IT Security Training for Distributed Infrastructures

S. Gabriel[1,2]

[1]Nikhef [2]EGI CSIRT

March 2026

What is this talk about . . .

Outline:

- Distributed IT infrastructures.
- Example: EGI
- How to identify gaps that benefit from training.
- How to address the gaps by a specific training..

What is this talk about . . .
Outline:
- Distributed IT infrastructures.
- Example: EGI
- How to identify gaps that benefit from training.
- How to address the gaps by a specific training..

Distributed IT infrastructures

Distributed:

- . . . in terms of location of services.
- . . . in terms of multi stake holders.
- what to do with entangled different distributed IT infrastructures.

Distributed IT infrastructures

Distributed:
- . . . in terms of location of services.
- . . . in terms of multi stake holders.
- what to do with entangled different distributed IT infrastructures.

1. Looking back, when we started the Grid (early 2000s), infras where usually part of a single organisation, maybe with a backup location to deal with business continuity, resilience, or disaster recovery aspects
2. Over the years and with the development of virtualisation technologies this concept is changing towards distributed services with centralized governance. (ex. Gmail, M365, AWS, Cloudflare, finance (blockchain), EDNs (streaming services ex Netflix, wikipedia), P2P file sharing, ... etc

EGI: Advanced Computing for a Data-Driven Future

We are the federation of computing and storage resource providers united by a mission of delivering advanced computing and data analytics services for research and innovation.[1]

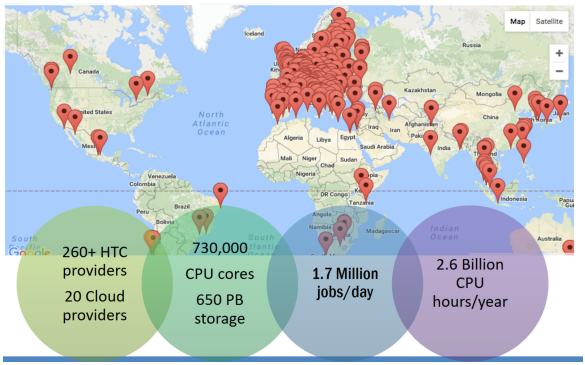
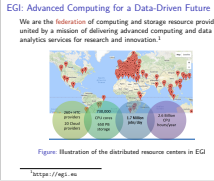


Figure: Illustration of the distributed resource centers in EGI

[1] https://egi.eu



1. While this picture shows the easy part, distributed compute resources, it also points to more challenging aspect of governance in a distributed multi stakeholder environment
2. Example: DNS

Federation of computing and storage resource providers

This implies distributed multi-stakeholders, for that one needs to clarify:

- Governance, Risk Management and Compliance (GRC).
- Agree on Responsibilities, (security) Policies, SLAs, MoUs
- IT Security Incident Response Procedures (response times, confidentiality, etc)

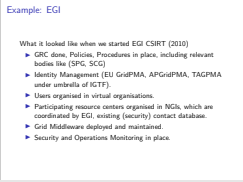
Federation of computing and storage resource providers
This implies distributed multi-stakeholders, for that one needs to clarify:
- Governance, Risk Management and Compliance (GRC).
- Agree on Responsibilities, (security) Policies, SLAs, MoUs
- IT Security Incident Response Procedures (response times, confidentiality, etc)

1. Governance: Sets the strategy and "rules of the game." It involves defining policies, assigning responsibilities, and ensuring that IT security supports the overall business objectives.
2. More or less the rules of participation.
3. Risk Management: The process of identifying, assessing, and responding to threats (like cyberattacks or data breaches). It helps organizations prioritize resources to tackle the most critical vulnerabilities first
4. Compliance: Ensures the organization follows external laws (like GDPR or NIS2) and industry standards (like FitISM, ISO 27001 or). This protects the company from legal penalties and reputation damage

Example: EGI

What it looked like when we started EGI CSIRT (2010)

- GRC done, Policies, Procedures in place, including relevant bodies like (SPG, SCG)
- Identity Management (EU GridPMA, APGridPMA, TAGPMA under umbrella of IGTF).
- Users organised in virtual organisations.
- Participating resource centers organised in NGIs, which are coordinated by EGI, existing (security) contact database.
- Grid Middleware deployed and maintained.
- Security and Operations Monitoring in place.



