

# Secuirty Service Challenge SSC-23.03,

challenging incident response of CMS resources.

D. Crooks <sup>1,3</sup>    S. Gabriel <sup>2,3</sup>    K.Ellis <sup>1</sup>    EGI CSIRTs IRTF

<sup>1</sup>UKRI STFC    <sup>2</sup>Nikhef    <sup>3</sup>EGI CSIRT

GDB 13.12.2023



# Introduction



# Overview

- ❖ Evolution of the Security Landscape
- ❖ Security Architecture
- ❖ Challenging the Security Architecture
- ❖ Blue Team/Red Team
- ❖ Results
- ❖ Q 'n A

# Evolution of the Security Landscape

- ❖ EGEE: Centrally coordinated infra, one set of policies, homogeneous grid middleware
- ❖ VO specific Workload management systems emerged late in EGEE
- ❖ EGEE  $\Rightarrow$  EGI, OSG, NDGF, who takes care of operational security?, and what does this imply?
- ❖ More grid middleware software flavours, VO WMS became standard.
- ❖ Virtualisation Technologies (Cloud, Container technology)
- ❖ New AuthN/Z technologies (Tokens), external Identity Providers (Social Media accounts, Identity Federations)
- ❖ Operational security in "*The Grid*" got more complex.
- ❖ (WLCG Security on purpose not mentioned here :- ) new WLCG Security Officer just started)

# Operational Security Architecture [1]

- ❖ What are the controls and processes we have in place to support our operational security
- ❖ Which of these do we want to test in this exercise?
- ❖ These are defined in the scope of EGI CSIRT; part of this exercise is also to explore how to most effectively collaborate across the full WLCG scope

# Operational Security Architecture [2]

Control/Process	Detail	Examined in this exercise?
Vulnerability Handling	Using pakiti to poll worker node patch status and correlate with critical vulnerabilities	No; part of daily operations for IRTF
Site communications	Handling communications with sites based on specified security/CSIRT contacts	Yes
Central suspension	Using ARGUS network to disseminate DNS to be suspended	Yes
Incident response procedures	Using SEC01 and otherwise to perform incident response across the infrastructure	Yes

# What, Why, How (EGI CSIRT perspective)

Goals of the Security Service Challenge (SSC) I, [Assessment Security Incident Management](#)

- ❖ EGI CSIRT: Test our incident response capabilities, are our procedures ready to deal with a multi Resource Center (RC) incident
- ❖ Assess the required collaboration with partner Security Teams (OSG, eduGAIN)
- ❖ How does it look at borders? Collaboration with Identity Providers Security teams

Goals of the Security Service Challenge (SSC) II, [Assessment of the Incident Response activities, Forensic skills.](#)

- ❖ Containment: act on a compromised account, suspend access to the infra
- ❖ Stop, and analyse malicious activities -
- ❖ → Capture the flag <https://ssc.egi.eu/>

# The Playground





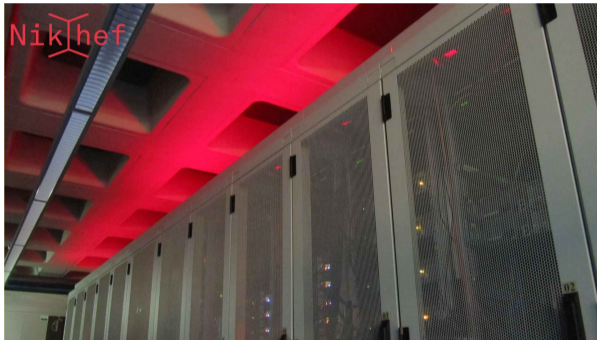
# The playground, Context, Resource Centers



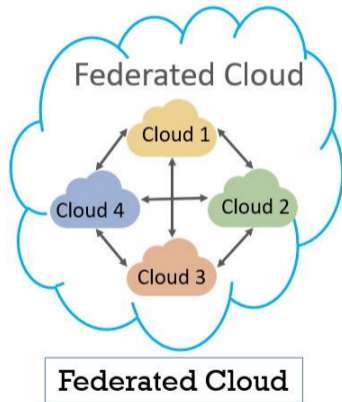
Old map, for illustration purposes only

# The playground, type of resources

## Compute Clusters



## Clouds



# The playground, Organisational Borders

170+ Resource Centers distributed over 40+ countries in WLCG are coordinated through the following organisations:

- ❖ OSG <https://osg-htc.org/networking/>, US based RCs
- ❖ The Nordic e-Infrastructure Collaboration , <https://neic.no/>, northern Europe.
- ❖ EGI <https://egi.eu>, ... the rest

A tempting target for crypto currency mining, d-dosing, ...

