Security operations

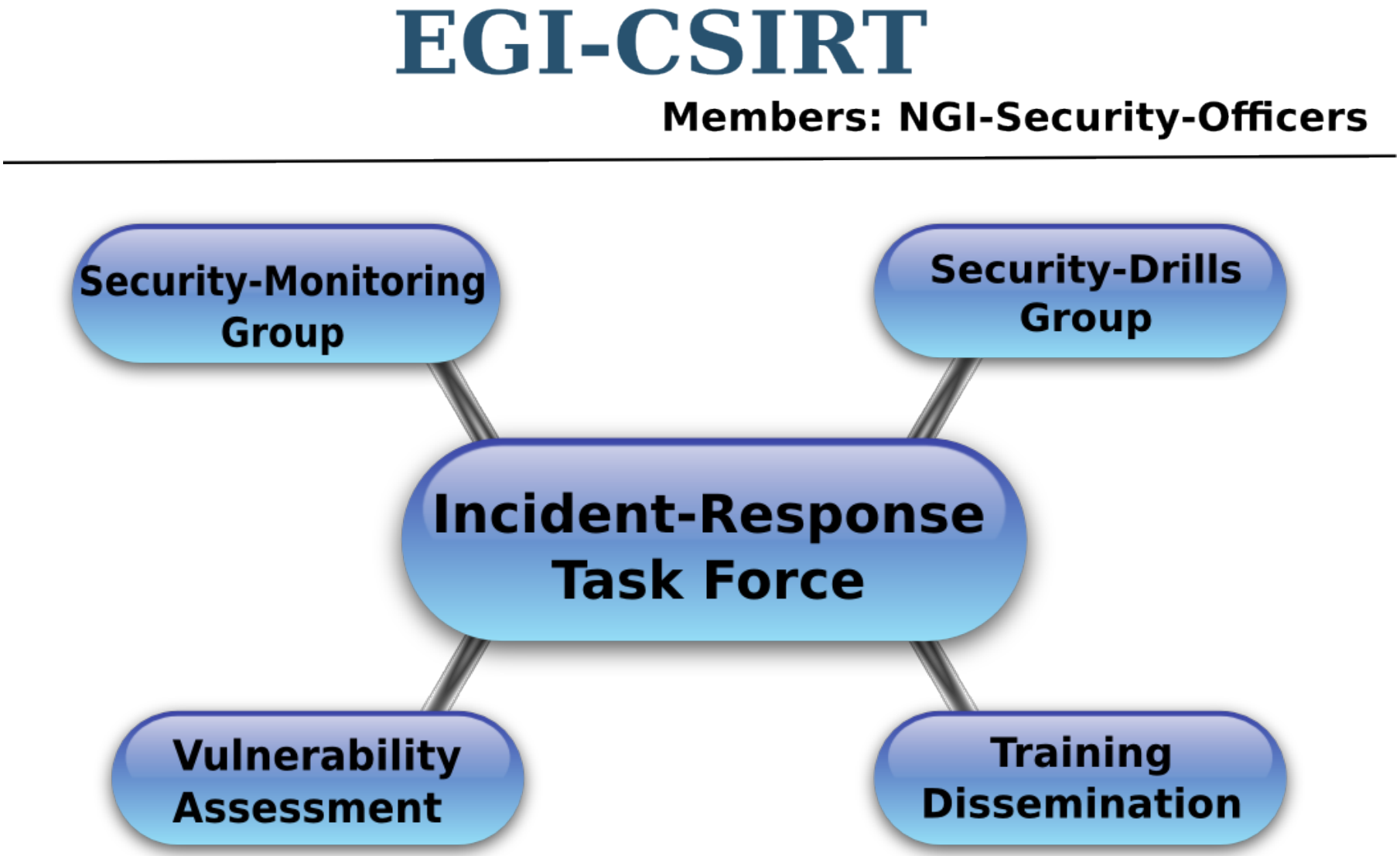
Sven Gabriel, Nikhef, EGI CSIRT

Oct 2023

Overview

EGI CSIRT

EGI-CSIRT



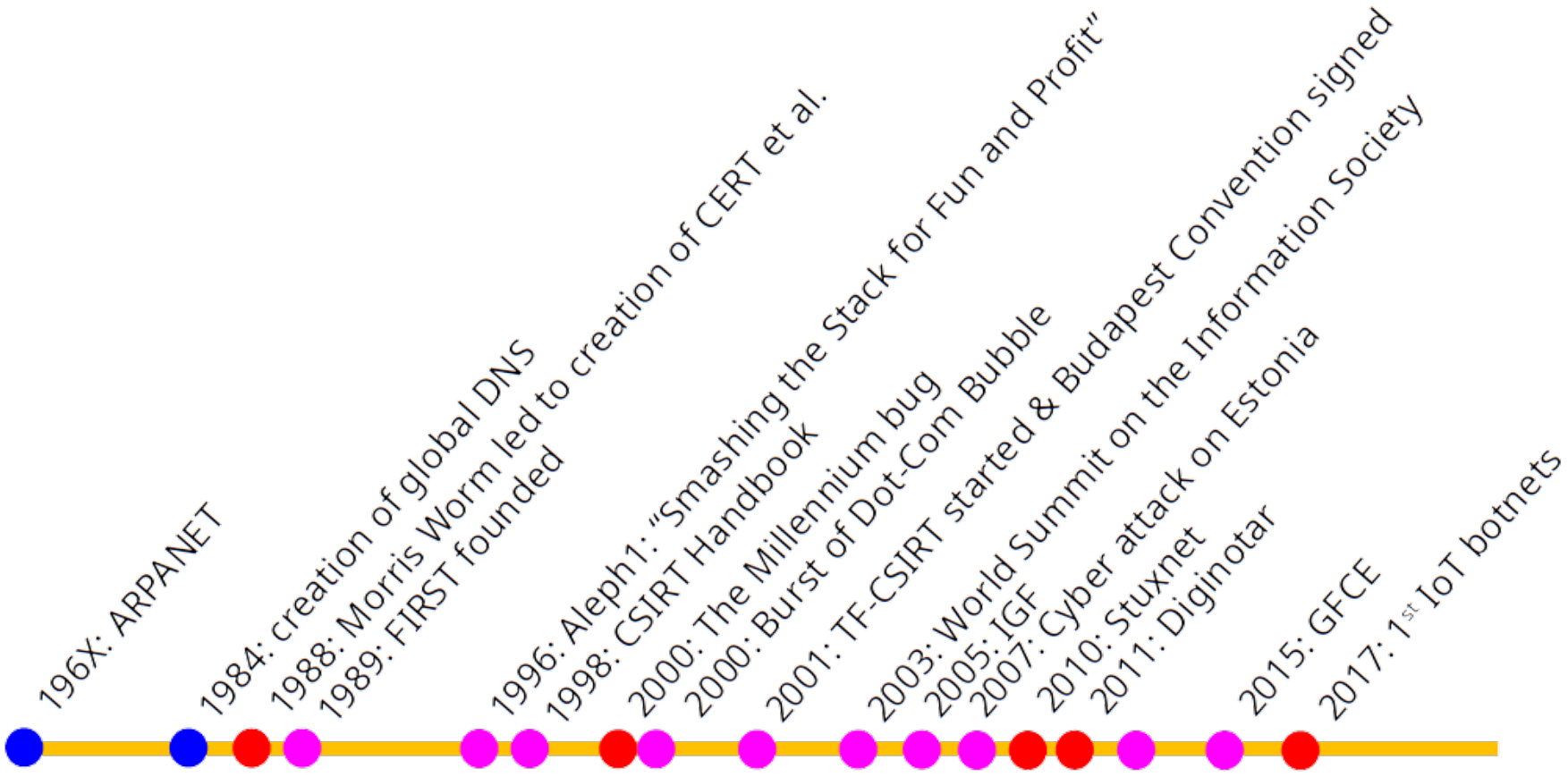
https://csirt.egi.eu

Some aspects of Operational Security

Reliable Systems

- Threat to reliability (availability).
  - Bad software update
  - Hardware failures
  - Issues tracked with a Ticket-System
- Threat to security
  - Vulnerabilities
  - Adversary actively exploiting the system, affecting CIA triad.
  - Issues tracked with a Ticket-System (the same as above?)

Security Teams, . . . a look back [1]



[1] Timeline courtesy FIRST

additional "entertaining" reads

- https://en.wikipedia.org/wiki/The_Cuckoo%27s_Egg_(book)
- https://en.wikipedia.org/wiki/23_(film)
- https://www.youtube.com/watch?v=fj8S6Hd-5bk

Security Teams and Incident Management

Terminology:

- CERT: Computer Emergency Response Team
  - Origin 1988, later trademarked
  - CERT Coordination Center (CERT/CC)
  - Permission to use: http://www.sei.cmu.edu/legal/permission/index.cfm
- CSIRT: Computer Security Incident Response Team
  - Origin 1998: http://www.cert.org/archive/pdf/csirt-handbook.pdf
  - Free to use !
- IHT, SIRT, CIRT, IHC, SOC (a story in itself), etc. etc.

CSIRT Organisation and provided Services

CSIRT Management

Managerial and technical aspects of CSIRT Management are topics in TRANSITS I trainings.

- Organisational and Technical module are half day courses.
- check https://tf-csirt.org/transits/transits-events/transits-i/
- Here we will cover just a subset of the topics.

CSIRT Services I

The services a CSIRT should provide and the needed tooling depends on the mandate of the CSIRT, examples.

- Coordinating CSIRT
  - eduGAIN CSIRT, needs a communication infrastructure to coordinate incident response activities among the participants.
  - EGI CSIRT, coordinating security activities for EGI. In addition to the communications infra, + a lot more
  - How to efficiently do threat intel sharing?
- Organisation/Company CSIRT
  - Constituency is defined easier.
  - Stronger mandate, organisation can more easily decide on policies.

Talking to a CSIRT

Trust, Transparency, What to expect from a CSIRT $\rightarrow$

- RFC-2350.
- TermsOfReference (TOR): Mandate/Authority given to the CSIRT, Responsibilities of the CSIRT.
- Responsible disclosure: RFC-9116 (security.txt).

CSIRT Services revisited, EGI

- Incident Management (tested and maintained Communications infra)
- Forensics support (malware analysis)
- Vulnerability Management (separate talk)
- Trainings (see Intro to forensics)
- Intel sharing, WLCG-SOC (more in the SOC session)
- Security Challenges (not really pen tests, rather an assessment of the security situation).

CSIRT Communities

- Now, that you have a CSIRT with a mandate, public contact info for reporting security issues, you now would need to collaborate with other CSIRTs. For example participating in:
- TF-CSIRT https://tf-csirt.org/
- FIRST https://www.first.org/
- Sectoral Communities (PSIRTs, Critical Infra, National CSIRTs, etc)