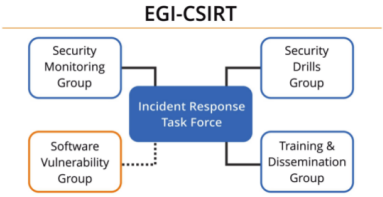
1. From a security viewpoint this looked pretty straight forward.
2. This is particularly note worthy, since I did the same for a different infrastructure, but with people who had an interesting management style.
3. if time allows tell the story of what "ja ja" means
4. So it seems the security team has everything in place, lets start

Example: EGI

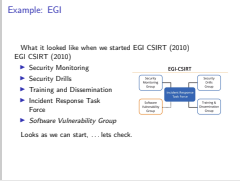
What it looked like when we started EGI CSIRT (2010)

EGI CSIRT (2010)

- Security Monitoring
- Security Drills
- Training and Dissemination
- Incident Response Task Force
- *Software Vulnerability Group*



Looks as we can start, . . . lets check.



1. In our context here, how can we provide the people dealing with training with information on *what to train*
2. *Answer: Do an assessment of the posture of the infra towards security*

Security Service Challenge to identify weak spots

Security Drill Framework allows for:

- Various job-submission methods, Storage operations.
- Defined set of tasks (Communication, User/Process management with target times)
- Automated Report generation / Scoring schema.
- Keep history/monitor Progress.

Security Service Challenge to identify weak spots
Security Drill Framework allows for:
- Various job-submission methods, Storage operations.
- Defined set of tasks (Communication, User/Process management with target times)
- Automated Report generation / Scoring schema.
- Keep history/monitor Progress.

Security Service Challenge to identify weak spots

- Per site training exercise.
  - "You are on your own", limited external information source
  - Training Site-operations, goal: improve/measure site response capabilities, procedures.
- Multi site incident simulation exercise.
  - Various information sources / focus on collaboration/information sharing

Security Service Challenge to identify weak spots
- Per site training exercise.
  - "You are on your own", limited external information source
  - Training Site-operations, goal: improve/measure site response capabilities, procedures.
- Multi site incident simulation exercise.
  - Various information sources / focus on collaboration/information sharing

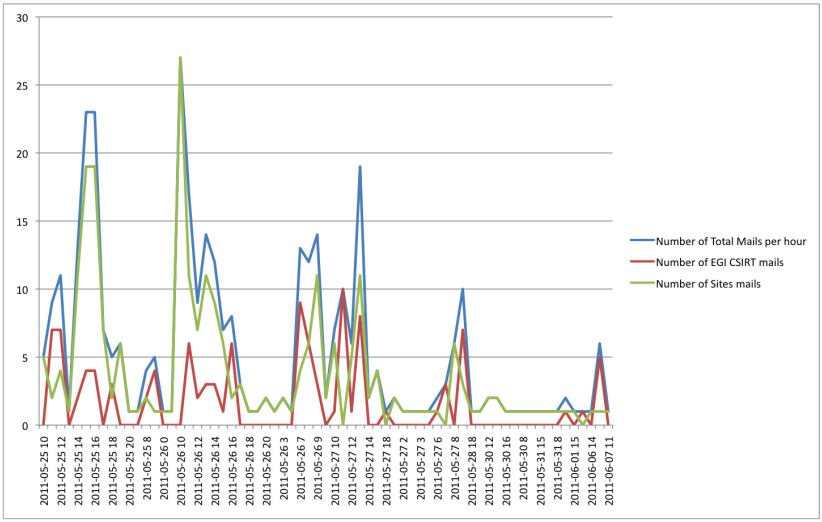
48h IR in 5min

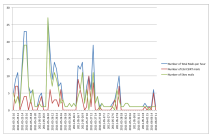
Feedback for Training and Dissemination

- Operational: Targeted response difficult.
- Containment had a serious impact on the availability.
- Access management at some sites not sufficient.
- High communication load on incident coordinators

