Results of a Global Security Exercise
or how AAI facilitates new friendships between Security Teams

David Crooks $^{1,3}$  
Sven Gabriel $^{2,3}$  
Jouke Roorda$^2$

$^1$UKRI STFC  $^2$Nikhef  $^3$EGI CSIRT

Internet2 Technology Exchange Sept. 18-22 2023 Minneapolis, Minn.
Introduction
Overview

- Introduction [David]
- Identities, Access and Red Team introduction [Sven]
- Attack Infrastructure [Jouke]
- Blue Team [Sven]
- What comes next [David]
- Conclusions [Sven]
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 which a multi Resource Center (RC) incident
- Assess the required collaboration with partner Security Teams (OSG, eduGAIN)
- How does it look at boarders? 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, LHC
The playground, Context, Resource Centers

Old map, for illustration purposes only
The playground, type of resources

Compute Clusters

Clouds

Federated Cloud

Cloud 1

Cloud 2

Cloud 3

Cloud 4
170+ Resource Centers distributed over 40+ countries in WLCG are coordinated through the following organisations:

- **OSG** [https://osg-htc.org/networking/](https://osg-htc.org/networking/), US based RCs
- The Nordic e-Infrastructure Collaboration, [https://neic.no/](https://neic.no/), northern Europe.
- **EGI** [https://egi.eu](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
  - migration 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
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, ...
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 give access to Cloud Resources to host the attack infra
- Attack infra
Get Identities, access to the infrastructure
Access to Compute clusters

\*509 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, let's try this:

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
  - 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
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
What people get to in after work sessions

#2 getting a Check-in account associated with the GMail account
Check-in account is one email verification away

- Registering and managing EGI Check-in account at https://aai.egi.eu/registry
What people get to in after work sessions

#3: enrolling to a VO for piloting activities
Using Check-in to enroll to the VO

- **Enrolling:** [https://aai.egi.eu/registry/co_petitions/start/coef:240](https://aai.egi.eu/registry/co_petitions/start/coef:240)
#4: Going through the vetting process

Checking the Affiliation. Pointing to Dr Sobchak's research on ResearchGate...
What people get to in after work sessions

#7: A VO manager reporting to EGI CSIRT

EGI Foundation Central VO management team getting suspicious

- First report about suspicious activity sent to it-support@egi.eu
- Identifying the pretext's context
- Then forwarding to abuse@egi.eu
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...
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

Heh
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 ↔ HPC
- Many kernel versions
- Blue team tools can turn red
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](https://github.com/CESNET/pakiti-server)) is a useful tool.

<table>
<thead>
<tr>
<th>Hostname</th>
<th>HostGroups</th>
<th>Os</th>
<th>Kernel</th>
<th>Architecture</th>
<th>#installedPlugins</th>
<th>#CVEs</th>
<th>#Reports</th>
<th>LastReport</th>
</tr>
</thead>
<tbody>
<tr>
<td>Redacted</td>
<td>Redacted</td>
<td>CentOS Linux release 7.9.2009 (Core)</td>
<td>x86_64</td>
<td>1886</td>
<td>22</td>
<td>CVE-2022-2584</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>CentOS Linux release 7.9.2009 (Core)</td>
<td>x86_64</td>
<td>2056</td>
<td>51</td>
<td>CVE-2022-2584</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>CentOS Linux release 7.9.2009 (Core)</td>
<td>x86_64</td>
<td>1</td>
<td>10</td>
<td>CVE-2022-2584</td>
<td>1</td>
<td></td>
</tr>
</tbody>
</table>

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 :-)

The Red Team
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
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

Response Times (TZ Corrected)

The Results
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.
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 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
Capture The Flag, example challenge
Capture The Flag, Result statistics
### The Results

<table>
<thead>
<tr>
<th>Place</th>
<th>Team</th>
<th>Score</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td></td>
<td>5900</td>
</tr>
<tr>
<td>2</td>
<td></td>
<td>5900</td>
</tr>
<tr>
<td>3</td>
<td></td>
<td>5840</td>
</tr>
<tr>
<td>4</td>
<td></td>
<td>5700</td>
</tr>
<tr>
<td>5</td>
<td></td>
<td>5400</td>
</tr>
<tr>
<td>6</td>
<td></td>
<td>4950</td>
</tr>
<tr>
<td>7</td>
<td></td>
<td>4650</td>
</tr>
<tr>
<td>8</td>
<td></td>
<td>4400</td>
</tr>
<tr>
<td>9</td>
<td></td>
<td>4100</td>
</tr>
<tr>
<td>10</td>
<td></td>
<td>3900</td>
</tr>
<tr>
<td>11</td>
<td></td>
<td>3200</td>
</tr>
<tr>
<td>12</td>
<td></td>
<td>3120</td>
</tr>
<tr>
<td>13</td>
<td></td>
<td>3030</td>
</tr>
<tr>
<td>14</td>
<td></td>
<td>2940</td>
</tr>
<tr>
<td>15</td>
<td></td>
<td>2850</td>
</tr>
<tr>
<td>16</td>
<td></td>
<td>2730</td>
</tr>
<tr>
<td>17</td>
<td></td>
<td>2600</td>
</tr>
</tbody>
</table>
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.
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
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.
What comes next
Combining the SSC and SOCs

- 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
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 that 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
Conclusions
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)
Federated Identities, Input to ACAMP I

- How to spread information about compromised credentials, identities that aren’t eligible anymore, misbehaving user.
- Information should reach relevant SPs in a timely manner.
- Services may be provided for long time ("detached" from the initial authentication), like spinning up a VM.
- Information about which services were accessed by the user might not be available (chained proxies). Logs may be missing.
- Linked identities, people using social identity (previously linked to an institutional identity) can continue to use the services even after they leave their institution.
- How can we address chained identities (chained proxies).
- Differences in technologies (on services): SAML only accepts initial assertion, OIDC (may) maintain access token (?)
Efficient Threat Intel Sharing is a problem.
On short-term we can live with mails (in eduGAIN CSIRT). Broadcasts go to 1000ds.
How could a info sharing platform look like? (GDPR conform, automated).
Review SIRTFI, how do we support automation of threat intel sharing?
What would be realistic scenarios for future exercises.
What format should these exercises have (table top, ”cheap”; hands-on exercises, ”more expensive”?)