



Enabling Grids for E-science

OSCT

6 years of successful security operations!

Romain Wartel, CERN IT.

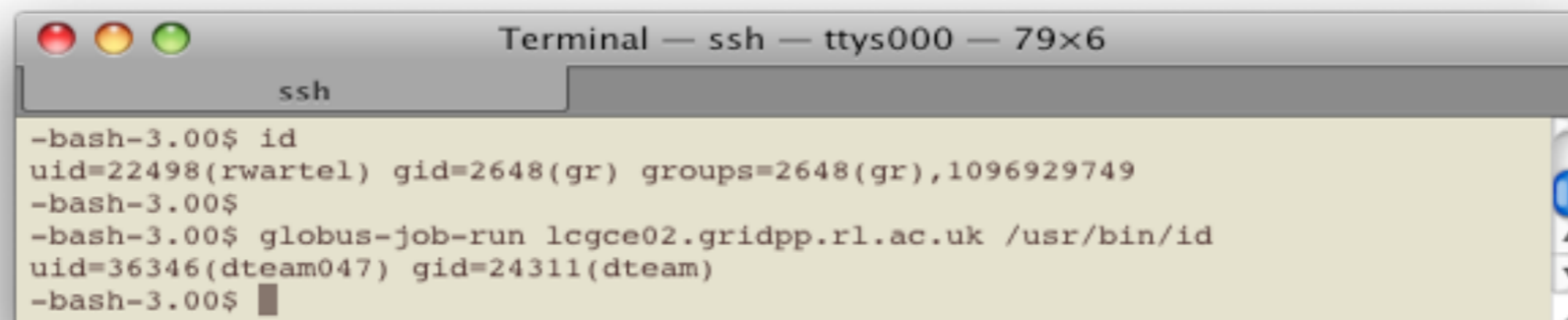
OSCT meeting, Nikhef, 22th March 2010

www.eu-egee.org



- **From the top level “grid security policy”:**
 - The responsibilities of Grid Security Operations include:
 - The maintenance of contact details of security personnel at each participating site and the facilitation of Grid-related communications between them.
 - Handling of operational security problems as they arise.
 - Providing incident response teams who will act according to the Grid Security Incident Response Policy [6].
 - Handling requests for exceptions to this policy as described in section 5.

- **Protect the grid infrastructure**
 - 240 institutions in 45 countries world-wide
 - As many local policies and different legal systems
 - Shared users from hundreds of organisations
 - Shared resources
 - Transparent, remote code execution across multiple domains