To get ready the Incident Response Procedures have to be harmonized across the organisations. .

# Access to the Playground, Identities

# Access, Identity Providers

- ❖ x509 certificates, CAs
  - ❖ meanwhile often coupled to institutes HR data
  - ❖ transition to tokens started.
- ❖ IdP proxy (egi-checkin)
  - ❖ Federated Identity Providers (eduGAIN)
  - ❖ Social Media accounts
  - ❖ EGI Check-in serves as a seamless bridge, enabling more than 17,500 registered users to access 150+ services effortlessly, using their own institutional identity providers and community AAI services.

# Access, compromised Identities

- ❖ x509 certificates, CAs
  - ❖ Certification revocation, strict rules on revocation, but possible
- ❖ IdP proxy (egi-checkin)
  - ❖ eduGAIN provides through SIRTfI a handle for Incident Response
  - ❖ good luck with social media accounts

# Access through Virtual Organisations

# Access, Virtual Organisation

- ❖ Users are not granted access to the resources directly, rather they have to join a Virtual Organisation (VO)
- ❖ A VO is a group of people (e.g. scientists, researchers) with common interests and requirements, who need to work collaboratively and/or share resources (e.g. data, software, expertise, CPU, storage space) regardless of geographical location.
- ❖ VOs can suspend their users based on token, certificate DN.
- ❖ RCs decide which VO they support, grant access to (a fraction) of their local resources, RC can block access for individuals, based on their certificate DN.



# The Red Team

# Red Team, the attack plan

Goals: Use the nice Playground for own purposes

- ❖ Crypto Currency Mining (we must not make money from the resources, start own currency (egoin))
- ❖ Rent out the resources under our control for DDoS campaigns, ...

# Scenario

- ❖ Get credentials, and use them for ...
- ❖ Deploy an attack infra (command and control system, ...)
- ❖ Create a Botnet on the infrastructures
- ❖ Does this seem unrealistic? Well, no.

# Red Team, the attack plan, needed ingredients

## 3 Major ingredients

- ❖ Credentials that give access to High Throughput computing
- ❖ Credentials that gives access to Cloud Resources to host the attack infra
- ❖ Attack infra

Get Identities, access to the infrastructure

# Access to Compute clusters

x509 credentials registered at CMS VO

- ❖ Coordinate with CMS VO to provide credentials used for the SSC

# Access to Cloud Infras

Identities from Social Media and Federated Identity Providers (ex. eduGAIN) can be used in egi-checkin (IdP proxy)

Motivation: several incidents with crypto currency mining, hosting of problematic material, lets make this part of the exercise.

- ❖ Social media account, well that's easy ...
- ❖ Identity from Federated IdP.
  - ❖ Find IdP that wants to collaborate on this security research project, *thanks DFN-AAI*
  - ❖ Invent a person, and provide it with some identity.
  - ❖ **Enrol this identity in a VO that has access to cloud resources.**
  - ❖ ...see next slides *Resilience of the VO membership vetting process*

# What people get to in after work sessions

Every Identity needs some background to stay consistent, lets try this:



The Red Team Next slides by Baptiste Grenier, Senior Service Delivery and Information Security Officer, EGI.





# What people get to in after work sessions



## #0: pretext impersonating a researcher in need of cloud resources

Welcome Dr Sobchack

- Dr Walter Sobchack is a researcher, looking for cloud resources to do some analysis in the context of their research

- **Identity card**

- Name: Walter Sobchack
- Title: Dr
- Institute: Nizhny Novgorod State Academy of Medicine (Russia)
- Email: [dr.walter.sobchack@gmail.com](mailto:dr.walter.sobchack@gmail.com)

- **Research papers - online proofs**

- <https://www.researchgate.net/scientific-contributions/DM-Sobchak-33763131>
  - Content already available online, from a real researcher with a similar name

- **Inspiration: Walter Sobchak character from "The Big Lebowski" movie**

- [https://coenbrothers.fandom.com/wiki/Walter\\_Sobchak](https://coenbrothers.fandom.com/wiki/Walter_Sobchak)



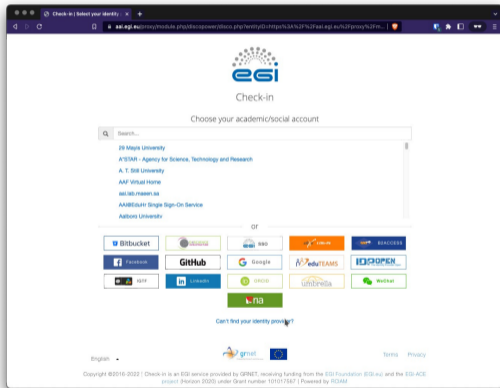
# What people get to in after work sessions



