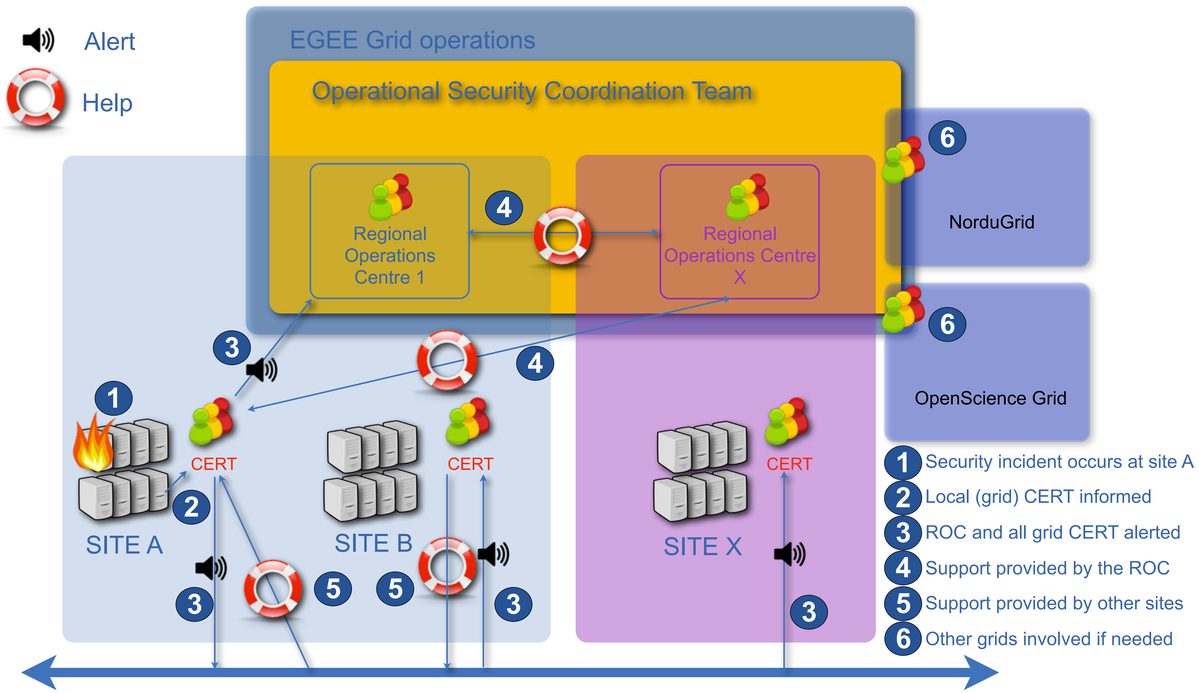
Scaling-up the response to grid security incidents

SA1
R. Wartel
Operational Security Coordination Team
Enabling Grids for E-sciencE



- **Incident Response: the role of the EGEE Operational Security Coordination Team**
  (The Operational Security Coordination Team includes security representatives from each ROC)
  – Coordinating the resolution of security incidents involving grid sites
  – Managing the flow of information between affected sites, and also with external organisations (ex: peer grids)

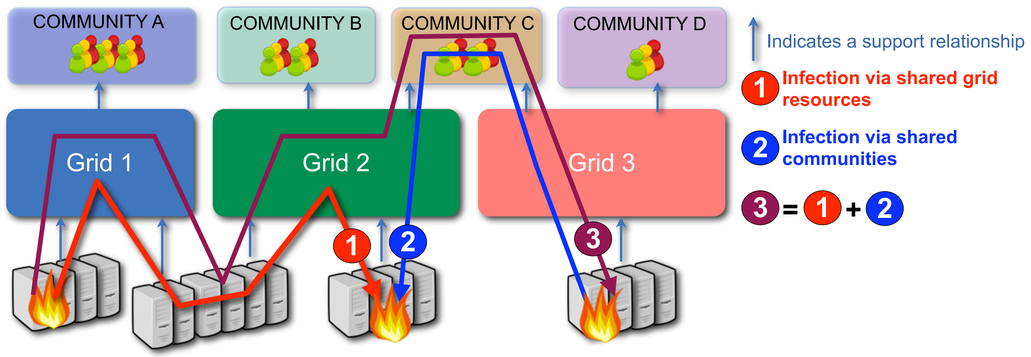
- **How does the Operational Security Coordination Team manage security incidents?**
  – For each incident, a coordinator from the Operational Security Coordination Team is responsible for:
    - Processing the available information as soon as possible and follow the most likely leads
    - Providing accurate information to the sites
    - Contacting and following up with the relevant CERTs (CERT: Computer Emergency Response Team)
    - Ensuring the incident response process does not stall
  – The objective is to:
    - Inform all the participating CERTs
    - 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

- **Experience gained with EGEE III**
  – Multi-site and cross-grid security incident management
  – Improved communication channels both within the project and with external organisations
  – Improved incident response procedures
  – Security drills organised to help sites improving their response to security incidents

- **Collaboration between grids and NRENs**
  – Sites may have separate separate grid and site/network CERTs
  – Cooperating and sharing information with major academic grid infrastructures is essential
  – Cooperating and sharing information with the National Research and Education Networks (NRENs) is essential
    - Grid and NREN CERTs have similar objectives, and limited resources

Cross-grid security incident propagation

– Grid resource providers may share their resources across different unrelated grids and user communities (case 1)
– Different computing grids may provide services to the same community (case 2)
– Attack vectorps may be combined (case 3), involving sites with no common grid and no common user community



Involving NRENs and peer grids

Representatives from the main academic grids and the NRENs share information when necessary