- Trust Groups (based on personal peer-to-peer trust relations)

Drivers for CSIRT Evolution

CSIRT Evolution

Drivers for Security Initiatives:

- (External, or self) Audit of the security framework (ISO 27k, SIM3[2])
- Compliance: Information Security regulations have to be met, for example in call for tenders [3]
- Risk Management (see later talk)

[2] https://opencsirt.org/csirt-maturity/sim3-and-references/

[3] https://www.surf.nl/en/stitch-a-short-checklist-for-application-security

Security Operations

Incident Response, get prepared

- Have your communications ready (users, escalation to management, legal, press). Update stakeholders frequently. (Crisis communication as a course in itself, you would need to deal with social media.)

Incident Response, get prepared

- Have your communications ready (users, escalation to management, legal, press). Update stakeholders frequently. (Crisis communication as a course in itself, you would need to deal with social media.)
- Security Monitoring, do you have a baseline of normal system behaviour? Do you monitor the patch status of your systems?

Incident Response, get prepared

- Have your communications ready (users, escalation to management, legal, press). Update stakeholders frequently. (Crisis communication as a course in itself, you would need to deal with social media.)
- Security Monitoring, do you have a baseline of normal system behaviour? Do you monitor the patch status of your systems?
- Have your Infra ready. Network segmentation. Can you find and isolate systems on your network, Central User/Password management: can you act on any user account. Can you trace activities (on systems and network) back to accounts.

Incident Response, prepare to fail

- Every Incident Response is challenging your CSIRT set-up, **Use Them!**
- You will find weak points in:
  - Tooling (Communication Infra (ticket system etc) and all other services you provide.
  - Policies
  - Procedures
- All the above are subject to constant review and development, start from a decent environment and evolve.

Lessons learned from Incidents

Examples why to prepare to fail

The incidents and Security Challenges discussed in this section are not limited to incidents handled by EGI CSIRT.

- Attack on EGI Confluence . . . and then the documentation and mail infra went dark
- . . . and then the other end got silent
- Crypto Currency mining using grid technology . . . and then an insider thought he could smart out the forensics team.

Subsection 1

Attack on EGI Conflence

EGI-20190411-01

To understand the impact of this incident better, lets look at the services EGI CSIRTs Incident Response Task Force uses:

- Mail: Communication to Resource Centres
- Ticket system: RT-IR
- Private Wiki

Atlassian Confluence attack

- March 20^{th}: Critical vulnerability published
- Week of April 8^{th}: Multiple Confluence attacks: EGI and at least two close organizations affected
- At least two confirmed different attackers:
  - One had the exact same methodology as Jenkins

$\rightarrow$ Wide-scale successful attack within 3 weeks!