## # 1: Getting a social media account integrated with Check-in

May options to choose from

- Google, GitHub, ORCID, LinkedIn...
- Decided to go with a **Google account** as it also provides a convenient way to have a **working email address**
  - Easy to create and manage
  - **One requirement:** having a phone number used at account creation



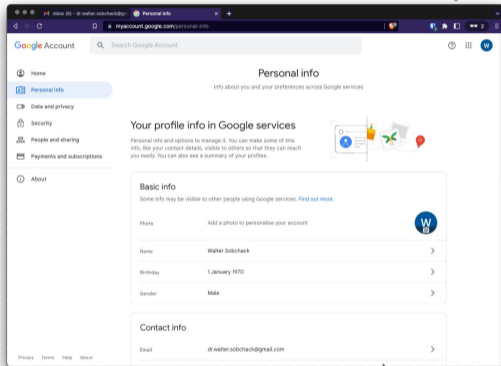
# What people get to in after work sessions



## # 1: Dr Walter Sobchack's Google account

An easy first step

- Welcome Dr Sobchack!
- Email: [dr.walter.sobchack@gmail.com](mailto:dr.walter.sobchack@gmail.com)



# What people get to in after work sessions



## EGI Security Service Challenge

- Overall goal: **deploying VMs for an attack** spreading across the EGI infrastructure and services
- Some mapping with [MITRE ATT&CK](#) knowledge base:
  - [Establish Accounts](#) via a [Trusted Relationship](#), interacting with a [Command and Control](#) aiming at doing [Resource Hijacking](#)
- Persona:
  - Uli Kunkel, a **German staff researcher**
  - Account from an **eduGAIN-federated trusted IdP**
  - **Online presence** to appear more legitimate
    - A **personal page** created
    - Real researchers having similar names and public information, including publications
- **Caught during the initial vetting process**
  - **Kudos to the VO managers!**
  - Eventually joined a VO allowing to deploy VMs...

Uli Kunkel - Staff Researcher

### My background

I am currently a staff researcher at the Federal Laboratory of Sciences, where my focus lies on static analysis of legacy software systems, such as early financial systems. These systems make up a significant part of our hidden daily life and are, more often than not, aging. My goal is to identify strongly coherent 'islands' of software that can be replaced with smaller, easier to maintain, modern equivalents. To that extent, the well-known concept of micro services plays an important role, together with parsing and correlation engines.

### Experiments

Much of this work revolves around parsing of large, real systems. This requires a lot of processing power. To counter unnecessary use of this compute power, we developed a framework based on the language Haskell. This framework specializes in generating and analysing ASTs, and is easily runnable to various environments that support the underlying language. Another upside of this approach is that it easily portable between common architectures, as long as a C compiler exists.

### Personal

Whenever I have the time, I like to play music - in the past also as part of the band 'Autobahn'.

[imprint](#) | [privacy notice](#)



# The Attack Infrastructure

# Red Team, Find the right people

- ❖ Middleware Expertise
- ❖ Incident Detection Expertise
- ❖ Malware/Forensics Expertise
- ❖ Job Submission Expertise
- ❖ CMS specific Expertise
- ❖ Identity Federation Expertise
- ❖ Incident Response Expertise
- ❖ Federated Services Expertise
- ❖ International Liaisons
- ❖ CMS Liaisons

# Find space in everyone's agenda

Major coordination task, at the end a multiple days hackaton at CERN resulted in the needed progress. Expert knowledge in a wide area needed.

# RedTeam, explore target's technology & infra

- ❖ RCs running HTCondor
- ❖ RCs running ARC-CE
- ❖ CRAB pilots
- ❖ CMS Connect pilots
- ❖ Storage (out of scope)

## World wide env'ment

- ❖ Heterogenous setups
- ❖ Local solutions
- ❖ Different deployment models
- ❖ Range: shoebox  $\longleftrightarrow$  HPC
- ❖ Many kernel versions
- ❖ Blue team tools can turn red



# Red Team Engineering

Build a framework to talk to frameworks that talk to frameworks that talk to compute elements that run our malware that returns commands that runs some other file that talks to another framework that looks like actual malware.

# RedTeam, Select a malware framework

## Write it yourself?

- ❖ Not enough time
- ❖ Why reinvent the wheel
- ❖ Full control over functionality

## Vet an existing framework

- ❖ Open Source
- ❖ Open Source
- ❖ Limited investments
- ❖ No built in grid support

# Red Team, Submit some jobs, look around

Initial tests of the malware

- ❖ Submit to friendly sites (Red team developers' home institutes)
  - ❖ Prevent actual response from local admins

# Red Team, Blue team tools can turn red

Pakiti (<https://github.com/CESNET/pakiti-server>) is a useful tool.

