Security operations

S. Gabriel[1,2]

[1]Nikhef [2]EGI CSIRT

Sept. 2026

Where we are now in the tCSC ...

- We learned about the first steps how to study the security situation of our infra, what do we really need to protect, and who is responsible for what (IT Security Risk Management)[1]
- We learned about the security architecture aspects of our infra.
- We learned about some aspects of how to do secure access management.
- We learned about to monitor the security perimeter of our infra
- We learned how attacks on our infra could look like
- Now lets look at how we can organize IT security, also in context of a wider picture, ... we are not on an isolated island.

[1] The remaining steps are more accessible to technical people, we only looked at the steps which are thematically distant from technical people's background/daily work

Using what we talked about this week ...

"IT-Security" is a decision of the organisations leadership.

- Scope of the Security Team needs to be aligned with the Organisation's Objectives.
- Management needs to agree with the suggested CSIRT scope, or define one themselves.
- From that follows whether you need to set up an IT Security team for an Organization or a Federation.

Input for Operation level

Organisational CSIRT vs. Federation(Coordinating) CSIRT

Aspect	**Organisational CSIRT**	**Federation CSIRT**
Primary purpose	Protect and respond to incidents within one organisation	Coordinate incident response and information sharing across multiple member organisations or CSIRTs
Constituency	A single organisation, such as a university, company, or government department	A federation, consortium, group of institutions, or interconnected organisations
Operational scope	Internal systems, networks, users, applications, and data	Cross-organisational incidents, user communities shared services, common risks, and incidents affecting several members
Authority	Direct authority over the organisation's systems and response teams	Coordination authority; member organisations retain operational and technical authority

Organisational CSIRT vs. Federation(Coordinating) CSIRT

Aspect	Organisational CSIRT	Federation CSIRT
Incident handling	Detects, analyses, contains, eradicates, and recovers from incidents affecting its organisation	Coordinates escalation, mutual assistance, joint analysis, communications, and collective response
Information sharing	Shares relevant information with management, IT, legal, law enforcement, and trusted external parties	Aggregates and distributes indicators, alerts, advisories, lessons learned, and threat intelligence among members
Resources and expertise	Dedicated or part-time internal staff and tools	Shared expertise, specialist teams, common services, and mutual-support arrangements
Typical outputs	Incident reports, forensic findings, remediation actions, lessons learned, and security improvements	Federation-wide alerts, coordinated response plans, joint exercises, and common playbooks

Main distinction in IR Organisational/Coordinating CSIRT

Organisational CSIRT: responds within one organisation

Federation CSIRT: coordinates response across organisations

CSIRT Tasks: Operational and Technical Response

Task area	Organisational CSIRT	Coordinating CSIRT
Incident intake and triage	Receive, validate, classify, prioritise, and assign incidents	Receive notifications from member CSIRTs; correlate incidents and identify events requiring joint action
Incident analysis and response	Investigate incidents; perform technical analysis and forensics; contain, eradicate, and recover	Coordinate specialist assistance, escalation, and cross-organisational response activities
Situational awareness	Monitor threats affecting the organisation and maintain an internal threat picture	Build a broader threat picture by aggregating and sharing information from member CSIRTs and trusted partners
Information sharing	Share indicators, findings, and recommendations with internal stakeholders and relevant external parties	Distribute alerts, indicators of compromise, advisories, and lessons learned across the constituency
Vulnerability management	Receive vulnerability reports; assess, remediate, and track vulnerabilities in organisational assets	Vulnerability Assessment, Security Monitoring, Federation wide alerting and follow up

Main distinction in Technical and Operational Response

Organisational CSIRT: performs the technical response;

Federation CSIRT: connects and supports multiple responders.