EGI services compromise
Timeline (April 2019)

- 4^{th}: Very first attempt to use the vulnerability
- 8^{th} afternoon: First confirmed attack
- 9^{th} and 10^{th}: Further attack activities
- 10^{th} lunch time: Attack detected
  - Malicious processes quickly isolated
- 10^{th} evening: Vulnerability patched
- 17^{th}: Servers rolled-back to safe backup

EGI services compromise

Impact

- Confluence co-hosted with various services
  $\rightarrow$ all co-hosted services affected
- Forensics analysis shows no sign of data exfiltration
- LDAP service not hosted on same service
  - LDAP passwords (hashed) not directly affected
  - Password of users who logged in on services with password potentially leaked (but no evidence)
- Forceful backup roll-back to safe backup
  - Data from April 3^{rd} to 17^{th} initially *lost*
  - Ongoing efforts to re-inject all data

Who is actually handling this incident?

- EGI CSIRT provides Operational Security for the Grid Sites in goc-db
- EGI CSIRT relies on services operated in EGI Back-Office
- A good example for legacy infra (10 years). Admin task was handed over multiple times, Experience, documentation lost. The last one who took this job had the hot potato, and some sleepless nights.
- Unclear responsibilities, who handles the incident, now sorted.
- Secure system operation will be discussed later this week.
- Risk Assessment: the risk from this set up would probably not been accepted.

Always have a fallback

- Standard communications were not available.
- Have multiple alternatives (IM like signal, keybase, mattermost) for trusted team communications.
- Collaboration tools not available (Wiki)
- Here we could move to gitlab (hosted elsewhere)
- Don't have all eggs in one basket

Stakkato incident

Get the full story at https://www.nsc.liu.se/~nixon/stakkato.pdf Here just the "highlights", imagine the case you are working on ends up in ...

Stakkato incident

Stakkato incident

The broader view

Some of the sites/companies/providers known to have been at the receiving end of an attack:

berkeley.edu
bonet.se
brandeis.edu
bredbandsbolaget.se
brown.edu
bu.edu
cam.ac.uk
cern.ch
chalmers.se
cisco.com
columbia.edu
csbnet.se
desy.de
epfl.ch
gatech.edu
iastate.edu
jhu.edu
ki.se
kralovopolska.cz
kth.se
liu.se
liv.ac.uk
lu.se
mit.edu
naqua.se
nasa.gov
nikhef.nl
pitt.edu
rr.com
rutgers.edu
sdsc.edu
seagull.net
simons-rock.edu
skanova.com
skogsbrynet.se
songnetworks.se
stanford.edu
technion.ac.il
telia.com
uchicago.edu
uci.edu
ucolorado.edu
ucsc.edu
ucsd.edu
uiuc.edu
umea.se
umearc.se
umn.edu
umu.se
unige.ch
uta.fi
utk.edu
uu.se
wsmr.army.mil

This is just a small sample; from August 2003 through March 2005 something like a thousand sites were attacked.

Stakkato incident

Takeaways. (This was in 2006, the "same" malware appeared later again.)

- Have sufficient log verbosity in sshd.
- Preferably no password auth.
- Watch out for ssh keys without password.
- Manage from cron (at least) the ssh keys in the privileged accounts.
- The concept is still popular, prepare for response (being able to react to compromised accounts).

The French Case

- RC Admin spotted unusual load patterns on WNs, running strings on binary pointed to crypto currency mining. $\rightarrow$ INTRUDER ALERT
- adversary used grid technology (WMS, CE, WN) to submit crypto currency mining jobs to the grid. All jobs could be traced back to a UI machine in F.
- AuthnZ via x509 personal certificates. Traces left on all elements of the job submission chain (repudiation rather difficult).
- It was possible to attribute $\approx$ 100 core years to this activity. Worth a second look.

The French Case, Scanning available data

- Accepted password for root from 202.6.92.8
- Various malware found (ssh password brute-force scanner).

The French Case, Scanning available data

- Accepted password for root from 202.6.92.8
- Various malware found (ssh password brute-force scanner).
- Forensics team got image of the host in question **and** network logs (flow data)

The French Case, Scanning available data

- Accepted password for root from 202.6.92.8
- Various malware found (ssh password brute-force scanner).
- Forensics team got image of the host in question **and** network logs (flow data)
- Wait a moment, system logs and network logs don't match

The French Case, Scanning available data

- Accepted password for root from 202.6.92.8
- Various malware found (ssh password brute-force scanner).
- Forensics team got image of the host in question **and** network logs (flow data)
- Wait a moment, system logs and network logs don't match
- A look, this IP from China was never used/routed

The French Case, Forensics

- ctime of the rotated /var/log/secure$*$ are different
- Various malware found (ssh password brute-force scanner).

The French Case, Forensics

- ctime of the rotated /var/log/secure$*$ are different
- Various malware found (ssh password brute-force scanner).
- filesystem journal showed the last commit blocks had a slightly different (newer format) then the rest, . . . with timestamps. This happens when you mount a filesystem on a system with a newer kernel.

The French Case, Forensics

- ctime of the rotated /var/log/secure* are different
- Various malware found (ssh password brute-force scanner).
- filesystem journal showed the last commit blocks had a slightly different (newer format) then the rest, . . . with timestamps. This happens when you mount a filesystem on a system with a newer kernel.
- The last 2 logins (after the incident was discovered) apparently legitimate. First one is missing in /var/log/secure, only found /var/log/lastlog

The French Case, Forensics

- ctime of the rotated /var/log/secure* are different
- Various malware found (ssh password brute-force scanner).
- filesystem journal showed the last commit blocks had a slightly different (newer format) then the rest, . . . with timestamps. This happens when you mount a filesystem on a system with a newer kernel.
- The last 2 logins (after the incident was discovered) apparently legitimate. First one is missing in /var/log/secure, only found /var/log/lastlog
- System logs are clearly tempered with, *after* the incident was discovered. No backdoors etc discovered

The French Case, Forensics

- ctime of the rotated /var/log/secure* are different
- Various malware found (ssh password brute-force scanner).
- filesystem journal showed the last commit blocks had a slightly different (newer format) then the rest, . . . with timestamps. This happens when you mount a filesystem on a system with a newer kernel.
- The last 2 logins (after the incident was discovered) apparently legitimate. First one is missing in /var/log/secure, only found /var/log/lastlog
- System logs are clearly tempered with, *after* the incident was discovered. No backdoors etc discovered
- Reconstructed timeline clearly showed that the "evidences" (rootkit, ssh-scanner) were placed after the incident was reported.