The screenshot shows the Pakiti web interface. At the top, there is a navigation bar with links for Hosts, Vulnerabilities, Host groups, Packages, Oses, VDS, CVE Tags, Exceptions, Users, and Statistics. Below the navigation bar, there are three shortcut buttons: "With tagged CVEs in the last 24 hours", "Inactive longer than 7 days", and "Report in the last 48 hours sorted by hostname". A search section includes a "Search Term:" input field, a "Search" button, and four dropdown menus for "CVE", "CVE Tag", "Activity", and "Host group". Below the search section, it says "39 hosts found". A table displays the results with columns for Hostname, HostGroups, Os, Kernel, Architecture, #InstalledPkgs, #CVEs, Tagged CVEs (only EGI-Critical), #Reports, and LastReport. The first two columns are redacted. The table shows three entries for CentOS Linux release 7.9.2009 (Core) with CVE-2022-2588. A red arrow points to the CVE-2022-2588 entries with the text "Also ancient CVEs".

Hostname	HostGroups	Os	Kernel	Architecture	#InstalledPkgs	#CVEs	Tagged CVEs (only EGI-Critical)	#Reports	LastReport	
Redacted	Redacted	CentOS Linux release 7.9.2009 (Core)	3.10.0-1160.76.1.el7.x86_64	x86_64	1886	22	CVE-2022-2588	1	2023-03-27 02:29:56	Delete
Redacted	Redacted	CentOS Linux release 7.9.2009 (Core)	3.10.0-1160.76.1.el7.x86_64	x86_64	2059	51	CVE-2022-2588	2	2023-03-22 03:18:08	Delete
Redacted	Redacted	CentOS Linux release 7.9.2009 (Core)	3.10.0-1160.76.1.el7.x86_64	x86_64	1	10	CVE-2022-2588	1	2023-03-22 03:04:10	Delete

Also ancient CVEs



# Red Team, Start the SSC

Murphy's Law, obviously

- ❖ C2 Software breaks spectacularly
  - ❖ Reset your database (bad, bad choice)
- ❖ Get caught scouting environments
- ❖ Miner traceability is sub-optimal

Find the right balance between red & blue

Hide behind `cms.nikhef.de` (as opposed to `nikhef.nl`)

- ❖ Let's see how well known Nikhef is as an institute :-)

# Red Team, Check your own responsibilities

SSC23: Incorporate MISP into the collaborative CSIRT response

- ❖ EGI CSIRT internal task, even we gain something from this SSC :-)
- ❖ Listen to David Crook's talks on MISP/collaborative SOCs

# The Blue-Teams

# Goal of the blue team activities

Coordinate security response activities over:

- ❖ 4 Organisations (EGI, OSG, eduGAIN, CMS VO).
- ❖ 58 Resource Centers (with local security teams).
- ❖ 141 gateways to the infra (controlled by the local security teams, proxy gateways controlled by VO).
- ❖ 2 proxy gateways that potentially circumvent local access control mechanism.
- ❖ Stop 2 Credentials from accessing the infras.



# The task

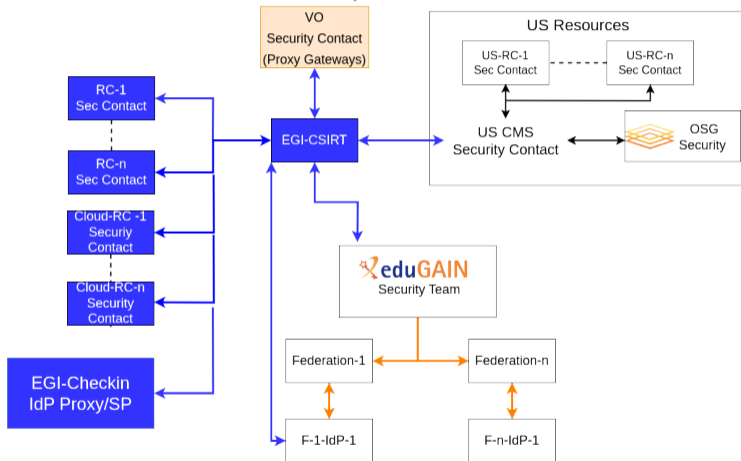
# The Task

- ❖ Identify affected Resource Centers, Organisations.
- ❖ Stop malicious processes on the affected Infra.
- ❖ Stop/Suspend accounts used to initiate the malicious processes.
- ❖ Collect sufficient forensics information to resolve the incident.

