Security at Open Science Grid

Jeny Teheran
Security Analyst - OSG Security Team
WISE Workshop – XSEDE'16
July 18th, 2016

Open Science Grid

OSG and Security

- OSG implements an integrated cyber security model:
  - enables open science collaboration among users, sites and software providers.
    - these may operate under different security models!
  - Prevent loss of effort and resources due to security problems.

Open Science Grid

OSG Security Team

- Led by Mine Altunay at FNAL, OSG Security Officer.
- Susan Sons at Indiana University, next OSG Security Officer starting April 2017.
- Dave Dykstra and Jeny Teheran at FNAL.
- Anand Padmanabhan at University of Illinois-Urbana-Champaign.

OSG Security Team: our mission

- Protect OSG users and resources from security breaches.
- Provide convenient access to OSG resources.
- Be a security hub; disseminate security knowledge, best practices, and education for all our users.

Open Science Grid

Operational Security

- OSG Security Plan describes the procedures to maintain its operational security and the protection of OSG assets:
  - Tangible assets: the software infrastructure, the hosts and instances of the hosted operational services, the software distribution system.
  - Intangible assets: the reputation, the good will and credibility of the Consortium and its members.
- Risk assessment is performed annually by executing the security controls in our security plan.
  - The threat environment is constantly changing and evolving.