The French Case, conclusion

Conclusion?

Subsection 2

Highly Sensitive Incidents

No slides here

Intentionally left blank

Subsection 3

Incidents with media attention

Uni Maastricht, Ransom Attackd

- Uni Maastricht was very open about the incident
- 2h of public(recorded (in Dutch)) debriefing Youtube https://www.youtube.com/watch?v=ik-ZVvZ2-xU, here also payment of ransom is discussed! including the process on how to pay via bitcoin, proof that data can be decrypted.
- FOX-IT called in for support.
- Debriefing also has a report from FOX-IT including how they organised Incident Response, and what actions the victim should take to prevent future incidents. https://www.maastrichtuniversity.nl/file/49750/download?token=cT_19j-W

How it began . . .

- Night 23rd - 24th Dec. 2019 Uni Maastricht calls FOX IT.
- Intrusion (via phishing) happend on Oct. 15, various activities of the attackers could be reconstructed.
- Some Servers not reachable because of an ransomware attack.
- On 24th Dec 16:00 FOX IT starts assisting in the incident response process.
- 1st Phase support of Crisis management, start forensic investigation, goal: find out how the attack was done.
- Priority on busines continuity.

Uni Giessen, Response and Media attention

Bei der Ausgabe der neuen Passwörter kommt es zum Teil zu langen Schlangen. FOTO: LKL © Lena Karber

. . . oh, and is the response really targeted/balanced? [4] [5]

[4] https://www.degruyter.com/document/doi/10.1515/abitech-2022-0005/html

[5] https://www.bbc.com/news/technology-50838673

Subsection 4

Security exercises

Results from earlier exercises

- Outdated contact data → Run Communication Challenges
- Poor quality of report's → Provide Communication templates
- Slow responses → Response times covered in Incident Response procedures
- Insufficient knowledge in forensics → Provide Instructions, Trainings

Assessment of Incident Response readiness

Layout:

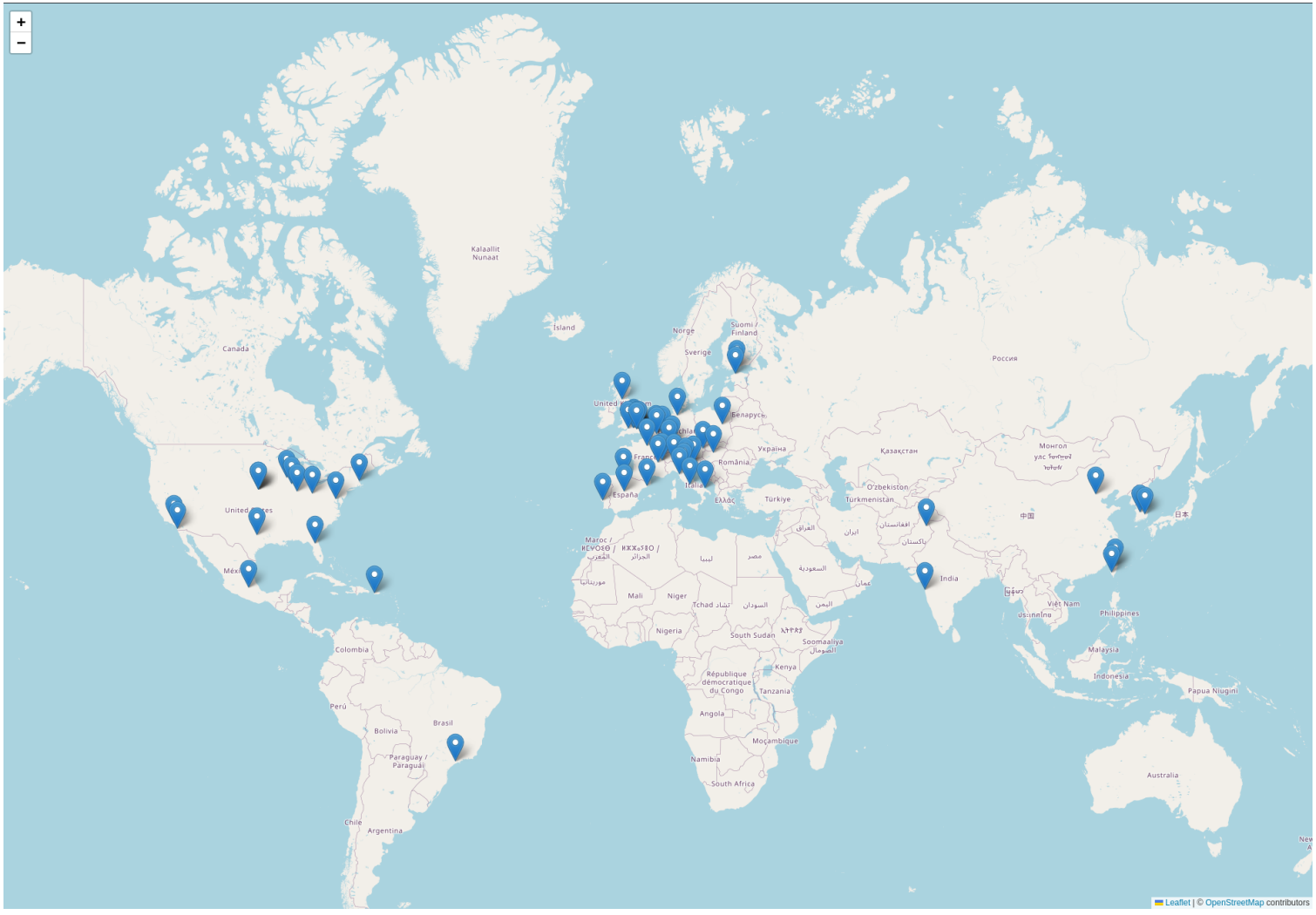
- Realistic Simulation of an Incident involving CSIRTS 58 Resource Centers 4 Organisations (EGI, OSG, eduGAIN, CMS VO).
- Malware (Bot-Net) was deployed with help of a VO-Job-Submission Framework.
- Attack Infra ran on VMs, started under identities from social media, Federated IdP.
- Massive coordination problem.