# The Communication Endpoints

# Communication Network

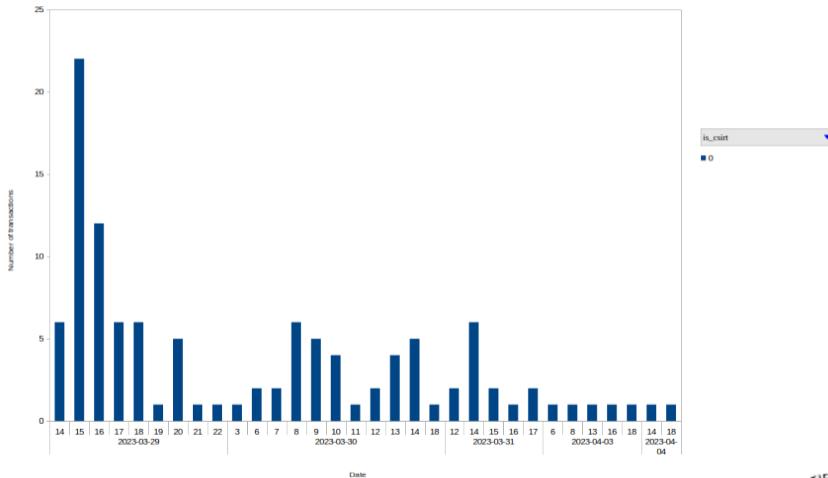
## Connected Communication Endpoints and Gateways



# Communication Volume

creator | - multiple -

Transactions



created\_date | created\_hour

# Blue Team Resources

The coordination, inclusive the assessment of feedback for further intel sharing was done by 2 Persons. **Heavily Understaffed**

# The Results



# Results, what was evaluated

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

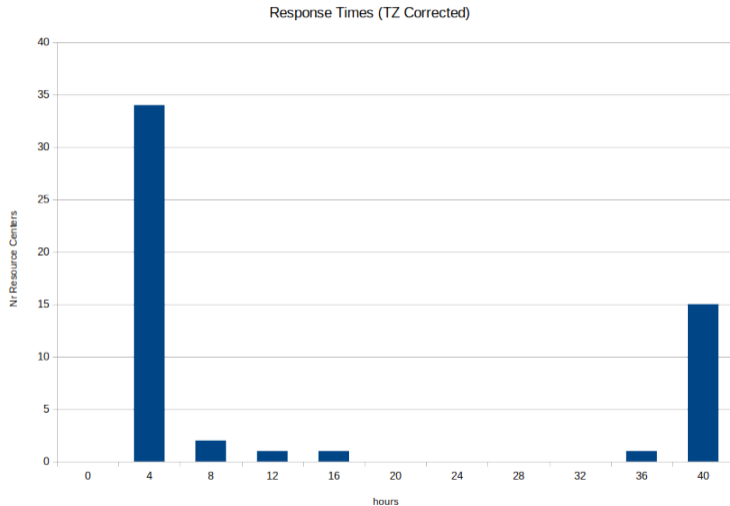
- ❖ Communications: Response times
- ❖ Containment: Stop malicious processes, suspend reported credentials
- ❖ Forensics: On/Offline forensics of the malicious processes running at the resource center. Capture The Flag, participation optional.



