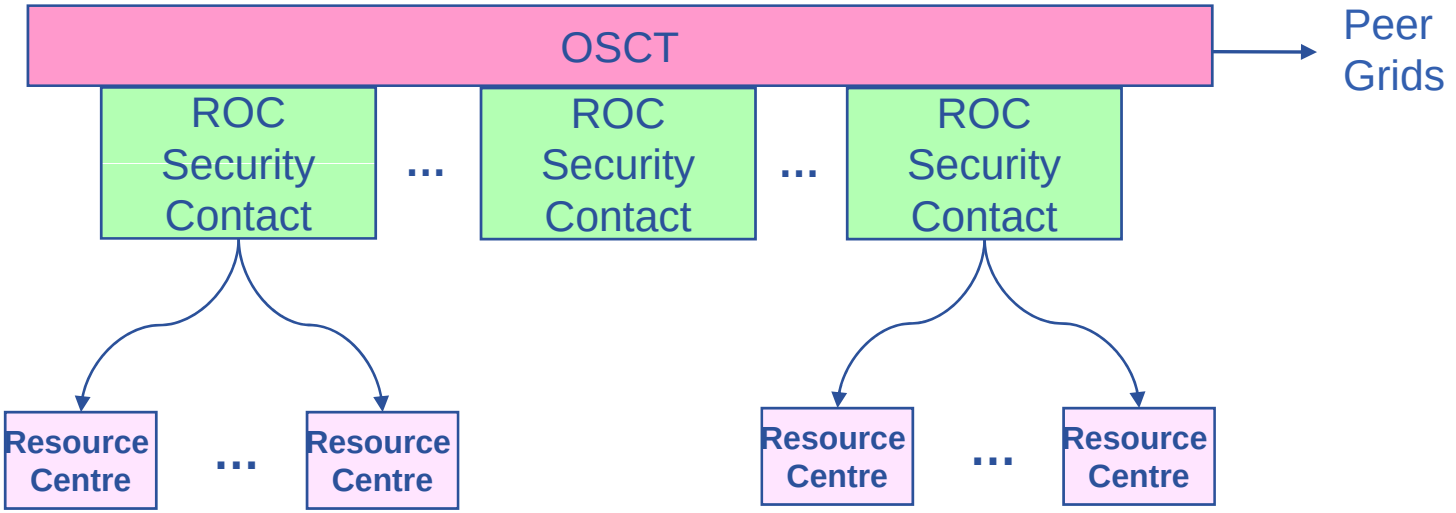
Incident response procedure for grid host

6. Coordinate with your local security team and your ROC Security Contact to send an incident closure report within 1 month following the incident, to all the sites via project-egee-security-contacts@cern.ch, including lessons learnt and resolution.

7. Restore the service, and if needed, send an EGEE broadcast, update the GOCDB, service documentation and procedures to prevent recurrence as necessary.

Incident response coordination

- ROC Security Contacts are part of the EGEE Operational Security Team (OSCT)
- Small incidents coordination: first site reporting the attack
- Large incidents coordination: ROC Security Contact on duty



Incident response coordination

A large part of IR coordination consists in managing the flow of information

- **The role of the coordinatior is to:**
  - Process the available information as soon as possible and follow the most likely leads
  - Provide accurate information to the sites
  - Contact and follow up with the relevant CERTs/CSIRTs
  - Ensure the process does not stall
- **The objective is to:**
  - Understand what was the vector to attack (ex: entry point)
  - Ensure the incident is contained
  - Establish a detailed list of what has been lost (ex: credentials, data)
  - Take corrective action to prevent re-ocurrence

Conclusion

- **Know the Incident Response procedure (https://edms.cern.ch/file/428035/LAST_RELEASED/Incident_response_Guide.pdf)**
  - Make sure your team has read it
  - Keep updated
- **Make your own IR guide**
- **Define the responsibilities**
- **Report your incidents and share the investigations and results**