Open Science Grid

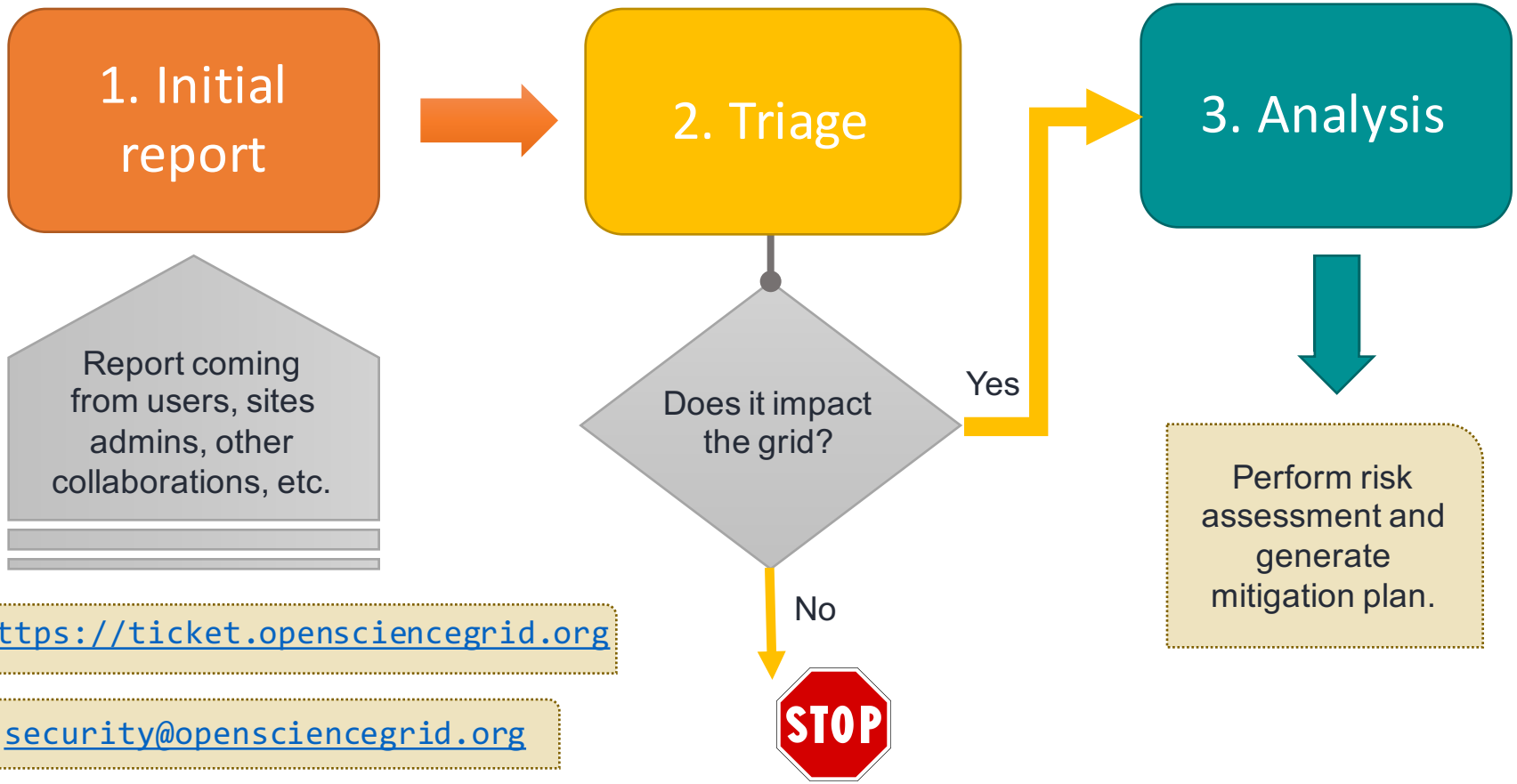
Operational Security

- Fire drills are constantly performed to measure readiness and security awareness in coordination with OSG Grid Operations Center at Indiana University.
- Security training for our members and teaching the best practices.
  - Security training for each new VO joining OSG.
  - We learn from our users about difficulties of security practices and policies.

Incident Management Response at OSG

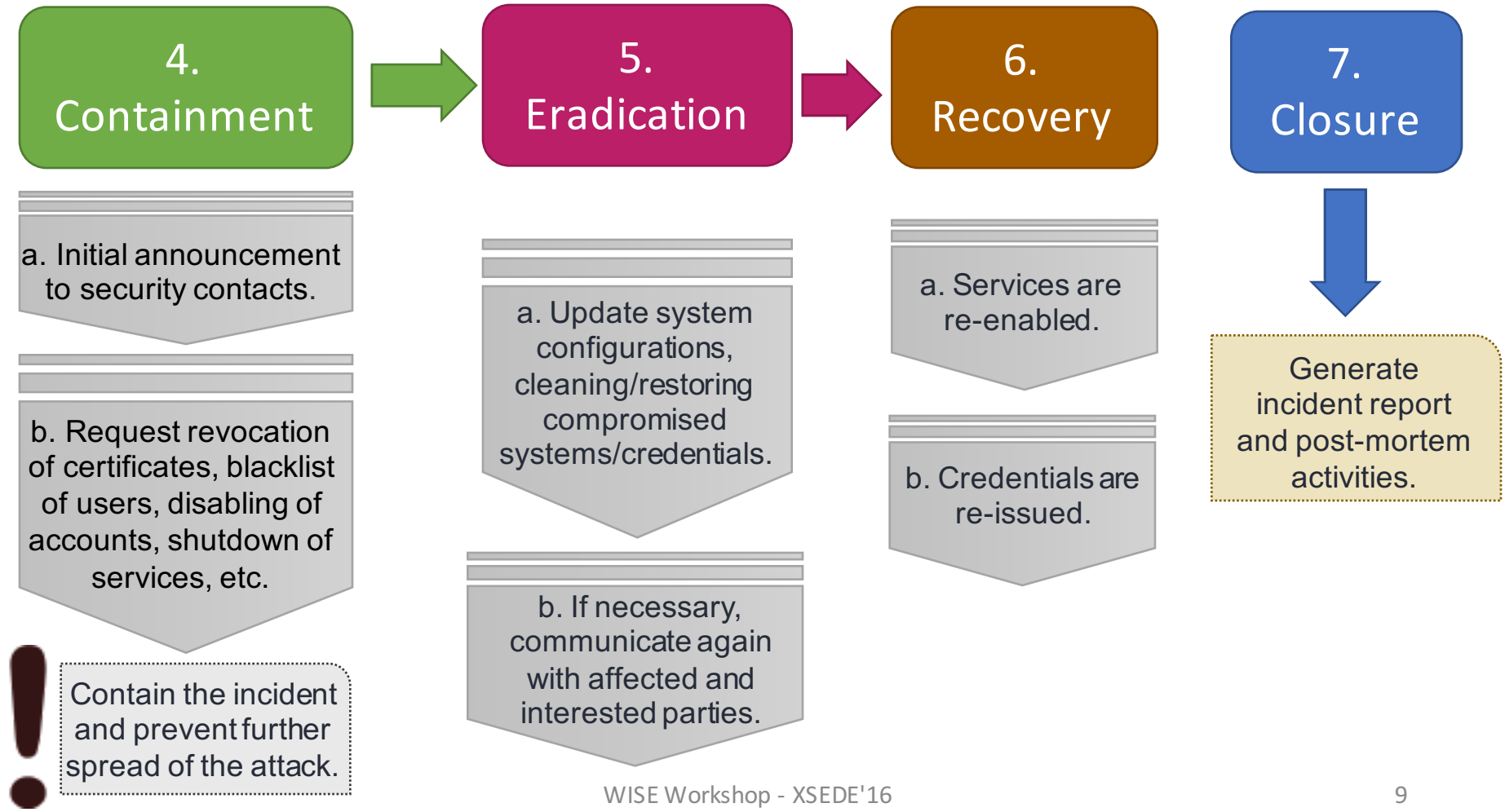
- In OSG, a security incident is an activity that compromises the security of OSG services, resources, infrastructures or identities.