# Resource Centers Response Times



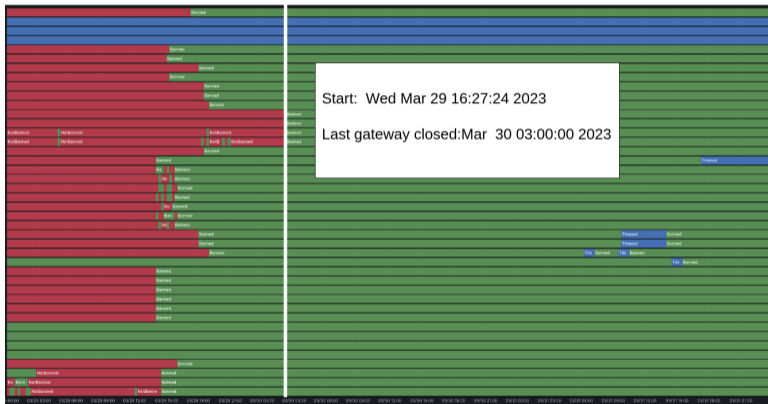
# Communications, Response Times



## Resource Centers Incident Response capabilities

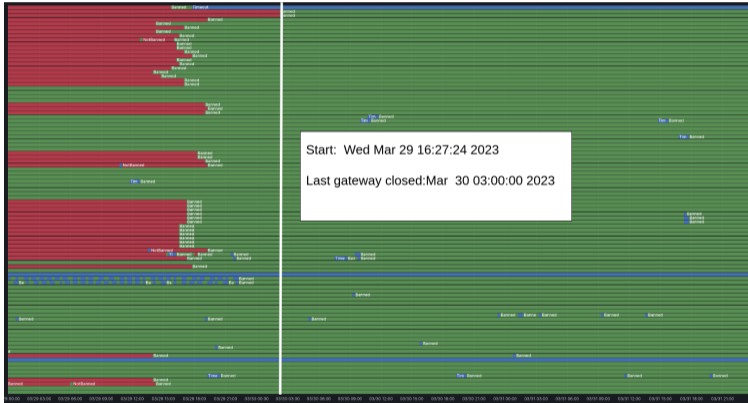
# Containment, Suspend malicious credentials

## Gateway system 1, local resource security teams



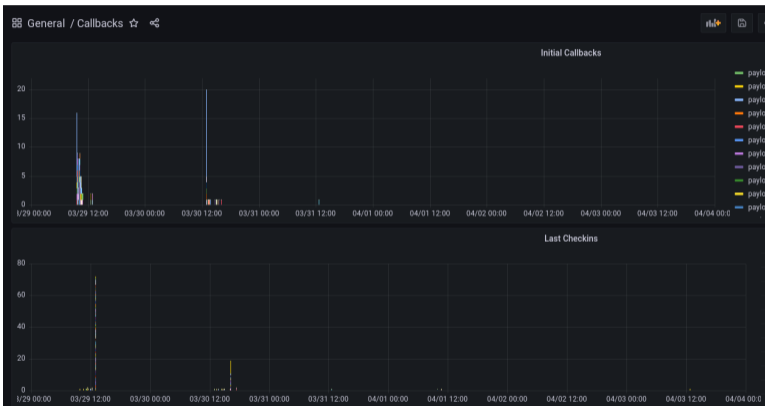
# Containment, Suspend malicious credentials

Gateway system 2, local resource security teams.



# 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, ...

- ❖ Significant delay between invalidating IdP identity at Federated IdP and the lifetime of VMs (or processes) started by that identity is an issue.
- ❖ on infrastructure IdP Proxy and the started VMs related to this identity (addressed EGI internally).
- ❖ Token Lifetime (is) was an issue.
- ❖ How can we mimic 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



## Welcome to the Forensics part of the CMS SSC 2023!

This is an **optional activity** of the Site Security Challenge (SSC).

By taking part in this game, you will be able to submit answers to additional questions.

The game will focus on selected areas of digital forensics which could be solved with the help of the information in the [forensics howto](#).

Then after the SSC you will have the possibility to opt-in for having your results added to the final report.

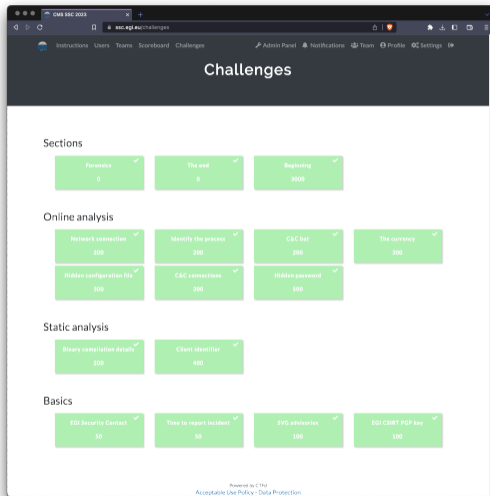
This exercise is organised by EGI CSIRT with the support of different collaborating organisations:

- CMS
- US CMS
- EGI

Information on the context of this exercise is available at the [CMS Security Challenge page](#).

If you already have an account you can [login and engage](#), if it is your first visit you should look at the [instructions](#) on how to take part to this challenge.