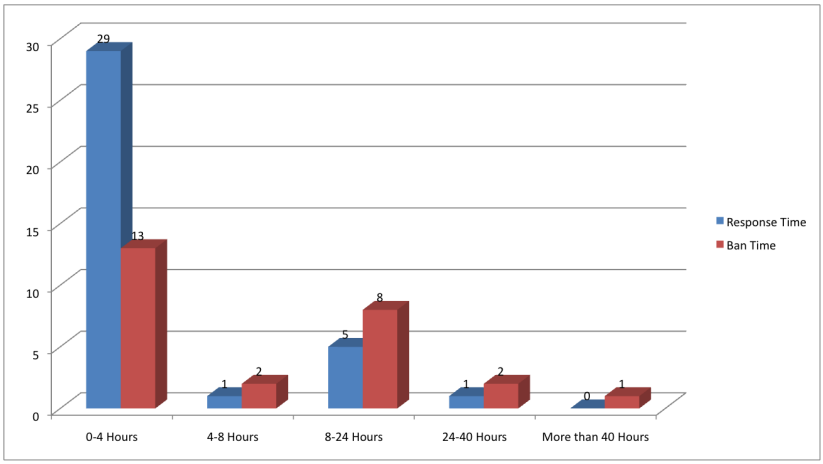
Feedback for Training and Dissemination
- Operational: Targeted response difficult.
- Containment had a serious impact on the availability.
- Access management at some sites not sufficient.
- High communication load on incident coordinators

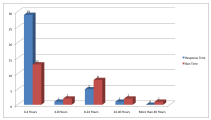
Feedback for Training and Dissemination





Feedback for Training and Dissemination





What to do with the results

What to do with the results

What to do with these results

- advanced admin skills not available everywhere.(provide means to share information from expert admins with the infra admins)
- Communication needs attention, Prepare Blue team to deal with high load, train resource centers on what are the relevant bits of information.
- Quality of information, not everyone is familiar with grid middleware (required for doing higher level forensics)
- Not all Resource Centers are aware of the importance of Central Logging
- Not all Resource Centers are aware of the importance of Vulnerability Management.

What to do with these results
- advanced admin skills not available everywhere.(provide means to share information from expert admins with the infra admins)
- Communication needs attention, Prepare Blue team to deal with high load, train resource centers on what are the relevant bits of information.
- Quality of information, not everyone is familiar with grid middleware (required for doing higher level forensics)
- Not all Resource Centers are aware of the importance of Central Logging
- Not all Resource Centers are aware of the importance of Vulnerability Management.

What to do with these results, PKI

External Distributed Infrastructure used for Identity Management (EU GridPMA, APGridPMA, TAGPMA under umbrella of IGTF)

- Lack of understanding how PKI works, we cannot just request to revoke a certificate.
- Crucial role for the VOs, they can suspend Identities (DNs)
- Authorization decision is ultimately with the Resource Centers, knowledge of the dedicated tools not available everywhere.
- Deploy central suspension system.

What to do with these results, PKI
External Distributed Infrastructure used for Identity Management (EU GridPMA, APGridPMA, TAGPMA under umbrella of IGTF)
- Lack of understanding how PKI works, we cannot just request to revoke a certificate.
- Crucial role for the VOs, they can suspend Identities (DNs)
- Authorization decision is ultimately with the Resource Centers, knowledge of the dedicated tools not available everywhere.
- Deploy central suspension system.

1. capability to centrally lift suspension is equally important
2. If all RCs modify their local access policies has a high risk of creating a mess, at latest when it comes to reinstating of credentials.
3. this is part of another infrastructure we silently made part of ours without making clear that these have completely different responsibilities, tasks goals. An ID must not revoked, just because it misbehaves, rather this offers a way to follow it. Revocation only makes sense when the identity is breached, i.e. someone else impersonate herself as someone else.

