Sécurité

parlons-en!

Sécurité

parlons-en!

parlons-en!

Sommaire

- rappel des procédures
  procédure grilles
  - (procédure clouds)
    valable pour EGI fed Cloud
    mais aussi pour des cloud
    locaux
- exemple
  (un vrai)
- horizon sécurité EGI-Conférence

Petit rappel des

PROCEDURES

Que faire un cas d'incident ?

Definition

- A security incident is the act of violating an explicit or implied security policy

  example:

  – local security policy,

  – EGI Acceptable Use Policy

Incident: Response -1

- Within 4hours **COMMUNICATE**

  inform:
  - your local security team,
    - the one you have in the GOCDB
    - your institute's security contact
  - your NGI Security Officer
    - ngi-france-security-contact-l@france-grilles.fr
  - the EGI CSIRT via abuse@egi.eu

- Within 1 working day
  - try to contain the incident:
    - unplugging all connections (network, storage, etc…)
  - DO NOT REBOOT or POWER OFF the host *(have a coffee first)*
  - note down carefully what actions you take with a timestamp
  - investigate

Incident: Response -1bis

- Within 1 working day
  - Confirm the incident to you local security team and EGI-CSIRT (reply to CSIRT emails)
    - If not confirmed -> you can breathe again

- If confirmed
  - If applicable : Announce downtime with the reason :

    "Security operations in progress"

Incident: Response -2

- As soon as possible
  - Analysis and information acquisition:
    - IP addresses,
    - log connections,
    - timestamps,
    - identities involved
    - sources of any suspicious connection
    - (see list in Appendix)
  - Objective:
    - understand the source and the cause of the incident, the affected credentials and services, and the possible implications for the infrastructure
  - A site MUST be able to produce these info
    - 3month prior to the incident
    - 6month prior to the discovery of successful SSH connections

Incident: Response - final

- Within 1 month
  - Restore (update) the service, its documentation and procedures to prevent recurrence
  - Send an incident closure report
    - Coordinate with your local security team and the EGI CSIRT
    - send to all the sites via *site-securitycontacts@mailman.egi.eu* including lessons learnt and resolution.
  - In practice:
    - EGI-CSIRT will do the communication with other sites
    - Reply to the email(s) you receive from EGI-CSIRT
    - abuse@egi.eu is the only email to remember

    (and the GOCDB)

Comme quoi, il n'est pas toujours facile de suivre la théorie

A TRUE EXAMPLE

To Conclude …

- Importance of reports and sharing with CSIRT
  - avoid spreading out
  - anticipate in all other sites across EGI
- Importance of broadcasts
  - do not miss them
- Importance of "Good practices"
  - keeping logs (syslog)
  - keeping network logs
  - DO NOT Delete a VM :
    - take a snapshot, suspend it (wait for further notice)

EGI CONFERENCE

CSIRT Status

- CSIRT organization unchanged:
  - IRTF +

  Monitoring, Vulnerability assessment, Training, Drills
- Task
  - 50 + jurisdictions, independents sites or part of big national facilities …
  - Since 2014: 19+ sites in EGI-FedCloud …
- Operation:
  - Follow the rules and policies or last resort suspension
  - Worked well for the Grid but gets blurry with the Cloud
    - cloud infrastructures shared among diverse communities
  - Toolset ready … for the Grid
    - Can suspend a DN, Get list affected site in case of a compromised DN, Can suspend sites from the infrastructure

Is it enough for the Cloud?

EGI-Engage

- Operation coordination
  - ok for the grid
  - + Include contacts and partnership with FedCloud actors
  - +Develop security operation for the Cloud:

  evolve the security to support new technologies:

    - Security requirements and risk assessment for new services, technology, and deployments *(RAT, SVG)*
    - The evolution of operational security *procedures*, including forensics *(IRTF)*
    - Develop a new trust framework and develop new policies *(SPG)*
    - Develop the security challenge framework *(SSC)*
    - Develop the software vulnerability handling process to adapt to new technology and deployments *(SVG, IRTF)*

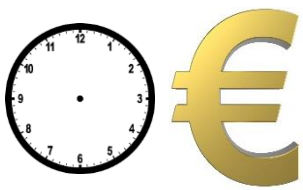
Monitoring

We Need To…

- Monitoring IaaS
  - Assessment of images
    - Up-to-date, no weak passwd…
    - Certification of VM on the AppDB level ?
  - Monitoring running VM
    - Part of certification, recommended best practices
    - Detection of weaknesses (passwd, ssh access, file permissions…)
  - Network monitoring
    - Recommendation for cloud providers and image owners
    - netflow tools for monitoring
- in EGI-engage
  - focus and collections and guidelines
  - support project
    - Checking images in AppDB ***
    - Certification of images ***

AppDB and security handling

- Light on AppDB due to the incident
- Discussions with developers
- appDB check and certification
  - add a sanity check of the VM
  - add a minimum security certification level of VM
    - before or after the VO endorser ?
    - certify software VO, VO endorser ??
  - possibility to suspend the VM image in the appDB
  - possibility to get the list of all instances
  - possibility to suspend all instances ?
  - …
- FedCloud made propositions to tackle these
  - Who can do that?