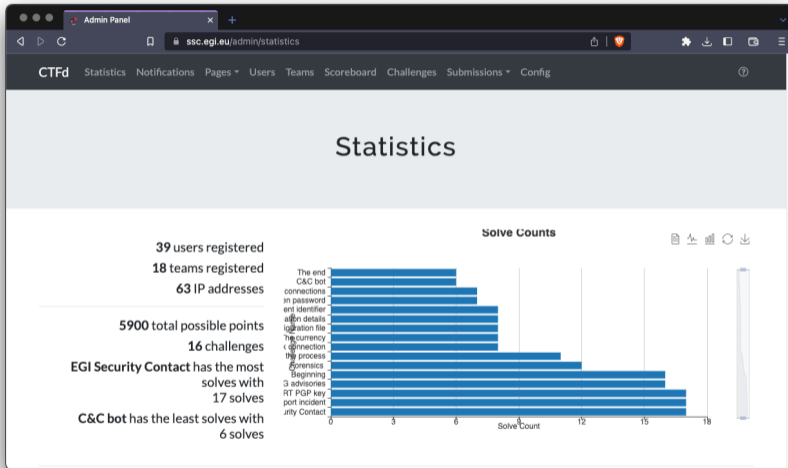
# Capture The Flag, example challenge



The screenshot shows a web browser window displaying a CTF challenge dashboard. The browser's address bar shows the URL `ssc-egi.challenges`. The dashboard has a dark header with the title "Challenges" and a navigation menu with items: Instructions, Users, Teams, Scoreboard, Challenges, Admin Panel, Notifications, Team, Profile, and Settings. The main content area is divided into several sections, each containing challenge cards with their names and scores. At the bottom, there is a small footer: "Powered by CTM | Acceptable Use Policy - Data Protection".

Section	Challenge Name	Score
Sections	Forensics	0
	The end	0
	Beginning	3000
Online analysis	Network connection	200
	Identify the process	200
	CAC bot	200
	The currency	300
	Hidden configuration file	300
	CAC connections	300
Static analysis	Binary compilation details	200
	Client Identifier	400
Basics	EGI Security Contact	50
	Time to report incident	50
	SVG advisories	100
	EGI CSIRT PGP key	100

# Capture The Flag, Result statistics



# Capture The Flag, Result Scores

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

Powered by CTFd  
Acceptable Use Policy - Data Protection

The Results



## 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.

What comes next

# New processes: Threat Intelligence

- ❖ Historically, indicators of compromise (IOCs) such as IP addresses and file checksums have been communicated by the EGI CSIRT IRTF by broadcast emails to security contacts
- ❖ This leads to delays before new information can be shared, as repeated emails would lead to overload
- ❖ In the modern research and education landscape, where the risk from cybersecurity attack is acute, we must work collaboratively to share accurate and timely threat intelligence - IOCs - in close to real time



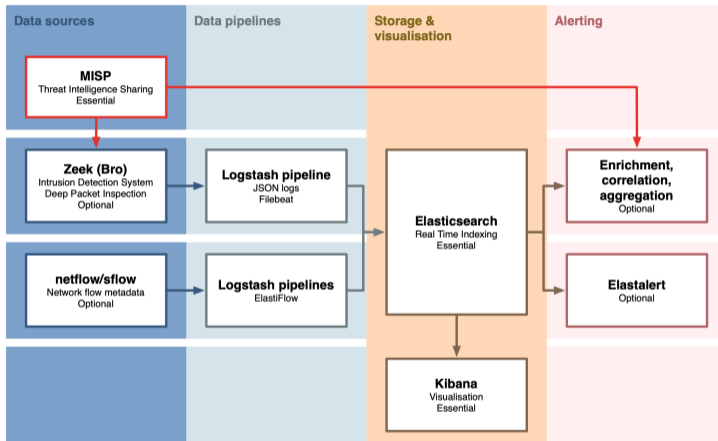
# Automated Threat Intelligence in this SSC

- ❖ This challenge included a side component using the MISP threat intelligence sharing platform to create a shareable event encapsulating all the intelligence related to the exercise gained through the investigation
  - ❖ <https://misp-project.org>
- ❖ MISP event built by team at STFC during challenge
- ❖ Next step is to test this against Security Operations Centres being deployed

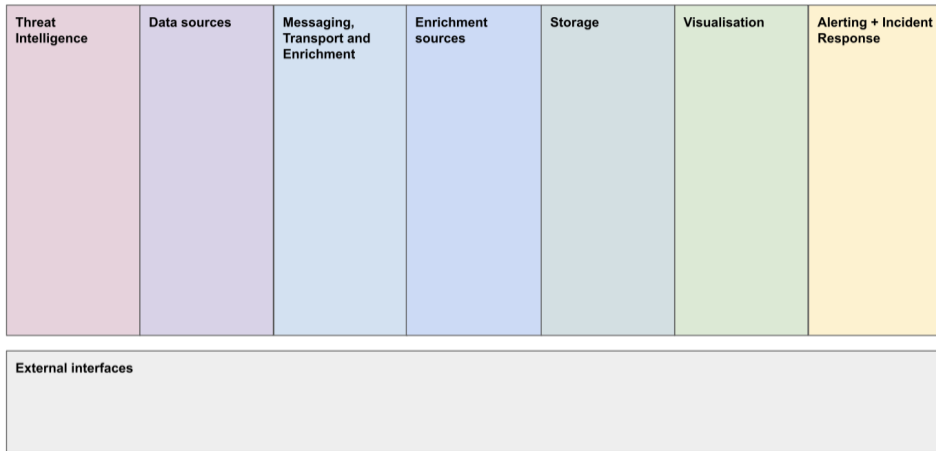
# Security Operations Centres capabilities