CSIRT Tasks: Coordination and Capability Building

Task area	Organisational CSIRT	Coordinating CSIRT
Communication and liaison	Coordinate with management[2], IT, service providers	Act as a trusted contact between member CSIRTs, external CSIRTs, federation partners
Policies and procedures	Maintain incident-response plans, playbooks, escalation paths, and contact lists	Develop common procedures, information-sharing rules, templates, and minimum response standards
Exercises and training	Conduct staff training, tabletop exercises, technical tests, and post-incident reviews	Organise federation-wide exercises, workshops, mutual assistance, and capacity-building programmes
Reporting and improvement	Document incidents, produce management reports, and track corrective actions and lessons learned	Publish aggregated reports, identify systemic risks, and recommend improvements for the constituency

[2] escalation to press, legal

CSIRT Tasks: Coordination and Capability Building

Task area	Organisational CSIRT	Coordinating CSIRT
Standards and guidance	Apply organisational security policies and response standards	Develop shared guidance, common terminology, maturity targets, and recommended practices
Resource coordination	Assign internal responders, tools, and specialist support	Match member needs with available expertise, tools, contacts, and assistance
Stakeholder support	Advise organisational leadership on risk, impact, and response priorities	Advise the federation on collective risk and coordinated response priorities

Main distinction Organisational/Coordinating CSIRT

Organisational CSIRT: owns internal accountability;

Federation CSIRT: enables cooperation and consistency.

Some aspects of Operational Security a federation CSIRT provides

Reliable Systems

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

Approach: security in EGI CSIRT

- Organization
  - What is the organizational structure (see previous talks), Governance, Responsibility Accountability.
  - What are the existing policies, agreements etc.
- Options
  - Set up trust network. Trust is in individuals.
  - Formally set up a security team (CRFC 2350 , TOR , mandate, services, ...etc.). Trust is in Organzations/Processes.

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.

Some Remarks on Communication

Talking to a CSIRT

Trust, Transparency, What to expect from a CSIRT →

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

How to Communicate Securely

- We don't mean encryption here!
- Rather, how to contain the *dissemination* of information by legitimate recipients.
- In other words: How to make sure that if you tell somebody a secret, that somebody does not blabber the secret to the rest of the world.
- Obviously an organizational measure, so all we can do is specify rules and then trust that everybody sticks to these rules.
- It should also be obvious that if somebody does not stick to these rules, they will not be trusted any longer.
- The set of generally-accepted rules is called the "Traffic Light Protocol" TLP.

TLP Principles

- Information is classified by the *sender* into one of these four categories: `TLP:CLEAR`, `TLP:GREEN`, `TLP:AMBER`, `TLP:RED`.
- The *recipient* is expected to treat the thusly-classified information in accordance with the TLP rules as laid out below.
- Information must be marked clearly with a TLP classification; it is generally a good idea to define a *default* classification in case there is no explicit marking. `TLP:AMBER` is usually a good starting point.
- The classification of a given bit of information may change over time (the classification is usually relaxed).

The TLP Classifications

- `TLP:CLEAR` (formerly `TLP:WHITE`): Information that can be shared freely with anybody—for instance, may be published on a public web page or released to the press.
- `TLP:GREEN`: Information that can be shared within the community—for instance, within the high-energy physics community—, but *not* released to the general public.
- `TLP:AMBER`: Information that may be shared *within the recipient's organisation and its clients*—for instance, within a university if the recipient is a member of a university, or a company *and its customers* if the recipient works for a company. If unsure, *ask the sender*. Additionally, `TLP:AMBER` may be restricted arbitrarily by the sender. For instance, `TLP:AMBER - FOR EDUGAIN ONLY` might be used so signal that information can only be shared with eduGAIN parties.

The TLP Classifications – cont'd

- `TLP:AMBER+STRICT`: This is a special, pre-defined restriction for `TLP:AMBER` that signals that information may be shared only within the recipient's organisation, but *not* with any customers.
- `TLP:RED`: This is the strictest classification and signals that information may *not be shared with anybody else whatsoever*. This means that whoever is told something under `TLP:RED` *cannot* tell *anybody* else this information.
  Note that this restriction in particular means that `TLP:RED` information cannot be shared through chat channels if a new member to the chat channel can read the channel history. If new members can read the history, then it is not clear who the ultimate recipients of a message will be because new members could be added at any time and thus gain access to earlier messages. Therefore, `TLP:RED` conditions cannot be guaranteed.

CSIRT Services revisited, EGI

- Incident Management (depends on 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[3])
- Compliance: Information Security regulations have to be met, for example in call for tenders [4]
- IT Security Risk Management (earlier talk)

[3] https://opencsirt.org/csirt-maturity/sim3-and-references/
[4] https://www.surf.nl/en/stitch-a-short-checklist-for-application-security

Tactical; 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 went silent
- Crypto Currency mining using grid technology ...and then an insider thought he could smart out the forensics team.