Technical Training organised as a response to the results

- ISGC 2013 (Probably); CTF like forensics training (Leif Nixon)
- ISGC 2014; best practices in System/Cluster security configuration
- ISGC 2015; Security Monitoring, Central Logging.
- ISGC 2016; Mechanisms of Inter-Federation, Trust Assurance an.d Policy for Federation
- ISGC 2017 IT Security Incident handling in Federated Clouds.
- ISGC 2018 Forensics on memory/persistent storage.
- ISGC 2021 Container Security
- ISGC 2022; Forensics training in a virtualised environment (VMs, Containers D. Kouřil and colleagues
- ISGC 2023 SOC deployment
- ISGC 2025 IT Security Risk Management; Collaborative Operational Security WLCG SOC WG.

Technical Training organised as a response to the results
- ISGC 2013 (Probably); CTF like forensics training (Leif Nixon)
- ISGC 2014; best practices in System/Cluster security configuration
- ISGC 2015; Security Monitoring, Central Logging.
- ISGC 2016; Mechanisms of Inter-Federation, Trust Assurance an.d Policy for Federation
- ISGC 2017 IT Security Incident handling in Federated Clouds.
- ISGC 2018 Forensics on memory/persistent storage.
- ISGC 2021 Container Security
- ISGC 2022; Forensics training in a virtualised environment (VMs, Containers D. Kouřil and colleagues
- ISGC 2023 SOC deployment
- ISGC 2025 IT Security Risk Management; Collaborative Operational Security WLCG SOC WG.

1. 2020 was the ¡corona year, only a very small group of people in TPE

Table-Top Training organised as a response to the results

- ISGC 2016 IT Security Incident Response in the Grid environment involving Federated Identity Management
- ISGC 2019 Developing Incident Response in a federated environment, a hands-on approach.
- ISGC 2024 Inter federation incident response (IR) in eduGAIN

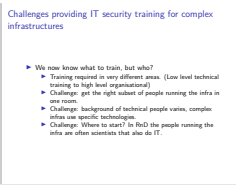
Table-Top Training organised as a response to the results
- ISGC 2016 IT Security Incident Response in the Grid environment involving Federated Identity Management
- ISGC 2019 Developing Incident Response in a federated environment, a hands-on approach.
- ISGC 2024 Inter federation incident response (IR) in eduGAIN

Summary

Summary

Challenges providing IT security training for complex infrastructures

- We now know what to train, but who?
  - Training required in very different areas. (Low level technical training to high level organisational)
  - Challenge: get the right subset of people running the infra in one room.
  - Challenge: background of technical people varies, complex infras use specific technologies.
  - Challenge: Where to start? In RnD the people running the infra are often scientists that also do IT.



1. In the training we often have very experienced people and others more or less starting
2. Usually the skilled technical people, are not too interested in the more high level aspects
3. Security Operations as multiple aspects of equal importance, a more high level example is communications
4. Some trainers from EGI CSIRT also teach TRANSITS courses (3 full days) covering Organisational, Operations, Communications and Technical aspects of IT security operations, so we came to the idea to develop a complete training, which would prepare the trainees to help developing/building a defensible distributed IT infrastructure

Training towards a defensible distributed infrastructure

This is basically what we did for this years ISGC ...

- IT Security Risk Management (Governance, Responsibilities, Compliance, what to defend and how)
- Secure Architecture
- Identity Management
- Incident Prevention and Detection (Vulnerability Management, Security Monitoring, SOC)
- Security Operations and IT Security Event/Incident Management
- Forensics

Training towards a defensible distributed infrastructure
This is basically what we did for this years ISGC ...
- IT Security Risk Management (Governance, Responsibilities, Compliance, what to defend and how)
- Secure Architecture
- Identity Management
- Incident Prevention and Detection (Vulnerability Management, Security Monitoring, SOC)
- Security Operations and IT Security Event/Incident Management
- Forensics

1. Goal is to make the participants think of what is needed to build a defensible infra, provide contacts who to ask for comment/help
2. Also, this could serve as a start to organize the ISGC Security Workshop with more contributions from APAC, and by that foster our collaboration in operational security in world wide distributed IT infras, like wlcg, eduGAIN, ...