- ❖ A Security Operations Centre (SOC) is a collection of people, processes and technology that augments the capabilities of a security team by aggregating and enriching security monitoring data, correlated with sources of threat intelligence, to improve overall incident response and investigation capabilities
- ❖ The SOC Working Group was established to create reference designs for the deployment of such a Security Operations Centre in a R&E environment
  - ❖ <https://wlcg-soc-wg-docs.web.cern.ch>
- ❖ In particular, the goal of this group is to allow sites to actively use threat intelligence by integrating it systemically into their security monitoring systems

# SOC WG Reference Design v1



# SOC WG Reference Design v2 DRAFT



# Combining the SSC and SOC's

- ❖ An important followup to this challenge is to work with sites that have deployed SOC capabilities to understand how these would have observed the ongoing events of the challenge
  - ❖ Such as STFC, Nikhef and CERN
  - ❖ Using the MISP event developed during the challenge
- ❖ The ultimate goal is to use the MISP threat intelligence sharing platform to make these threat feeds available
- ❖ EGI CSIRT now has the tooling to share MISP events using a R&E instance hosted at CERN, available to the community
  - ❖ Need to build this robustly into our procedures

# Active collaboration

- ❖ Ultimately a key goal of these challenges is to improve the collaboration between
  - ❖ Sites and security teams
  - ❖ Security teams and VOs
  - ❖ Security teams
- ❖ Between challenges, it is essential to maintain these links - through dedicated meetings, workshops and conferences such as this
- ❖ As with all collaboration, this is a continuously evolving area as people leave and join teams, and as infrastructure topologies change over time
  - ❖ Building and maintaining trust is particularly important in this domain

# The next challenge

- ❖ As we look to the next challenge, what aspects could we consider?
- ❖ One option: limit the scope to test particular areas
  - ❖ This would allow key processes to be tested independent of the whole infrastructure
  - ❖ Potential for higher challenge cadence where appropriate
  - ❖ Interspersed with full challenges
- ❖ This challenge had a far larger scope than previously; by design
  - ❖ It is essential for us to test our response to our current complex landscape
- ❖ How do we balance this increasing challenge complexity with security team resourcing?
  - ❖ Maintaining sufficient blue team capability

# Operational Security Architecture: outcomes

- ❖ What are the lessons we can take from this exercise
  - ❖ where are the opportunities to build in the future?
- ❖ Focus on EGI and OSG as NDGF doesn't have CMS sites (we believe)



# Site communications

EGI

Issues came from the initial comms check which impacted effective identification of participating sites

OSG

Comms handled by USCMS

- ❖ **To take forward**
- ❖ Refining comms check apparatus and continue collaboration with US Experiment infrastructures in combination with OSG security team

# Central Suspension

EGI  
OSG

Central process worked where in place  
Not currently part of central suspension  
process

- ❖ **To take forward**
- ❖ In concert with Authz and Token Trust & Traceability working groups, develop new model for central suspension in the context of the token translation

# Incident Response Procedures

EGI

Broadly effective with clear need for more resources for blue team

OSG

Emphasised importance of working closely with experiment teams

## ❖ To take forward

- ❖ The process of developing this exercise was critical in understanding the contact points particularly between EGI CSIRT and experiment security teams; opportunity to build on this

# Key outcome

- ❖ From EGI CSIRT perspective, this exercised emphasised again the importance of working closely with experiment security teams and staff
- ❖ Experiments of course provide continuity in their scopes across international boundaries; opportunity to work closely on effective security operations across the board

# Conclusions



# Conclusion, Discussion

- ❖ The complexity of the coordination of incident response activities is huge.
- ❖ Sufficient manpower needed for the coordination task.
- ❖ Plan for inter-organisational meetings at least once a day.
- ❖ Work towards automation, monitor the activities as far as possible.
- ❖ Various flaws in the response procedures detected and addressed (check efficiency of the current workflow, implement control loops)

# Conclusion, Federated Identities

- ❖ Review SIRTFI, how do we support automation of threat intel sharing?
- ❖ How can we address chained identities (chained proxies).
- ❖ What would be realistic scenarios for future exercises.
- ❖ What format should these exercises have (table top, "cheap"; hands-on exercises, "more expensive"?)
- ❖ Work towards automation, monitor the activities as far as possible.
- ❖ Various flaws in the response procedures detected and addressed (check efficiency of the current workflow, implement control loops)