



Enabling Grids for E-science

Operational Security in EGEE

Romain Wartel, CERN IT

EGEE Operational Security Coordination Team

<http://www.eu-egee.org/security/>

International Symposium on Grid Computing (ISGC) 2008

Academia Sinica, Taipei, 7 - 11 April 2008

www.eu-egee.org



- **What is a “Security Incident”?**

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

- **What can motivate attackers?**

- Money (and little risk of being caught)
- Less likely: political motivation, challenge, ego, fame, etc.

- **How do attackers often proceed?**

- Most attacks are partly/fully automated
- First find an entry point (weak network service, stolen credentials, etc.)
- Install necessary toolkit to maintain a 'quiet' access
- Implant payload (DDOS, Botnet, SPAM engine, etc.)
- Harvest additional credentials

LOADS.cc

- Home
- Price
- Stats
- Sign Up

Октябрь 31/2007
Есть очень много юсы оптом , загрузки с трафа за подробностями стучим в аську.

Октябрь 26/2007
Налетай на ES IT DE , идёт хороший подлив.

Октябрь 23/2007
Введена принудительная проверка грузимых файлов на предмет палености , если файл палится более чем 30% из тестируемых 11 антивирусов , то загрузка данной задачи прекращается и рядом с ней появляется уведомление. Проверка файлов производится через приватный сервис.

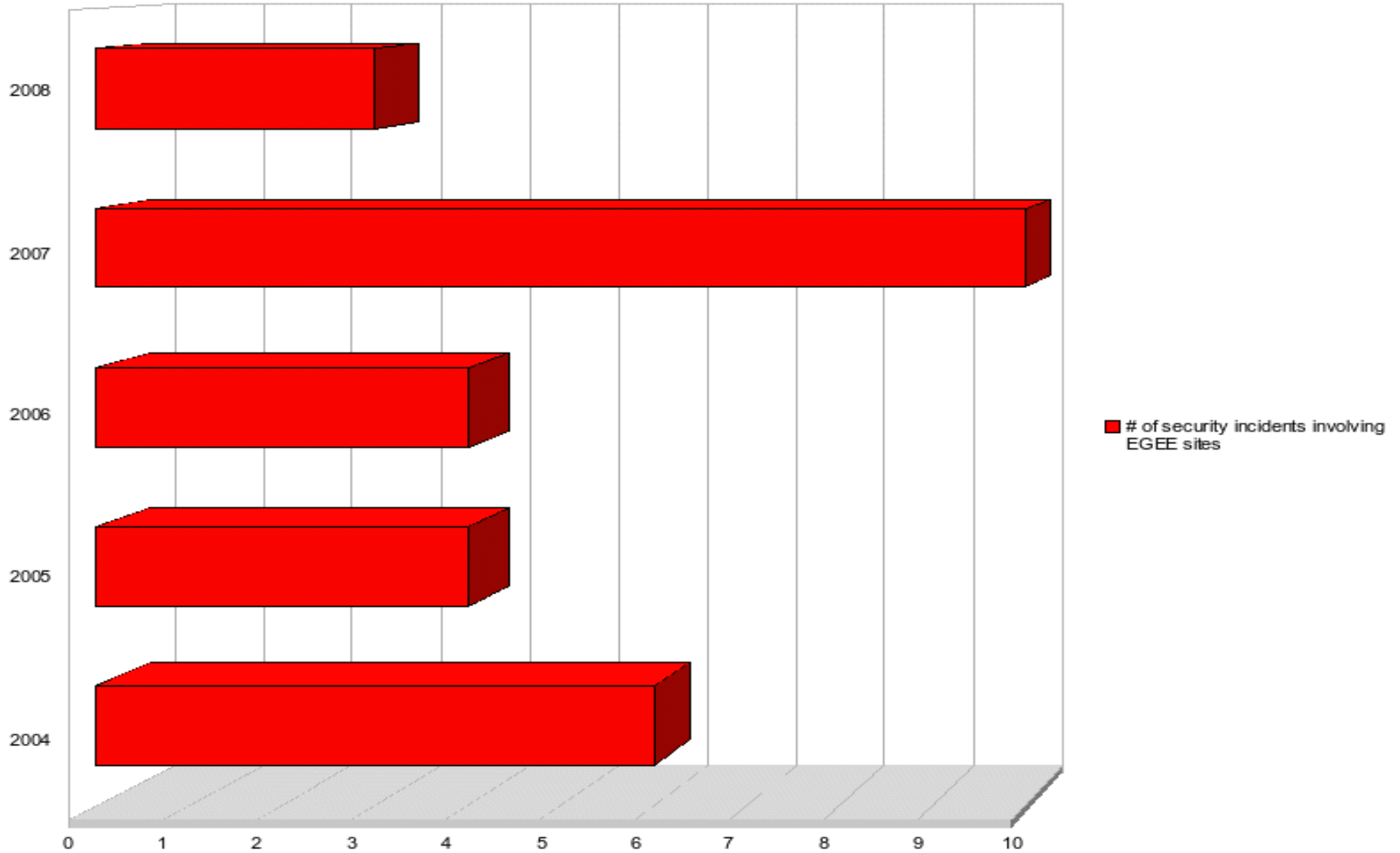
Октябрь 16/2007
Налетай не скупись покупай живопись) а точнее микс и юсу.