Others

- SPG
  - Modifying policies to generalize and include all EGI services (Grid & Cloud)

  Workshop session: modify Draft Policies
    - AUP
    - VM Operator (security responsible)
    - VM Consumer (end user)

- Working with other infrastructure
  - SCI : Security for Collaborating Infrastructure

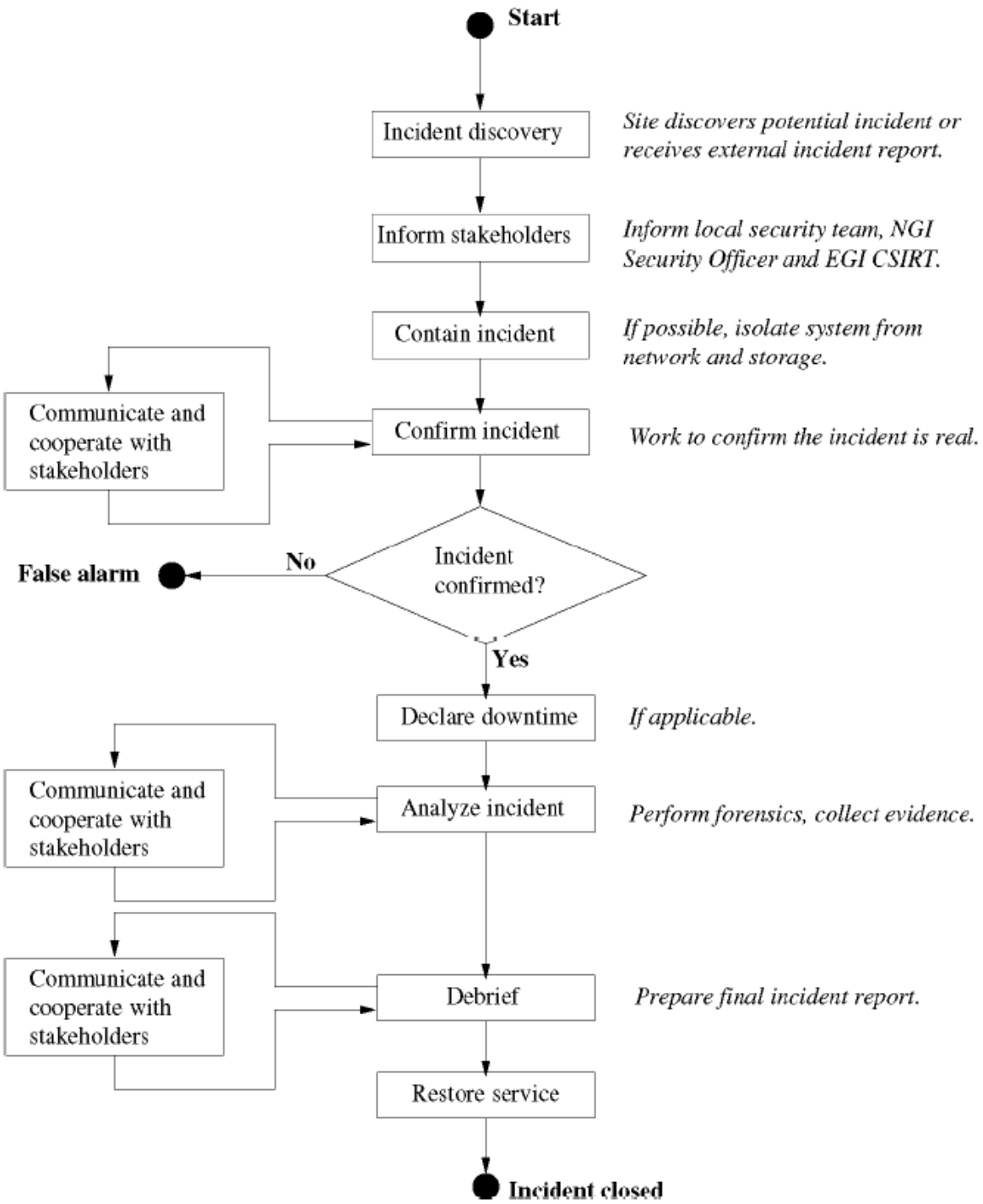
  "Standard best practices and trust"
  - PRACE, EUDAT, XSEDE

?

END

Information to produce in case of incident

- Host(s) affected (ex: compromised hosts, hosts running suspicious user code)
- Host(s) used as a local entry point to the site (ex: UI or WMS IP address)
- Remote IP address(es) of the attacker
- Evidence of the compromise, including timestamps (ex: suspicious files or log entry)
- What was lost, details of the attack (ex: compromised credentials, (root) compromised host)
- If available and relevant, the list of other sites possibly affected
- If available and relevant, possible vulnerabilities exploited by the attacker
- The actions taken to resolve the incident
- Identify and kill suspicious process(es) as appropriate, but aim at preserving the information they could have generated, both in memory and on disk.
- If it is suspected that some grid credentials have been abused or compromised, you MUST ensure the relevant accounts have been suspended
- If it is suspected that some grid credentials have been abused, you MUST ensure that the relevant VO manager(s) have been informed. VO contacts are available from: http://operations-portal.in2p3.fr/vo/search (Permalink)
- If it is suspected that some grid credentials have been compromised, you MUST ensure that the relevant CA has been informed. CA contacts are available from: https://www.eugridpma.org/showca
- If needed, **seek help from** your *local security team, from your NGI Security Officer* or from the **EGI CSIRT**
- If relevant, additional reports containing suspicious patterns, IP addresses, files or evidence that may be of use to other Grid parties SHOULD be sent to the EGI CSIRT.


Start
Incident discovery
Site discovers potential incident or receives external incident report.
Inform stakeholders
Inform local security team, NGI Security Officer and EGI CSIRT.
Contain incident
If possible, isolate system from network and storage.
Communicate and cooperate with stakeholders
Confirm incident
Work to confirm the incident is real.
False alarm
No
Incident confirmed?
Yes
Declare downtime
If applicable.
Communicate and cooperate with stakeholders
Analyze incident
Perform forensics, collect evidence.
Communicate and cooperate with stakeholders
Debrief
Prepare final incident report.
Restore service
Incident closed