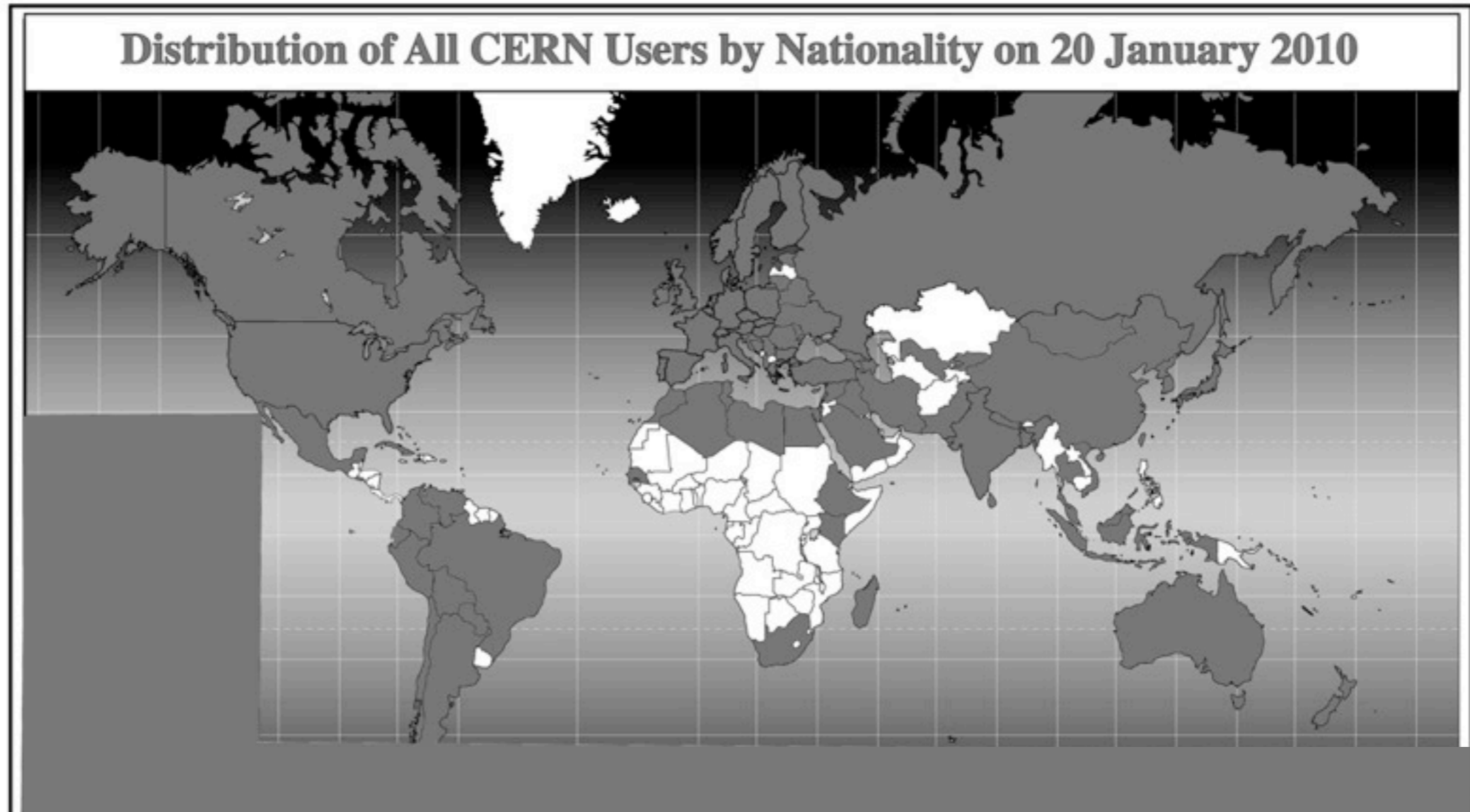


```

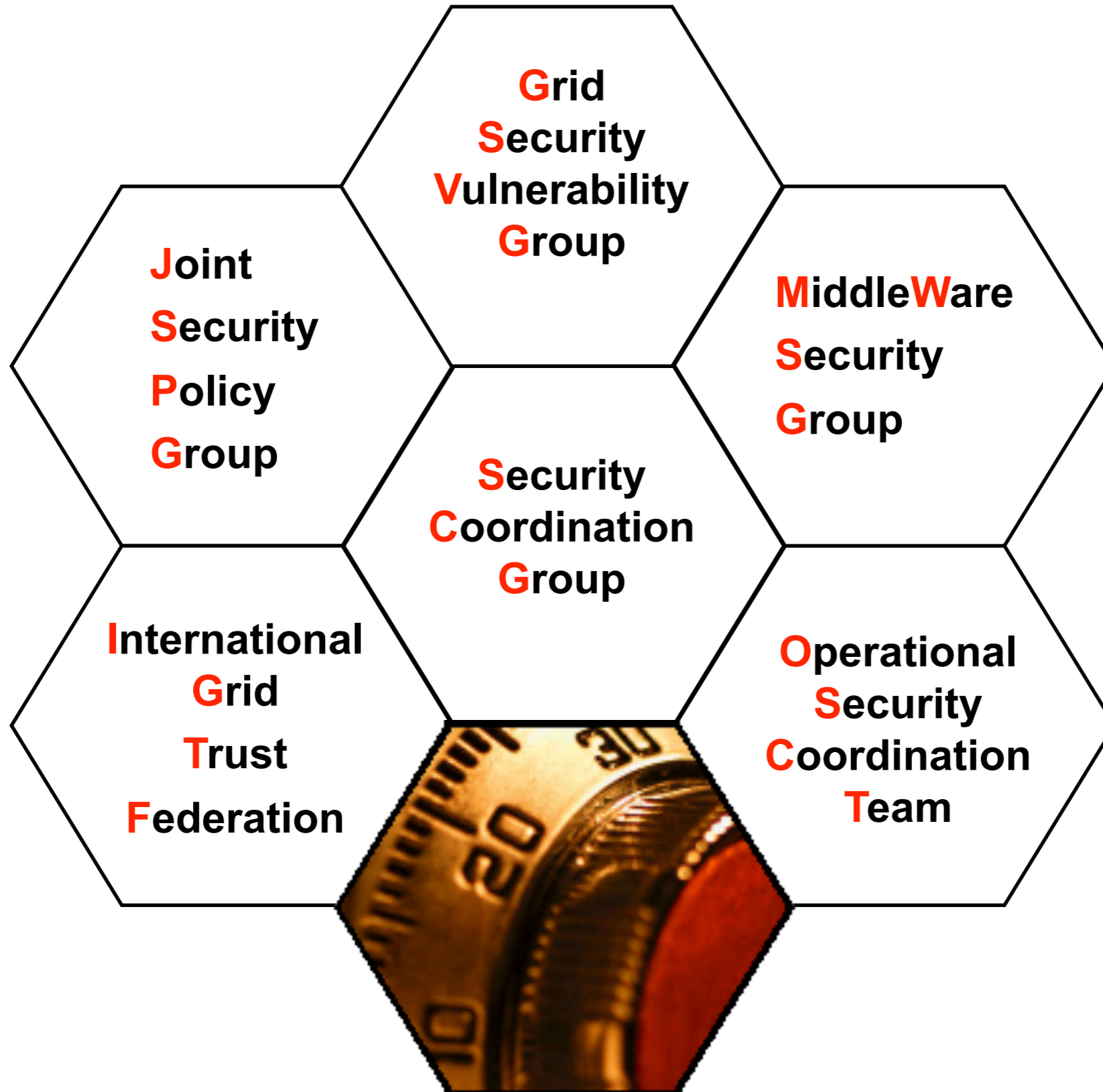
Terminal — ssh — ttys000 — 79x6
ssh
-bash-3.00$ id
uid=22498(rwartel) gid=2648(gr) groups=2648(gr),1096929749
-bash-3.00$
-bash-3.00$ globus-job-run lcgce02.gridpp.rl.ac.uk /usr/bin/id
uid=36346(dteam047) gid=24311(dteam)
-bash-3.00$
  