Incident Management Response at OSG



Incident Management Response at OSG

Open Science Grid



Day-to-day Security Operations at OSG (1)

- Assess the software used at OSG:
  - Check security advisories and bulletins:
    - CVE - MITRE https://cve.mitre.org/
    - RedHat - https://access.redhat.com/security/security-updates/
    - Qualys - https://www.qualys.com/research/security-advisories/
    - EGI - https://wiki.egi.eu/wiki/SVG:Advisories
    - US-CERT - https://www.us-cert.gov/ncas/bulletins
    - OpenSSH - http://www.openssh.com/security.html
    - OpenSSL - https://www.openssl.org/news/newslog.html
  - After assessing the impact to OSG, announcements with instructions to follow are sent to the community.

Open Science Grid

Day-to-day Security Operations at OSG (2)

- Reports about vulnerabilities, bug and issues also come from other collaborations and research institutions:
  - XSEDE, WLCG, EGI, CERN, FNAL.
- Observe the practices of our VOs and sites :
  - If they need additional help with managing their users, access control management and/or identity management, they can contact the OSG Security Team.
  - We can either work on the problem with them or put them in touch with experts in this area depending on their needs.

Communication with other collaborations

- XSEDE
  - CILogon OSG CA is jointly operated by XSEDE and OSG.
  - XSEDE Incident Response weekly meeting.
  - XSEDE Security Operations biweekly call.
- CERN
  - A couple of incident reports received from Romain Wartel, CERN Security Officer.
- EGI
  - Software Vulnerability Group (SVG)
  - grid-sec mailing list.
- WLCG
  - Operations call

Identity Management at OSG

- OSG Operates a PKI with a Certificate Authority as a key component to provide certificates to users, hosts and services.
- Started collaborating with XSEDE recently to create the CILogon OSG CA:
  - Transition successfully completed on June, 2016.
  - Around 50 Virtual Organizations are now using certificates issued by CILogon OSG CA.

Identity Management at OSG

- Can we use a different, more user-friendly technology instead of certificates?
  - Perhaps we can hide certificates in the background?
- Federated identities: Providing certificates via users' home credentials.
  - Example: Access to computing resources with CILogon Basic CA for Intensity Frontier experiments at FNAL.

Questions?