Assessment of Incident Response readiness

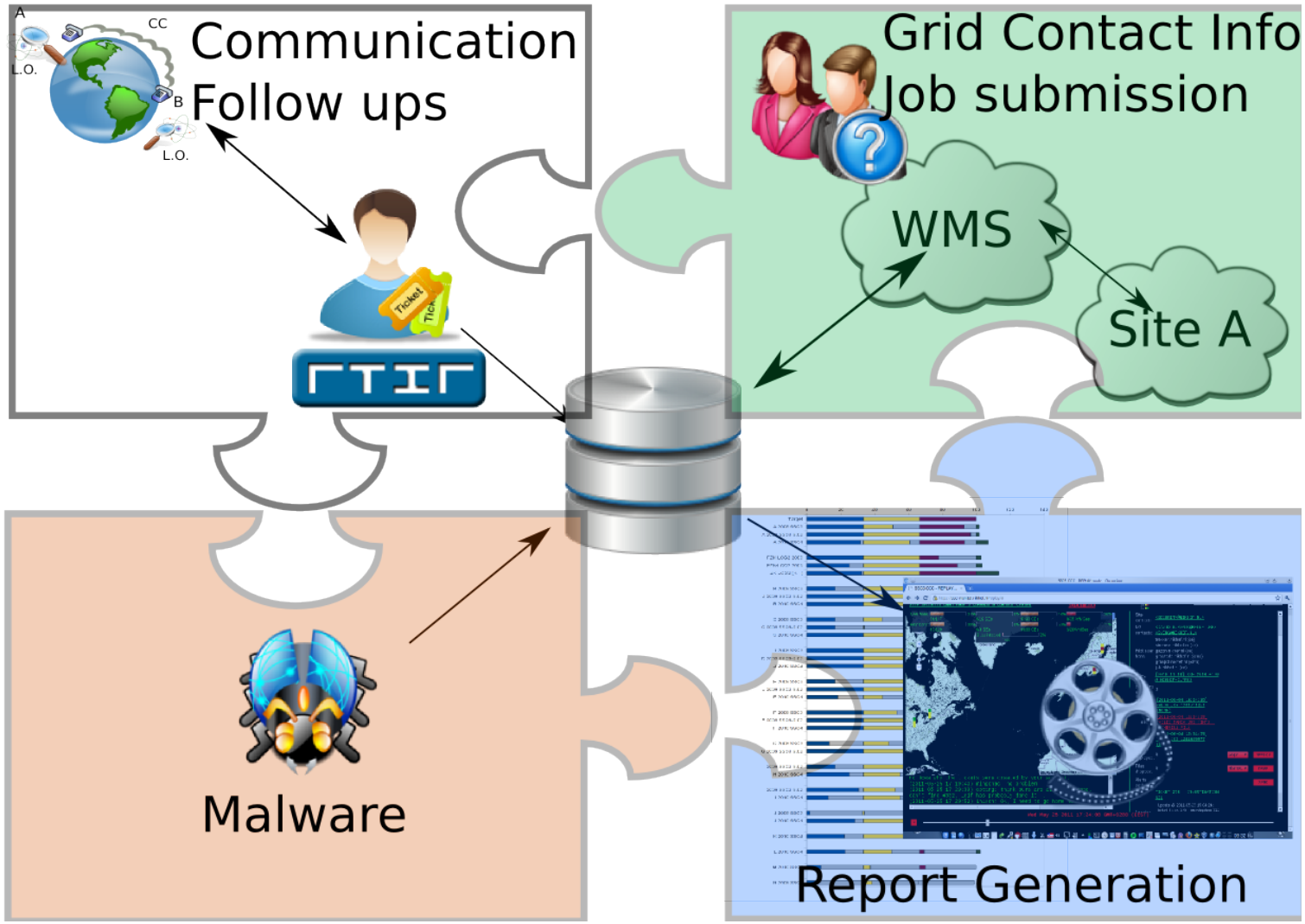
Targets/Expected Results:

- Project wide incident response capabilities.
- Trigger ad hoc Collaboration (EGI-CSIRT, VO-CSIRTS, CAs, ...).
- How long does it take to get the incident contained?
- Efficiency of security operations?
- Effects on the resource availability?
- Operational Problems in Incident Handling?
- Identify Experts: Forensics, Network-Analysis
- Assessment of tools used

Exercise playground: EGI, OSG, CMS, US-CMS Security (2023)



Assessment Framework Components



Subsection 5

Results

Results, what was evaluated

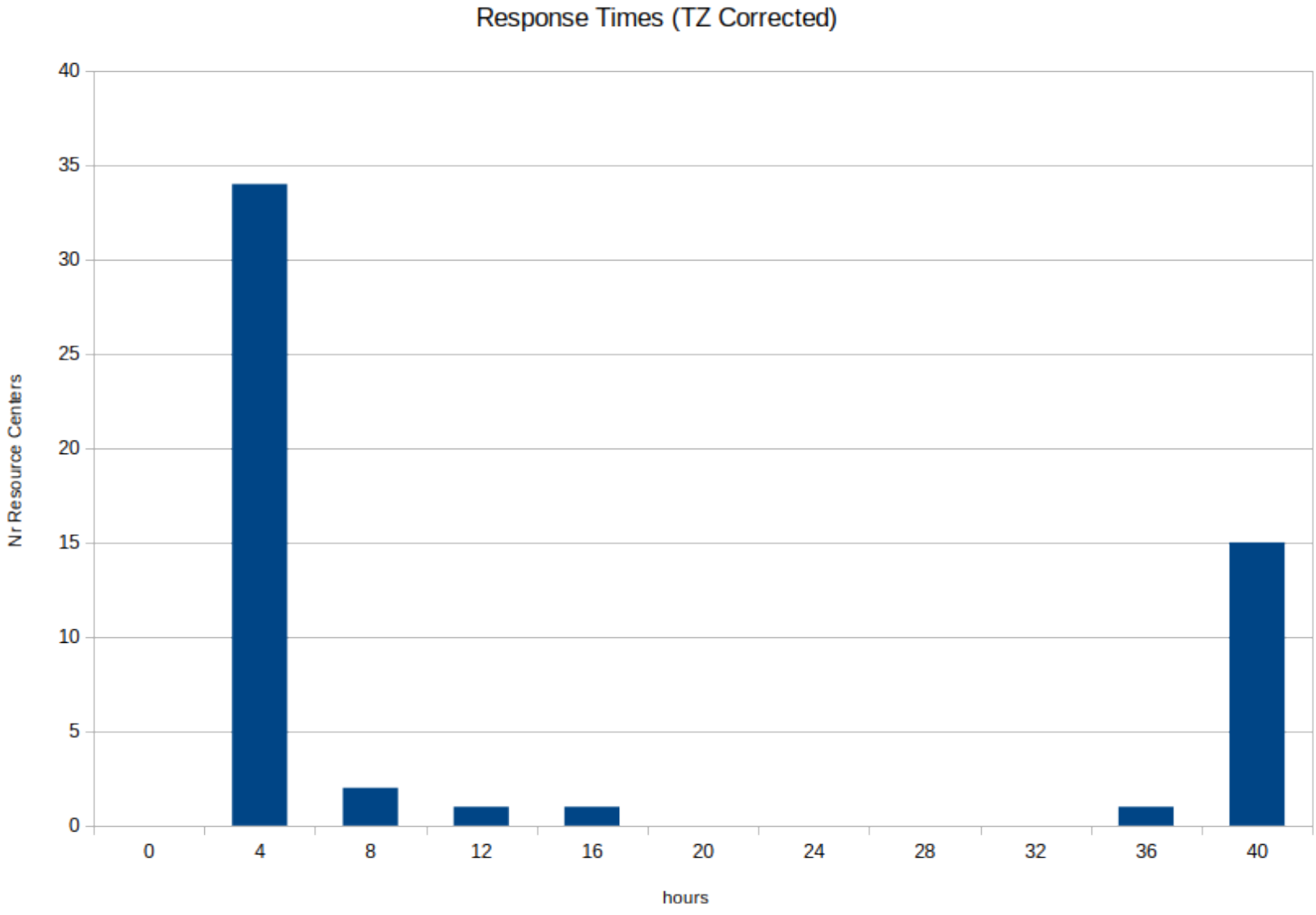
Goal: Assessment of the Incident Response capabilities at the Resource Centers