Attack on EGI Conflence

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.[5]
- Collaboration tools not available (Wiki)
- Here we could move to gitlab (hosted elsewhere)
- Don't have all eggs in one basket

[5] + a whole zoo of other apps (Rocketchat, slack, you-name-it), hard to be on everything

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

NSC

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

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

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).

Stakkato incident

- You may think: "*Come on Dude, this stuff is older then me*", but

Stakkato incident

- You may think: "*Come on Dude, this stuff is older then me*", but
- EGI-20230626-01 YYYYY Account Breach Leads to Widespread XXX Compromise
- EGI-20230502-01 Security incident suspected at ...
- " *...As far as we see, the hacker took over a personal system of one of our external users. He has stolen the user's privat ssh key on this system and used it to login into the system ...*"

Stakkato incident

- You may think: "*Come on Dude, this stuff is older then me*", but
- EGI-20230626-01 YYYYY Account Breach Leads to Widespread XXX Compromise
- EGI-20230502-01 Security incident suspected at ...
- " *...As far as we see, the hacker took over a personal system of one of our external users. He has stolen the user's privat ssh key on this system and used it to login into the system ...*"
- What would you want to have available when this happens at your infra?

Highly Sensitive Incidents

No slides here

Intentionally left blank

Incidents with media attention

Uni Maastricht, Ransom Attack

- 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? [6] [7]

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

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

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.

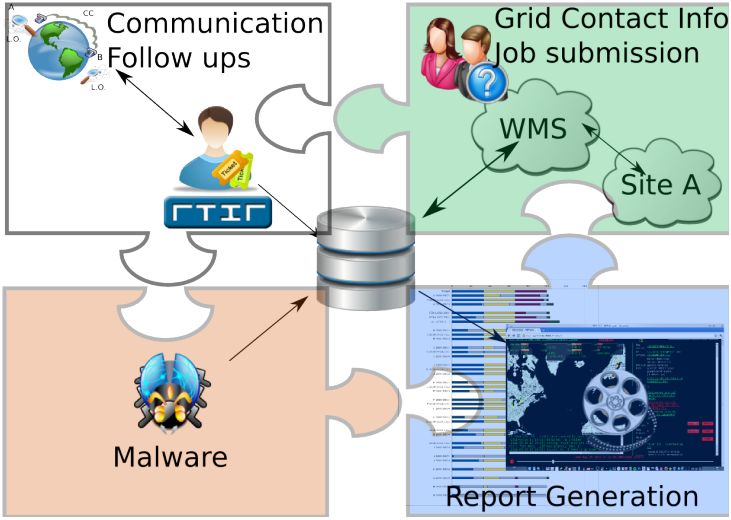
Assessment of Incident Response readiness

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



Results

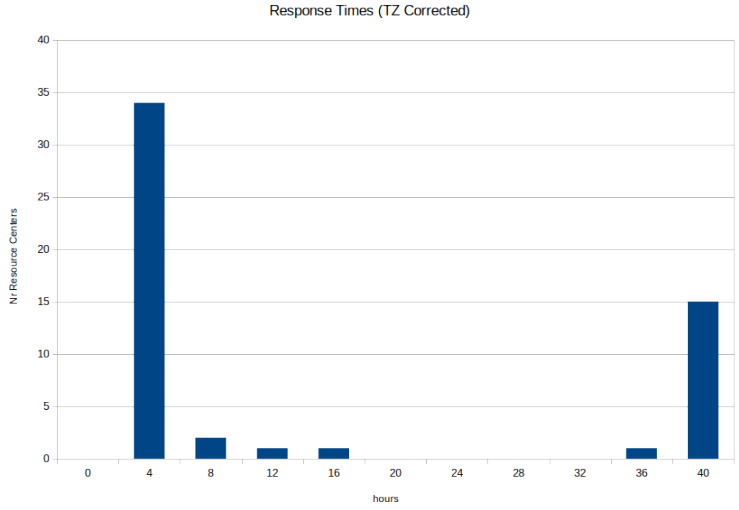
Results, what was evaluated

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.