```

- Heterogeneous staff resources and skills
- Several funding sources and chains of command

- Countries marked in white contain (probably) **no** CERN user



- The main CERN Linux cluster has 20 000+ users
- Collaboration is GOOD for science but brings a larger attack surface

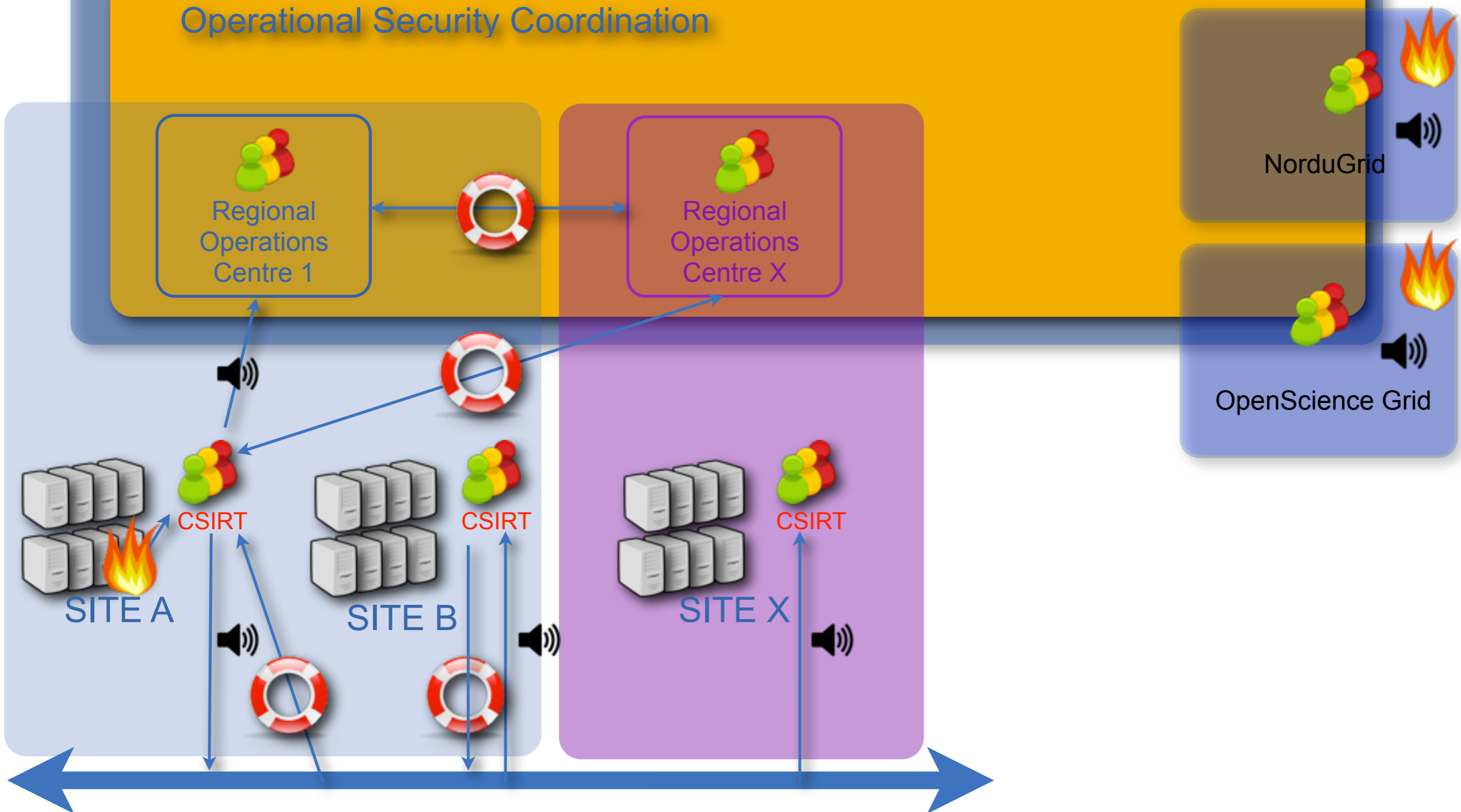


(Initial picture by Ake Edlund)