- Communications: Response times
- Containment: Stop malicious processes, suspend reported credentials
- Forensics: On/Offline forensics of the malicious processes running at the resource center. Capture The Flag, participation optional.

Subsection 6

Resource Centers Response Times

Communications, Response Times

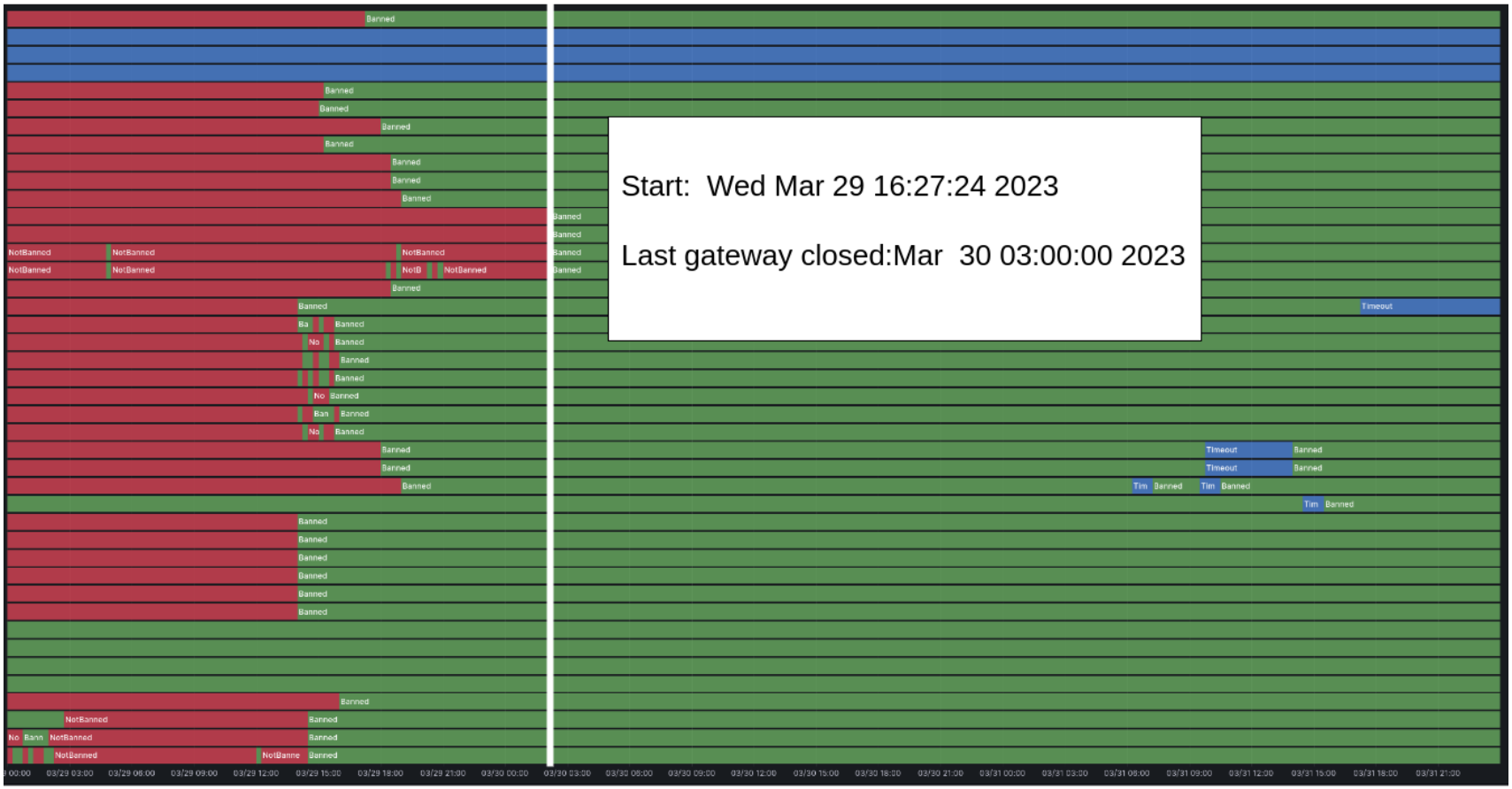


Subsection 7

Resource Centers Incident Response capabilities

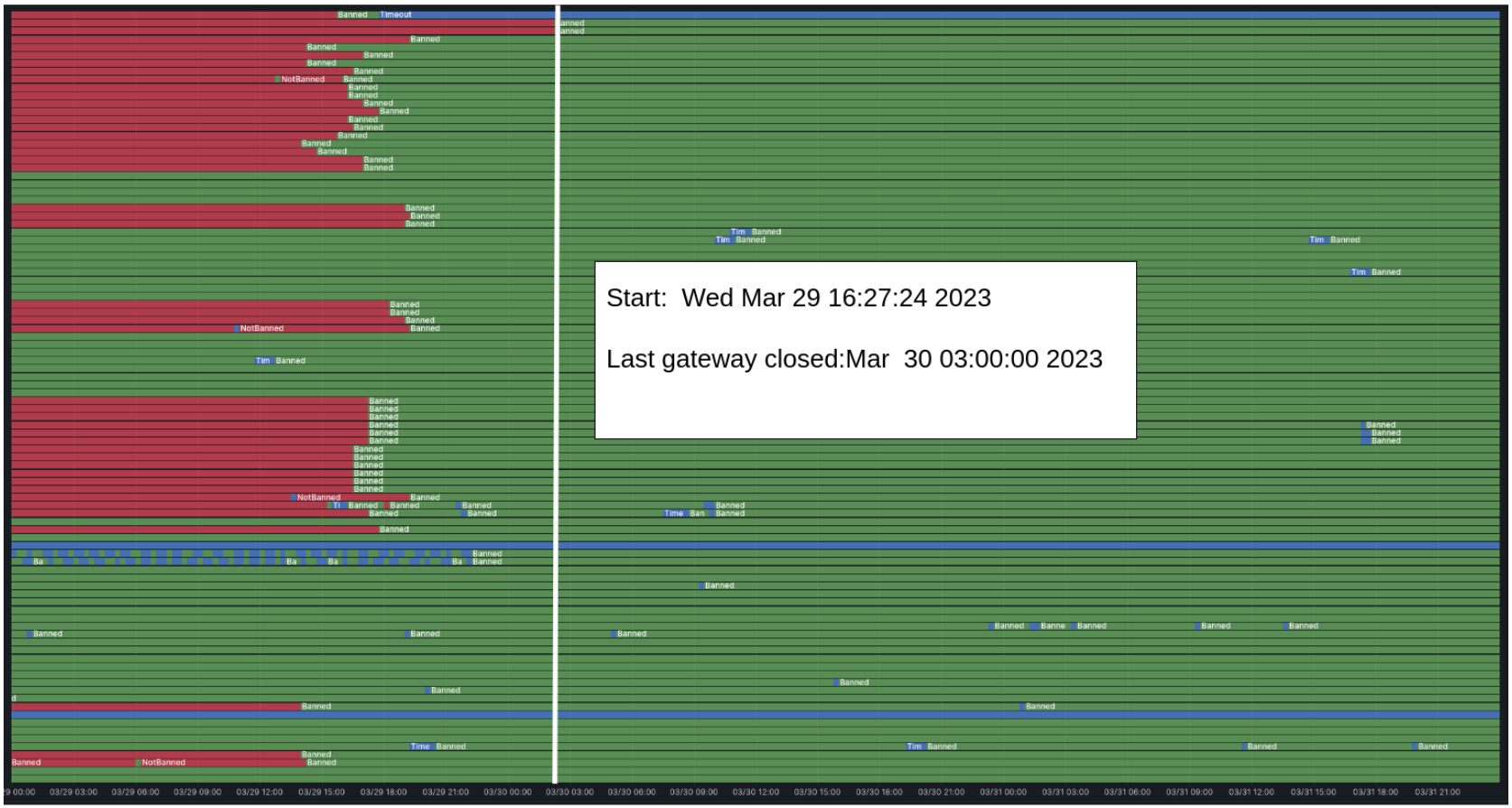
Containment, Suspend malicious credentials

Gateway system 1, local resource security teams, certificate revoked: Wednesday, March 29, 2023 13:17



Containment, Suspend malicious credentials

