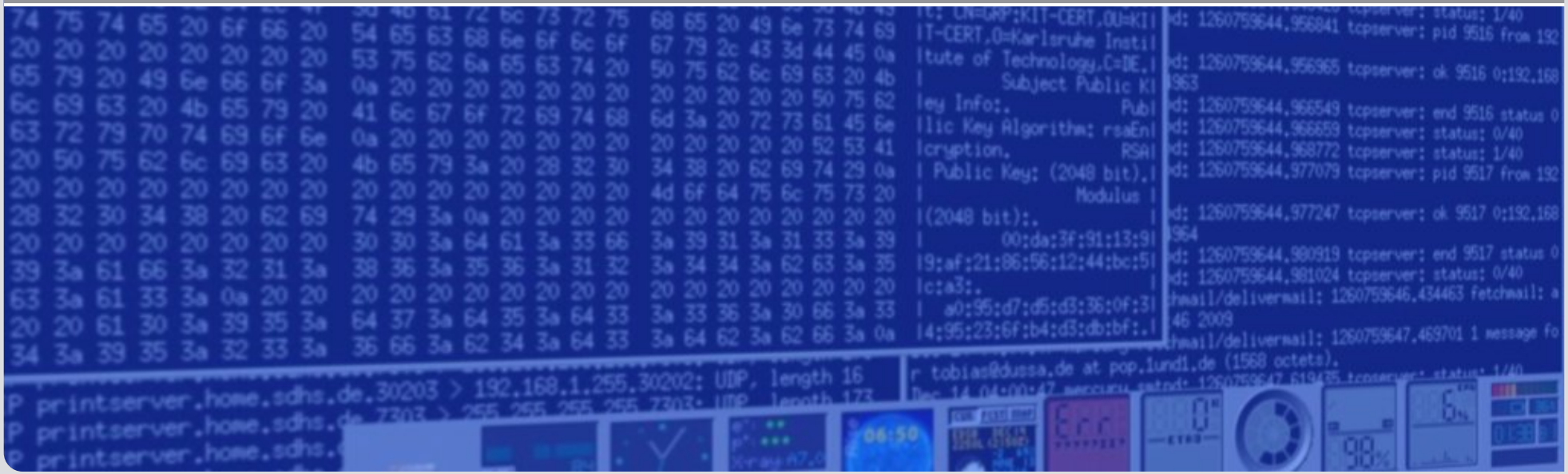
Karlsruhe Institute of Technology

# EGI Incident Response Procedure Introduction

**Tobias Dussa • EGI Technical Forum, September 17, Amsterdam**

COMPUTER EMERGENCY RESPONSE TEAM



# Introduction & Overview

Karlsruhe Institute of Technology

This talk

- introduces the new EGI incident response procedure,
- highlighting changes from the old EGEE IR procedure as well as
- points of particular importance.

# Purpose of the Procedure

Quote from the executive summary:

> *This procedure is aimed at minimising the impact of security incidents, by encouraging post-mortem analysis and promoting cooperation between grid sites.*

This roughly translates to “Make sites share information,” so that multi-site incidents can be detected and/or prevented more easily.

# Who's Who in EGI Security

- Site security officers.
- NGI security officers.
- EGI Computer Security Incident Response Team (CSIRT), which (confusingly) comprises
  - the Incident Response Task Force (IRTF),
  - the Security Drills Group (SDG),
  - the Security Monitoring Group (SMG), and
  - the Training and Dissemination Group (TDG).

  IRTF provides a Duty Contact (DC) for incident reports.

# Step 1: Detection & Information

When learning of a (suspected) incident involving grid resources or users, site administrators MUST inform

- the local security team,
- the appropriate NGI security officer, and
- the EGI CSIRT via `abuse@egi.eu`.

Time frame: MUST be done within 4 hours.

# Step 2: Containment

Next, if no immediate help can be reached, try to contain the incident

- iff you know enough about the system(s) involved and
- iff you are permitted to do so by local policy,
- unplug the system(s), but
- DO NOT power off or reboot!

Time frame: MUST be done within 1 working day.

# Step 3: Confirm the Incident

Once the initial steps have been taken,

- confirm that a security incident has taken place,
- if necessary, with help from
  - your local security team,
  - “your” NGI security officer, or
  - the EGI CSIRT.

Time frame: No particular limit.

# Step 4: Announce Downtime

If the incident results in resource downtime,

- announce the downtime for the affected resources
- in accordance with the EGI operational procedures,
- citing “Security operations in progress” as the reason.

Time frame: MUST be done within 1 working day.

# Step 5: Secure Evidence

Next, follow up on the incident:

- Secure all evidence and
- perform forensic analysis in cooperation with
  - your local security officer,
  - “your” NGI security officer, and
  - the EGI CSIRT.

Time frame: Requests from the EGI CSIRT MUST be followed-up within 4 hours throughout the analysis.

# Step 6: File a Final Report

Karlsruhe Institute of Technology

After the incident hhas been handled,

- compile a final report with
  - incident details,
  - resolutions and workarounds, and
  - lessons learned and
- provide it to all sites via
  `site-security-contacts@mailman.egi.eu`.
- This report is not public, but only for security officers!

Time frame: The report SHOULD be filed within 1 month after the incident.

# Step 7: Restore Affected Services

Karlsruhe Institute of Technology

After the incident has been handled,

- restore the disrupted services, if any (duh!), and
- update service documentation and/or procedures to prevent recurrence, if applicable.

Time frame: No particular limit.

# CSIRT's Role — Triage and Evaluation

Karlsruhe Institute of Technology

The first job of the CSIRT Duty Contact is to evaluate and correlate the initial incident report:

- Establish whether the incident is
  - previously known or new, and
  - isolated or part of a larger incident.
- Assign an incident number.

# CSIRT's Role — Follow Up

Karlsruhe Institute of Technology

As the investigation is underway, the incident handler

- Follows up on any information that is missing,
- offers direct support to the site,
- coordinates support by other EGI CSIRT members, and
- analyzes the incident.

# CSIRT's Role — Reporting

Finally, during the entire handling of an incident,

- the DC issues regular reports to all sites involved as well as
- to all other sites, without exposing any particular information that a site wishes to keep private, and
- generally promotes communication between all parties involved.

# Differences From the EGEE IR Procedure

- Most importantly, new mail addresses to be used:
  - `abuse@egi.eu` and
  - `site-security-contacts@mailman.egi.eu`.
- Information dissemination is now the CSIRT's worry.
- All new and shiny mail templates!
- Finally, all mails need to be classified with the Traffic Light Protocol (TLP).

# Traffic Light Protocol?!? — Part 1

Simple classification scheme to indicate how sensitive information is:

- **Red:** “Personal and for named recipients only.” Very sensitive information that should only be transmitted person-to-person.
- **Amber:** “Limited distribution.” Sensitive information that is not for general sharing. Originator may specify distribution limits (e. g. “need-to-know,” “IRTF members only”).

# Traffic Light Protocol?!? — Part 2

- **Green:** “Community-wide distribution.” May be distributed freely within a given community, but not made publicly available.
- **White:** “Unlimited.” Go wild.

# Facts to Take Home

- The IR procedure provides you with a checklist to tick off.
- The aim is to detect and contain multi-site incidents.
- Thus, information sharing is emphasized. Sharing of sensitive information with the CSIRT community is important!

# C’est ça!

Karlsruhe Institute of Technology

# Any questions?

# C’est ça!

Karlsruhe Institute of Technology

## Thank you for your attention!