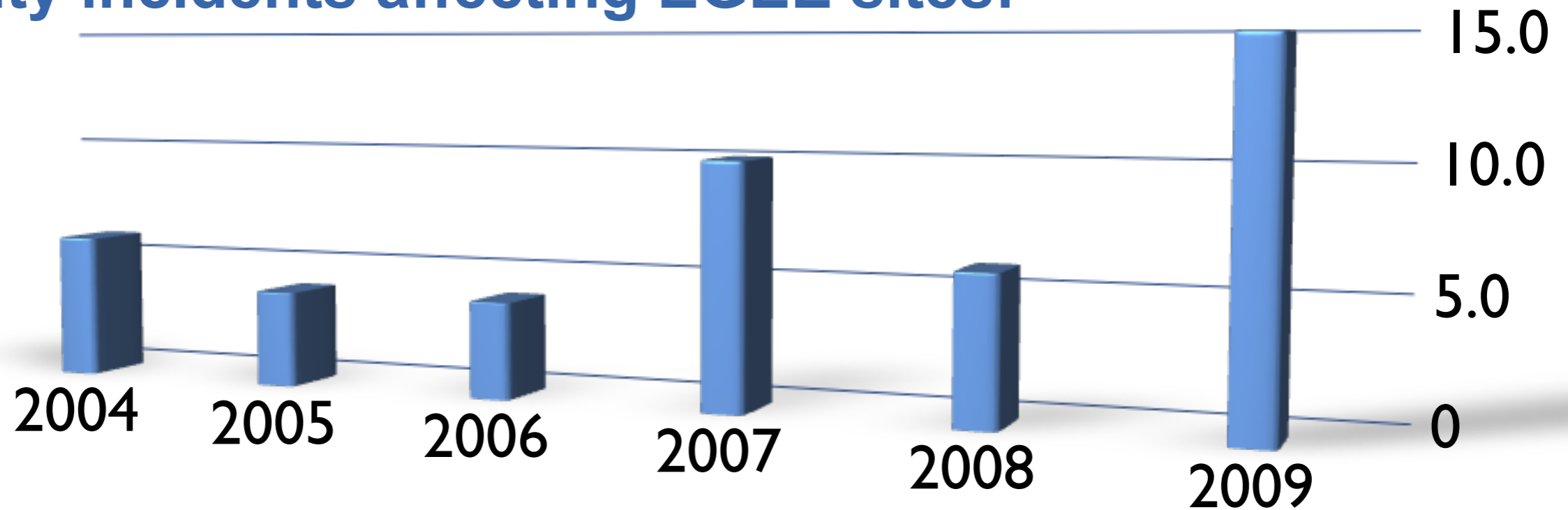
- **EGEE Operational Security Coordination Team (OSCT)**
 - Founded in 2004 (EGEE)
- **Mission:**
 - Provide an operational response to security threats against EGEE
 - Focus on computer security incidents handling
 - reporting channels
 - pan-regional coordination
 - support
 - Security monitoring
 - Best practice and advice to sites
- **Lead by the EGEE Security Officer**
- **Includes security contacts from each EGEE region**
 - support for daily security operations as part of an on-duty rota.