Август 30/2007
Введена новая фиша: ограничение количества загрузок в час , например грузить не более чем 200шт в час , актуально для соксов и иных ботов для поддержания одинакового среднесуточного количества онлайн.

Цены

Country	Price for 1k	
AU	300\$	Order now
DE	220\$	Order now
GB	210\$	Order now
IT	200\$	Order now
NZ	200\$	Order now
ES	200\$	Order now
US	110\$	Order now
BG	100\$	Order now
DK	100\$	Order now
FR	100\$	Order now
PT	100\$	Order now
NL	100\$	Order now
CA	80\$	Order now
JP	80\$	Order now
SE	70\$	Order now
BR	60\$	Order now
TR	60\$	Order now
NO	50\$	Order now
GR	50\$	Order now
PL	50\$	Order now
UA	40\$	Order now
RU	40\$	Order now
*	30\$	Order now

Кол-во возможных загрузок уточняйте в разделе [статистика](#)

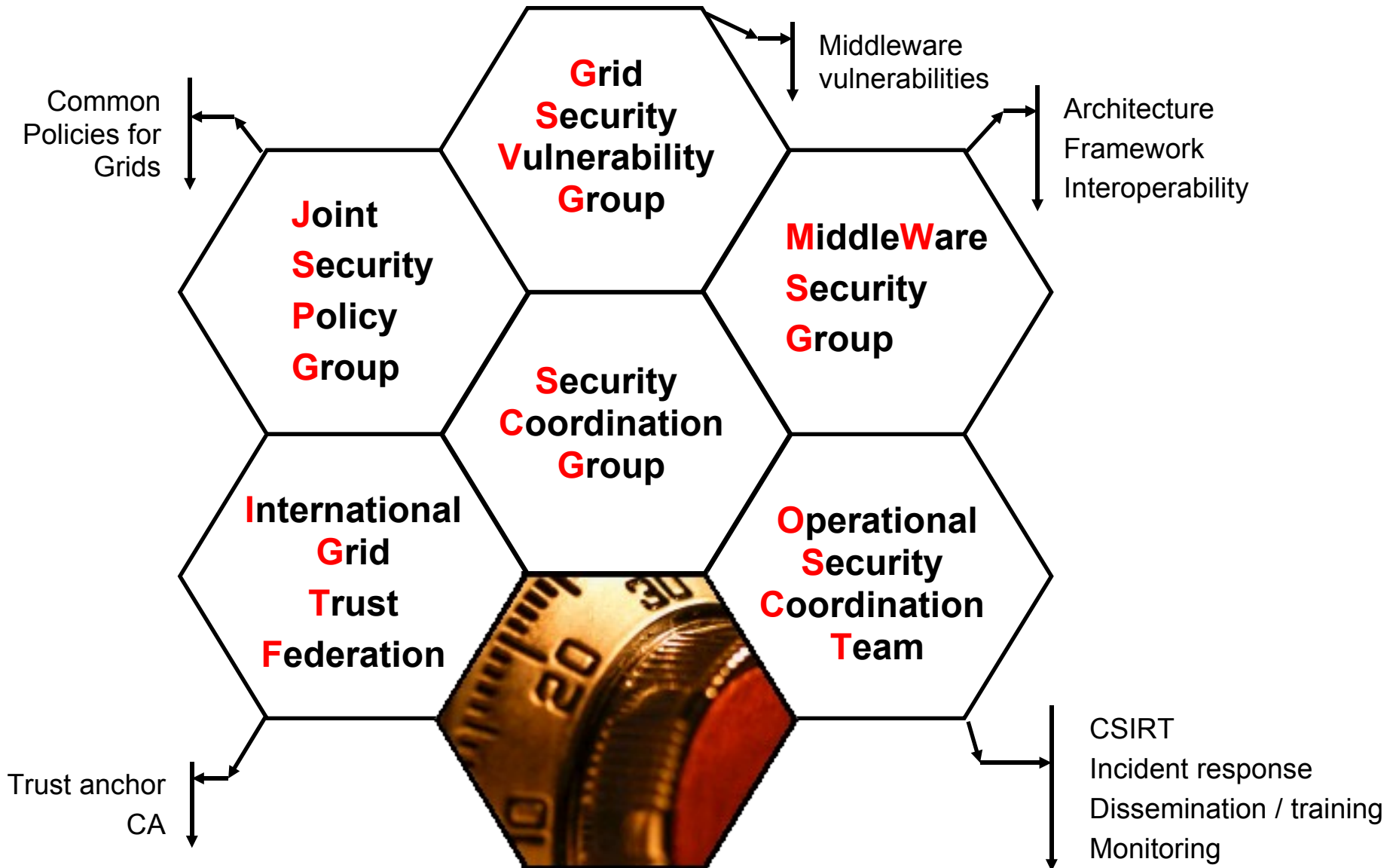


- **Attacks against other sites (ex: DDoS)**
- **Storage, distribution or sharing of illegal/inappropriate material**
- **Disruption of service, damage to user data**