Gateway system 2, local resource security teams, certificate revoked: Wednesday, March 29, 2023 13:17



Containment, Stop malicious processes

Kill the botnet, local resource security teams.

Containment on Cloud Infra

Stop malicious virtual machines. Kill the attack infrastructure, C2, Content delivery network, ...

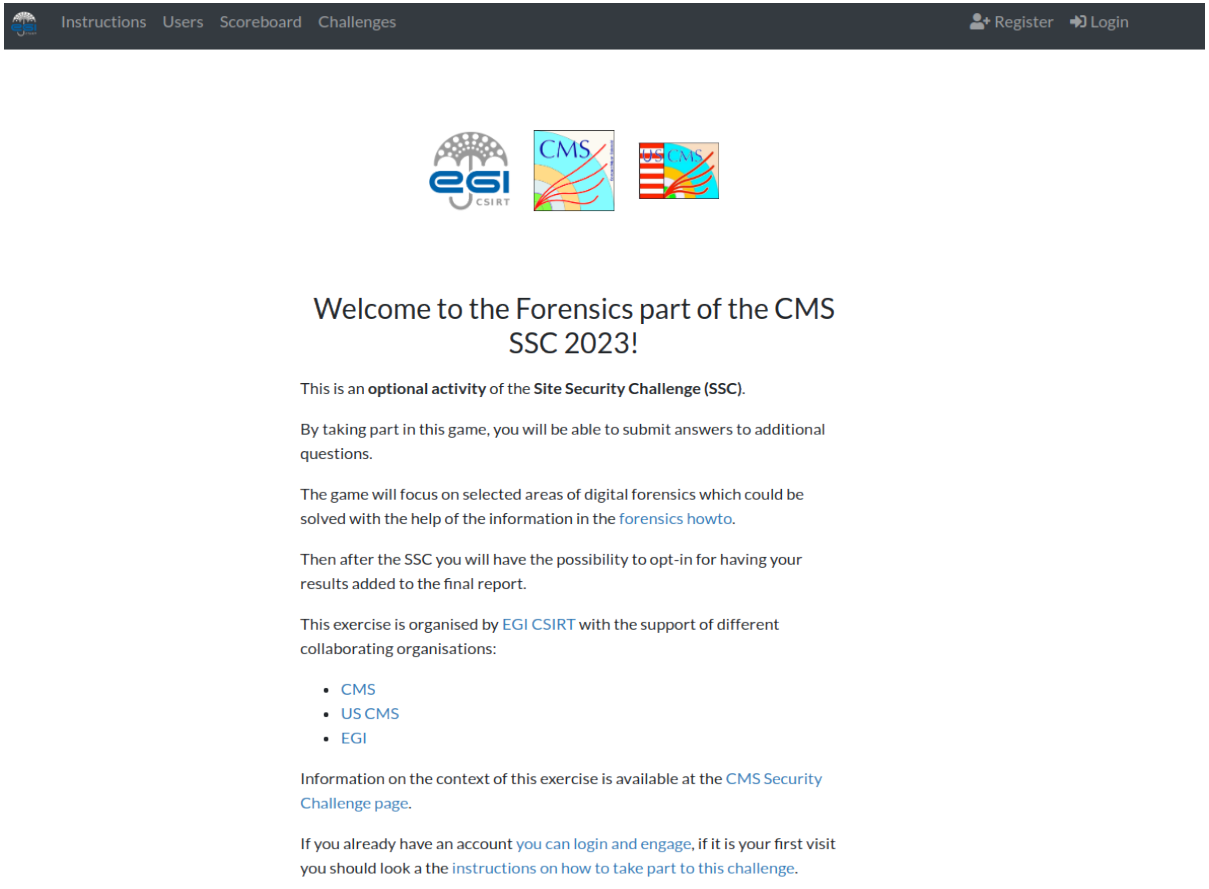
- Running VMs not affected, needed to be suspended by the local teams..
- Significant delay between invalidating IdP identity at Federated IdP and the lifetime of the token received from infrastructure proxy IdP(already addressed)
- Token Lifetime was an issue.
- (How can we mimick Certificate-Revocation-List functionality from the x509 world in the Federated Identity world?)