EGEE Grid operations

Operational Security Coordination



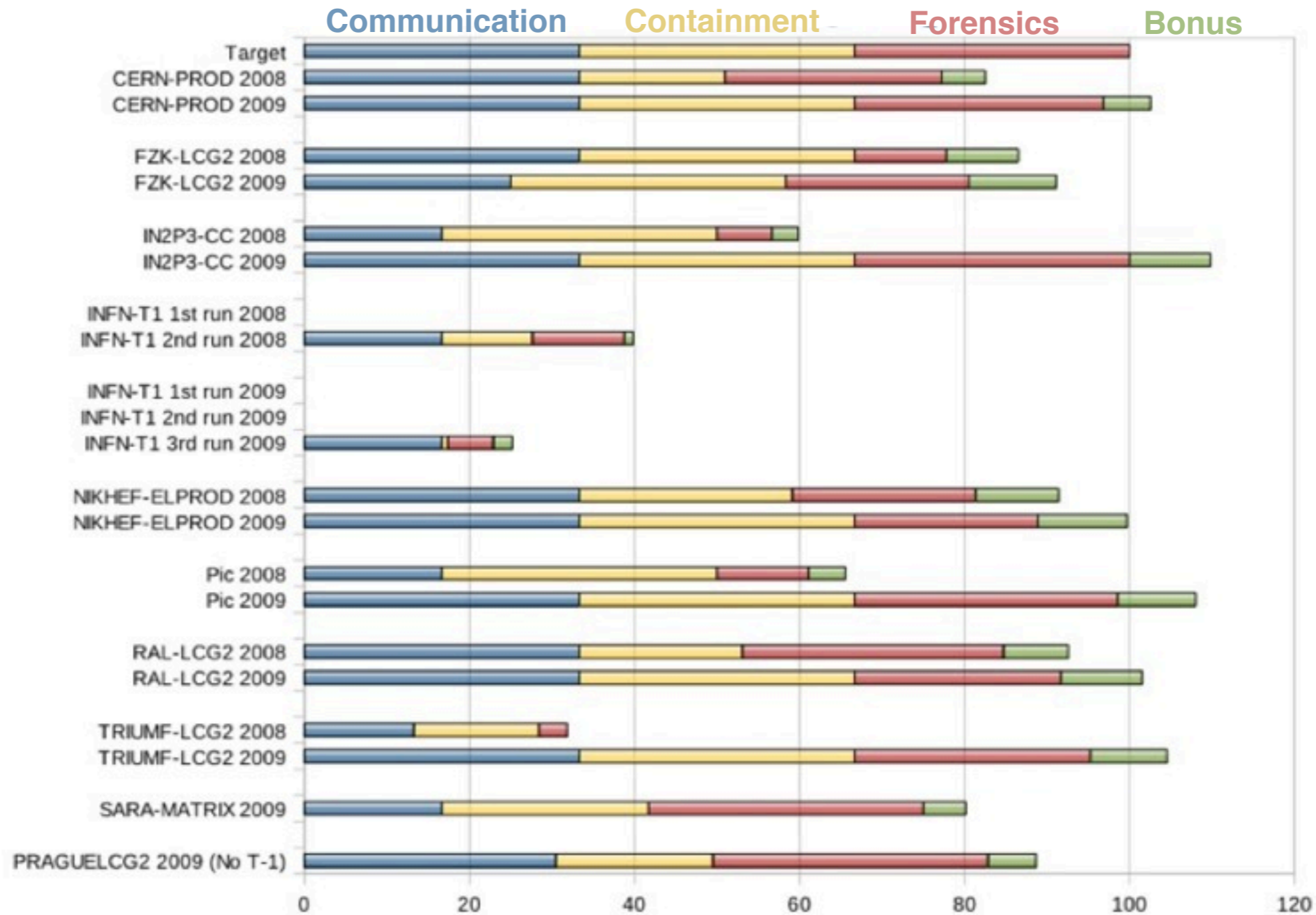
- Security incidents affecting EGEE sites:



- How many of these incidents were caused by the grid itself?

NONE

- All these incidents were **standard site security issues**
- However, the grid sites:
 - Could share information to **detect and prevent these incidents**
 - Could work together to **help the unexperienced sites**
 - Could collaborate to **resolve these incidents**
- **The grid helped re-enforcing academic security**



- **Distributed security operations**
 - Trust, cohesive team
 - OSCT-DC rota
 - Day-to-day operation handling, operational procedures
 - Direct communication with all partners during incidents
 - Strong cooperation with NRENs and peer grids

- **Security patching**
 - Effective monitoring in place
 - Significantly reduced patching window
 - Vanilla installs -> 75 days -> 7 days for critical vulnerabilities

- **Security incident management**
 - Lots of expertise in the team
 - Extensive connections outside of the team
 - Incident handled has part of normal operations

WELL DONE OSCT!



- **Lot of new challenges ahead**



- **More participants**
 - Restructuring of the procedures, communication channels
- **Limited EGI.org resources**
 - Security effort has to come from the NGIs
- **New attacks**
 - Expect more sophisticated, large scale security incidents