This can involve:

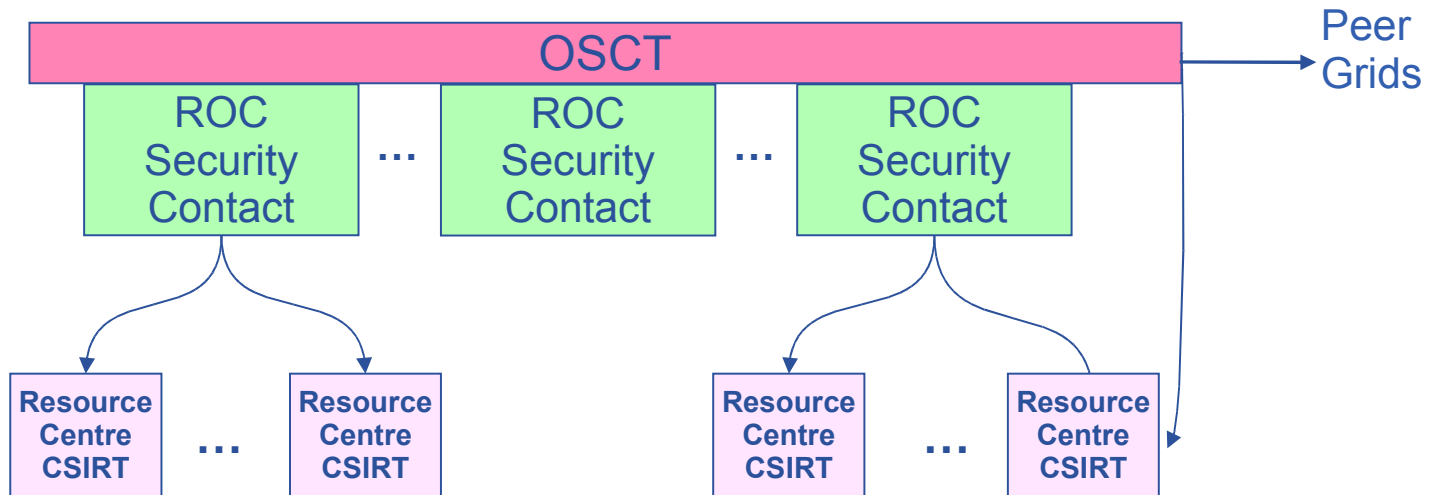
- **Damage to the project/sites reputation**
- **Legal/financial actions against participants**

<http://proj-lcg-security.web.cern.ch/proj-lcg-security/RiskAnalysis/risk.html>



- **JSPG is producing a set of security policies**
- **The following policies have been approved by the EGEE PEB and the WLCG GDB**
 - **Grid Security Policy (= top level policy)**
 - **Grid Acceptable Use Policy**
 - **Grid Site Operations Policy**
 - *Site Registration Policy*
 - *Audit Requirements Policy*
 - *Grid Security Incident Response Policy*
 - **VO Security Policy**
 - *VO Operations Policy*
 - *User Registration Policy*
 - **Approval of Certification Authorities**

- ROC Security Contacts are part of the EGEE Operational Security Coordination Team (OSCT)
- Incidents coordination: ROC Security Contact on duty



The EGEE Operational Security Coordination Team has three main activities:

