# Coordinating Operational Security in evolving distributed IT-Infrastructures

**Sven Gabriel, Vincent Brillault**

EGI-Engage is co-funded by the Horizon 2020 Framework Programme
of the European Union under grant number 654142

Introduction

Elements of Operational Security

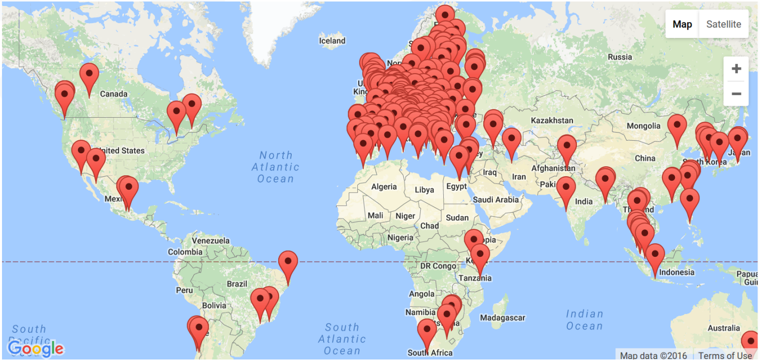
Incident Response in Evolving Infrastructures

# Introduction

# Introduction

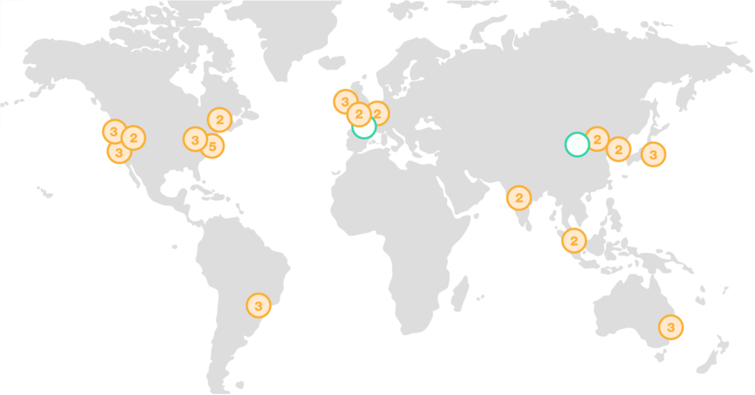
- What has to be coordinated, Elements of operational Security
- What are the requirements to do coordination
- Incident Response in evolving DIs

# Distributed Infrastructures, Examples



EGI: https://goc.egi.eu/portal/

# Distributed Infrastructures, Examples



Amazon https://aws.amazon.com/about-aws/global-infrastructure/

# Elements of Operational Security

# Elements of Operational Security

- Policy, development, enforcement (Define the perimeter)
- Provide Security Services (Security -Monitoring -Training -Drills, Vulnerability Assessment)
- Security Operations (Vulnerability Handling, Incident Response (incl. Forensics support))

# Governance/Management of Distributed Infrastructures

## Federative

- Ex.: EGI, largely autonomous sites.
- Federation agrees on policies
- Centrally distributed secure default configurations (ACLs, RCs), Final decision at site.

## Centrally Managed

- Commercial Providers, google, amazon etc
- Central body decides on policies
- Central Security/IR activities

# EGI-CSIRT central security services

- Sites are autonomous (final decisions/actions taken by the sites, examples:)
- EGI-CSIRT provides advisories on how to deal vulnerabilities
- EGI-CSIRT provides Security Monitoring
- EGI-CSIRT provides Incident Response coordination/support

# EGI-CSIRT central security services

No central roll-out of software pages, fabric management at the sites.

# EGI-CSIRT central security services

Central management . . .

# Just one of those days

- Central Operations, have a wide impact.
- 28th Feb 2017 Amazon Web Services (AWS) suffered an outage.
- . . . services like Netflix, Tinder, Airbnb, Reddit and IMDb offline.
- https://aws.amazon.com/de/message/41926/

# Just one of those days

http://www.datacenterdynamics.com/content-tracks/colo-cloud/aws-suffers-a-five-hour-outage-in-the-us/94841.fullarticle

# Just one of those days

- Central Operations, have a wide impact.
- 28th Feb 2017 Amazon Web Services (AWS) suffered an outage.
- ...services like Netflix, Tinder, Airbnb, Reddit and IMDb offline.
- https://aws.amazon.com/de/message/41926/
- **FedCloud Orchestration Services management?**

# Requirements for Security Coordinations

- Policy framework all adhere to
- . . . with options for enforcement
- advanced Communication infrastructure (do not rely on broadcasts)
- advanced Security Monitoring infrastructure
- Expert team to develop/maintain/run it.

# Challenges of Evolving Infrastructures

- evolve from a matured Infrastructure, use what already proofed to work well
- be careful with the sensitive components (Ex. Access Control to VMs)
- make sure new components are covered by a policy, have controls on software components
- EGI provides powerful tools, use them responsibly!

# Incident Response in Evolving Infrastructures

# Incident Response Task Force

- Small team: 7 people, partial time
- Highly distributed
- Main duties:
  - Incident coordination
  - Forensics capabilities
  - Critical vulnerability tracking

# Incident in 2015

- Compromised VM:
  - Very weak root password
  - Vulnerability present before contextualisation
- 2 compromised monitoring hosts:
  - Critical vulnerability in ElasticSearch
- Retired WLCG site root-compromised:
  - Stolen root credentials, SSHD trojan
  - Impacting our community: UI
  - Compromised accounts: CERN, China, Japan,...

# Vulnerabilities in 2015

| | |
|---|---|
| CVE-2014-9322 | Local escalation in Linux Kernel |
| CVE-2015-1815 | Local escalation in selinux tools |
| CVE-2015-3245 | Local escalation in libuser |
| CVE-2015-7181_2_3 | Remote execution in NSS |

# Vulnerabilities in 2016

CVE-2015-7547 Remote execution in libresolv

CVE-2016-1950 Execution via crafted certificate

EGI-SVG-2016-10837 dcache configuration issue

EGI-SVG-2016-11476 Impersonation in canl-c

CVE-2016-5195 Local escalation in Linux Kernel (*DirtyCow*)

# Incident in 2016 VMs - I

- User-compromised VM:
  - Bad tomcat configuration
- User-compromised VM:
  - Weak tomcat passwords
  - Created by shared contextualization script
- Compromised VM:
  - Vulnerability unclear (found reverse-shell)

# Incident in 2016 VMs - II

- Root compromised VM:
  - Bad NFS configuration (insecure export)
  - Same attacker as last 2015 incident
- Near-miss in VM:
  - Bad NFS configuration (insecure export)
  - Pushed by *orchestrator*
- Near-miss in VM 2:
  - Bad NFS configuration (insecure export)
  - Pushed by same *orchestrator*
  - Different copy of the same script

# Incident evolution in 2016
# VMs: return of basic issues

- Quite a few incident on VMs
- Very basic configuration issues
- VMs not maintained by System Administrators
- New problematic created by new players:
  - VM images maintained by users
  - Contextualization script maintained by users
  - Orchestration script maintained by users

→ Security audit and maintenance required on all levels

# Incident in 2016 Grid

- Root compromised host:
  - Attack vector unknown (old admin ssh key?)
  - *VENOM* backdoor found and analysed: `https://wiki.egi.eu/wiki/Venom_Rootkit`
  - Network traces of other systems
- Few systems administrator contacted directly
- Data shared with peers/publicly:
  - More than 25 compromised systems identified
  - Mostly in the astro-physics comunity

→ Collaboration with other (academic) communities critical!