- Clear communication
- Clear procedures



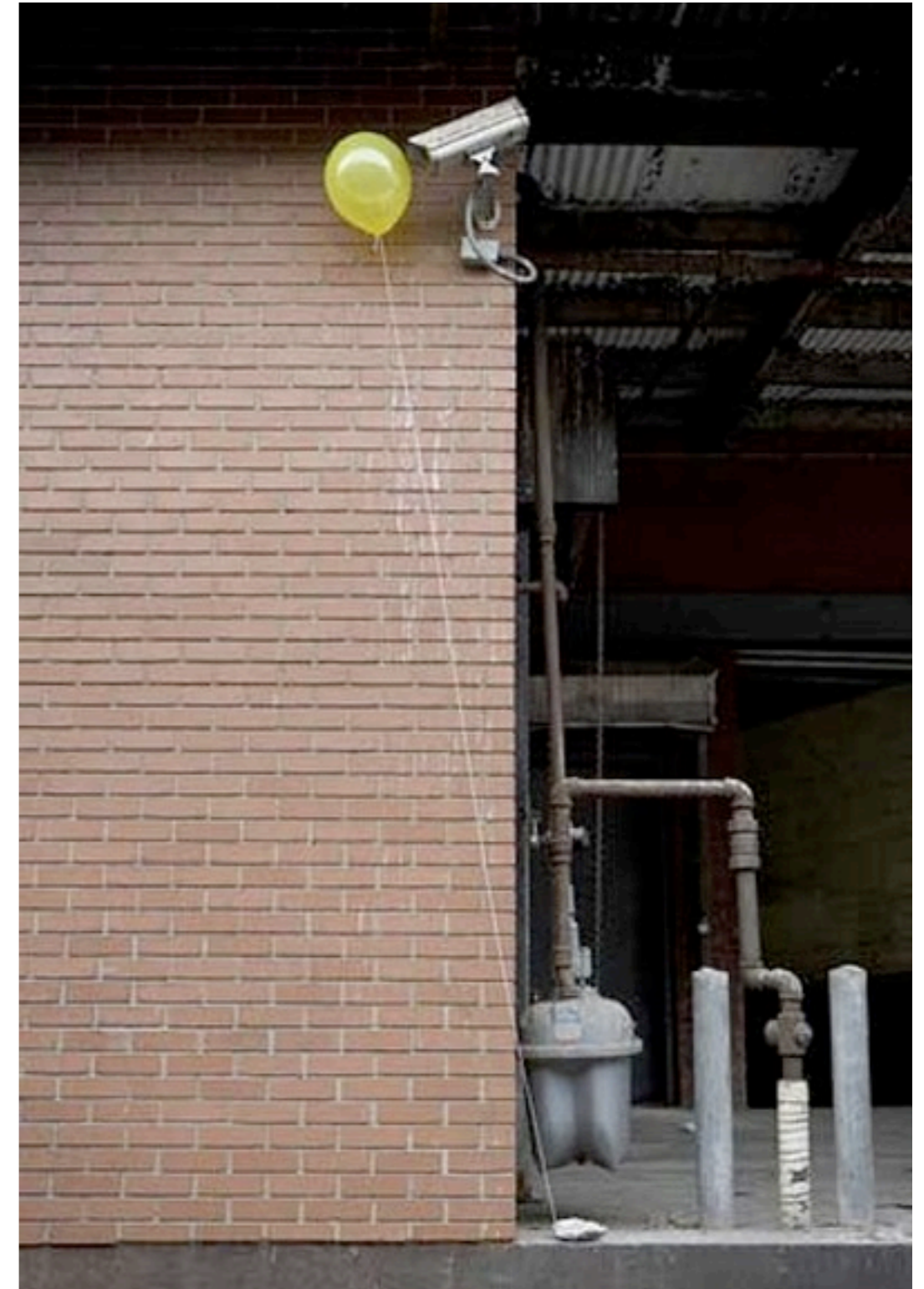
- **Identify the source of security incidents**
 - Essential to prevent re-occurrence



- Identifying the relevant threats and risks



- **Efficient, targeted monitoring**



- Prepare for sensitive information leaks and media interest



- **But, we are expert, right?**

Which links point to eBay?

- secure-ebay.com
- www.ebay.com/cgi-bin/login?ds=1%204324@%31%32%34.%31%33%36%2e%31%30%2e%32%30%33/p?uh3f223d
- www.ebay.com/ws/eBayISAPI.dll?SignIn
- scgi.ebay.com/ws/eBayISAPI.dll?RegisterEnterInfo&siteid=0&co_partnerid=2&usage=0&ru=http%3A%2F%2Fwww.ebay.com&raflid=0&encRaflid=default

...

Thank you

for your valuable help, effort, and commitment in EGEE !