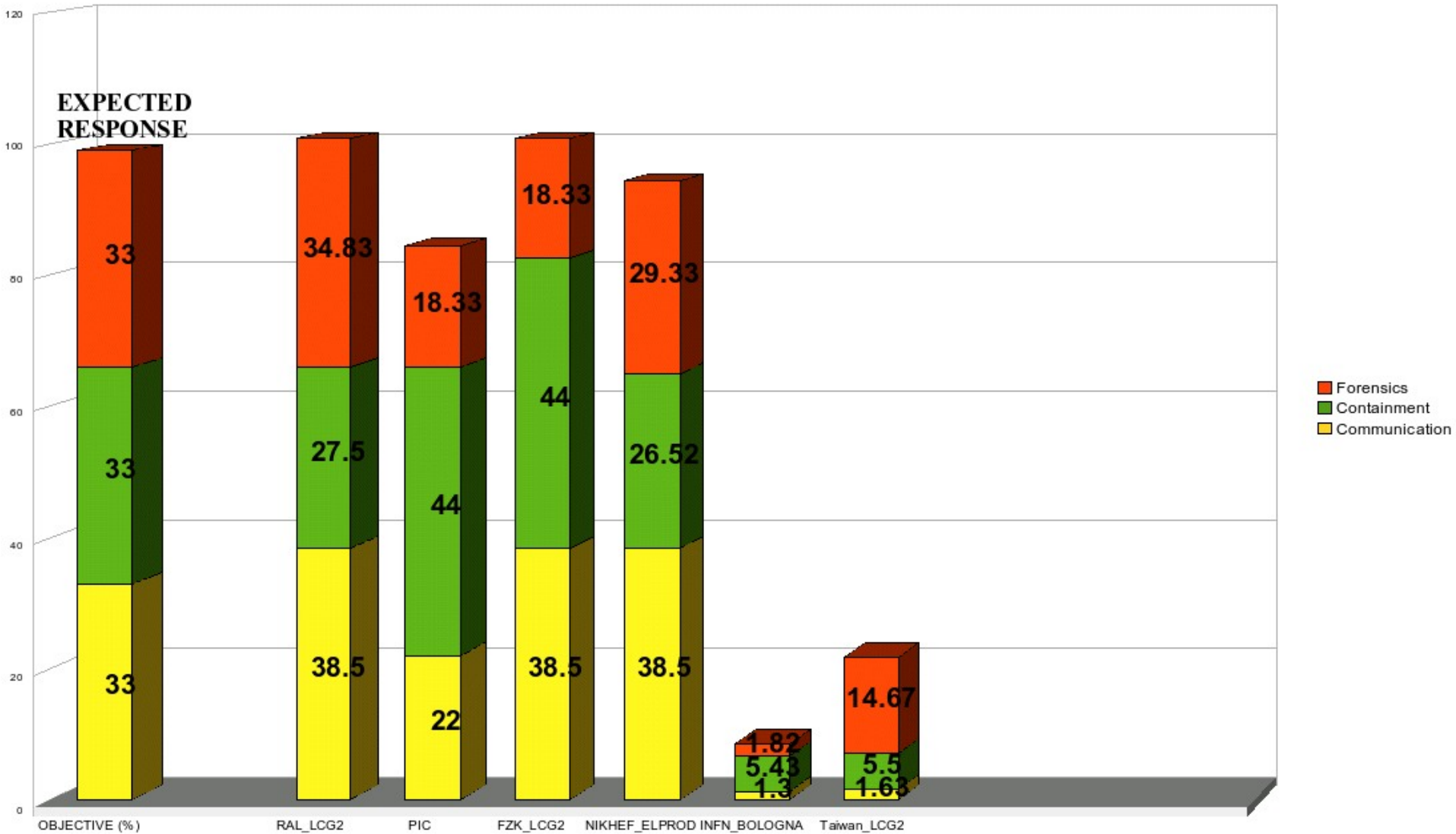
- **Incident Response improvement**
 - Security service challenges (SSC)
SSC1, SSC2, SSC3 (*in work*)
http://cern.ch/grid-deployment/ssc/SSC_2/SSC_2_google.html
 - IR channels (lists, IM)
 - IR Scenarios
- **Incident detection and containment (=monitoring)**
 - Several monitoring tools available to the sites
 - Central security tests (SAM)
- **Incident prevention**
 - Best practice
ex: <https://cic.gridops.org/index.php?section=roc&page=securityissues>
 - Training events

A large part of the incident response coordination consists in managing the flow of information

- **The role of the coordinator 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 of 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-occurrence**

- **Main issues:**
 - **It is essential to establish and maintain trust between the sites**
 - Obtain relevant and accurate information and collaboration from all possibly affected sites
 - Cope with the information flow (large incidents)
(during a multi-site incident, the coordinator had to process 500+ incoming emails during the first 5 days, including 280 at day 3)
 - Redistribute the information with an appropriate level of details
 - Prevent information leaks, which are a serious problem. They can discourage other sites from sharing their findings in the future and expose sensitive information (personal details, etc.)

SSC3: initial challenge



- **Training and dissemination requires significant efforts, as it is difficult to improve security practices at the sites**
- **Tests (security service challenges) are extremely useful**
- **Increased expertise in the team to manage multi-sites security incidents**
- **Need to build and maintain trust between the participants**
- **Cooperation and sharing with peer grids (ex: OSG) and with other involved parties (ex: NRENs) is essential**

Discussion