Resource Centers Response Times

Communications, Response Times



Resource Centers Incident Response capabilities

Containment, Suspend malicious credentials

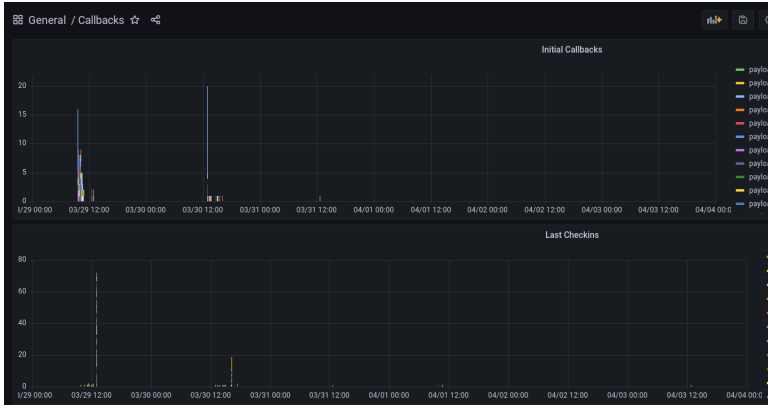
Gateway system 1, local resource security teams, certificate revoked: Wednesday, March 29, 2023 13:17

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

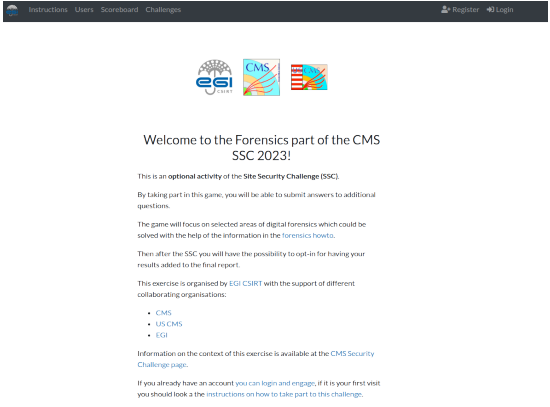
Stop malicious virtual machines. Kill the attack infrastructure, C2, Content delivery network, ...

- 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?)

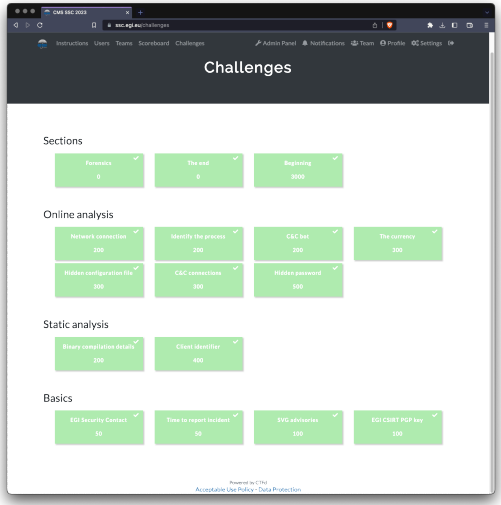
Resource Centers forensic capabilities

Capture The Flag, registration

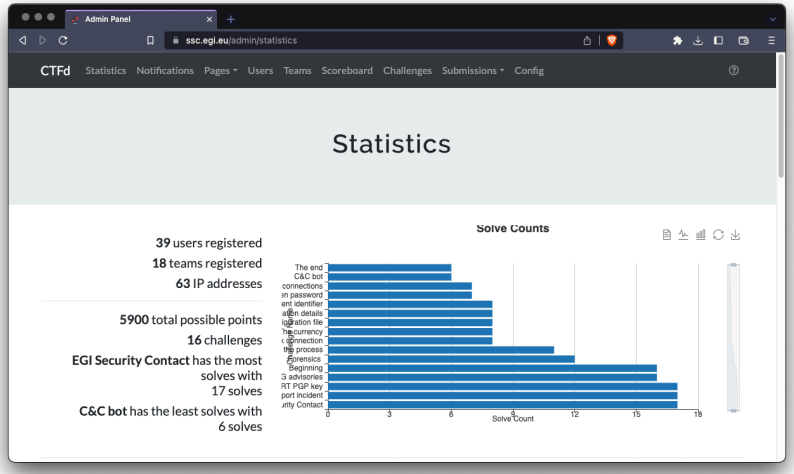
Registration to the CTF is optional, 18 Teams, 39 Users participated



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

Inter-Federation coordination

Inter-Federation 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.

Movie Time