Subsection 8

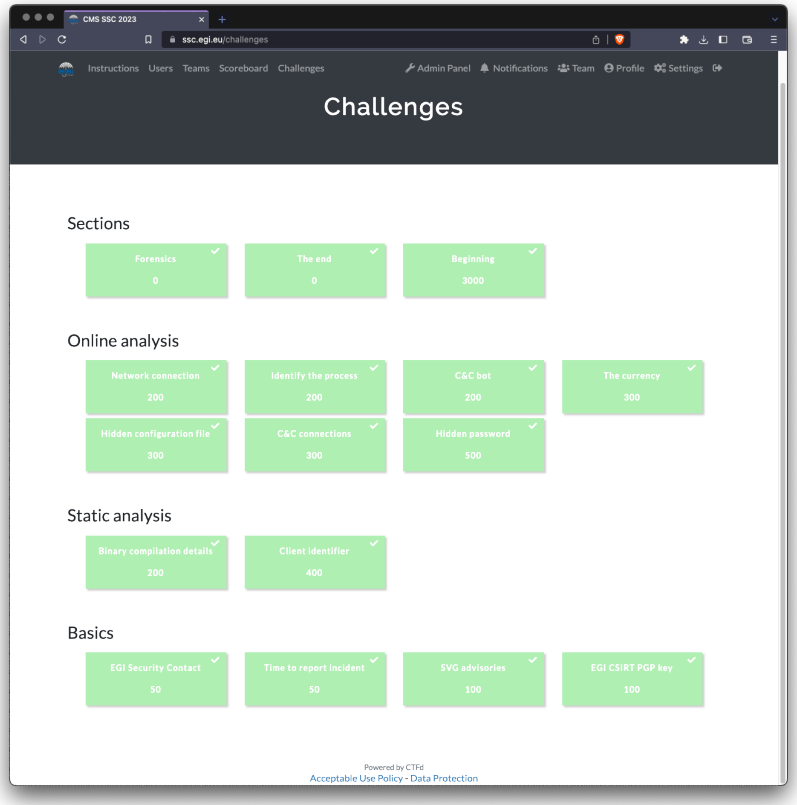
Resource Centers forensic capabilities

Capture The Flag, registration

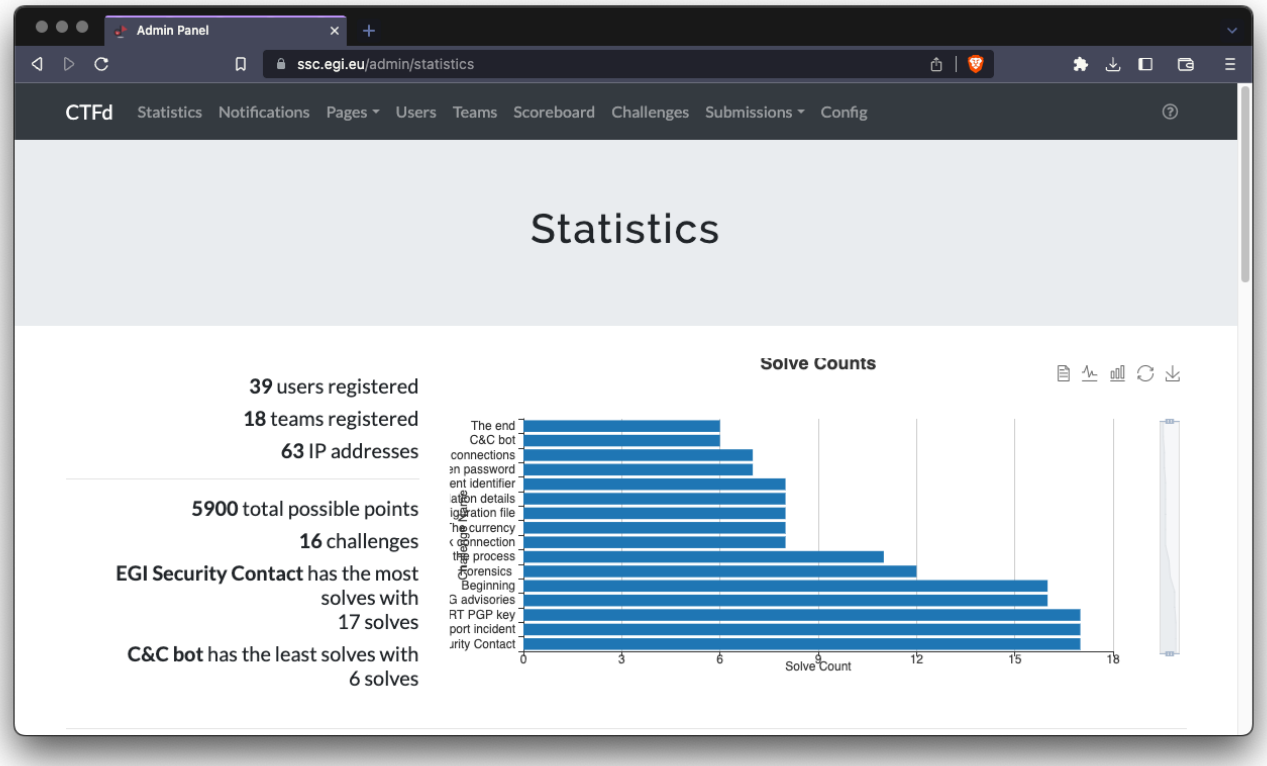
Registration to the CTF is optional, 18 Teams, 39 Users participated



Capture The Flag, example challenge



Capture The Flag, Result statistics



Capture The Flag, Result Scores

Place	Team	Score
1	[redacted]	5900
2		5900
3		5840
4		5700
5		5400
6		4900
7		4600
8		3500
9		3500
10		3300
11		3300
12		3300
13		3300
14		3300
15		3200
16		3100
17		200

Subsection 9

Inter organization coordination

Inter organization coordination

EGI/OSG

- Clear handover not implemented, daily meetings to synchronize the activities in the organisations needed.
- Collaboration with IdP worked flawless, very limited impact of the incident, therefore limited involvement of eduGAIN CSIRT. (OSG, eduGAIN)
- Very good collaboration with CMS Security.