

16-11-2018

# Incident Response Test Model for Organisations - Simulation #2

Deliverable MNA3.3.3

Contractual Date:	N/A
Actual Date:	16-11-2018
Grant Agreement No.:	730941
Work Package:	NA3
Task Item:	
Lead Partner:	CERN
Document Code:	

**Authors: H. Short (CERN), I. Neilson (STFC), D. Groep (Nikhef)**

© GÉANT on behalf of the AARC project.

The research leading to these results has received funding from the European Community's Horizon2020 Programme under Grant Agreement No. 730941 (AARC2).

## Abstract

Following work in the AARC Project to define an Incident Response Procedure for Federations, this report focuses on validating the proposal by developing tests that involve IdP, SP, Federation and Interfederation operators in simulated security incident response. This document contains a report of a second simulation of an Incident Response scenario.

<b>Simulation Methodology</b>	<b>3</b>
Test Description	3
Test Participants	3
Test Structure	3
Test Guidelines	3
Test Objectives	3
Test Scenario - Traceability Exercise	4
<b>Incident Response Simulation #2</b>	<b>5</b>
Communication Plan	5
Security Contacts	5
Instructions to Participants	6
Post-test Follow-up	7
Participants	7
Instructions for Compromised User	8
<b>AARC Pilot Report # 2</b>	<b>9</b>
Timeline	9
Questionnaire Results	11
Screenshots	14
Simulation Improvements	16
Summary	16
Conclusion and Next Steps	17

# Simulation Methodology

To test the validity of the AARC approach to incident response notification, we propose the following scenarios be simulated. It is expected that email will be the primary communication tool. In this report we provide an analysis of a series of flexible tests, in order to shed light on the reality of incident response in a federated environment. The objective is to test the process, rather than the performance of any of the participants.

## Test Description

### Test Participants

Volunteer participants should be identified, covering both Full-Mesh and Hub-and-Spoke architectures. The participating IdPs and SPs should be compliant with Sirtfi. Federation operators should also be approached to confirm their willingness to be involved, as well as interfederation operators where applicable.

### Test Structure

The test, described below, should be run twice, once purely using Sirtfi contacts from metadata, and a second time involving federation and interfederation operators. An interview should be conducted with the participants following each test.

### Test Guidelines

- Distinct participants should be identified such that roles do not overlap (e.g. the compromised account is the IdP operator)
- A realistic scenario should be identified to bootstrap incident response
- Participants should be warned in advance
- All communication should be clearly marked [TEST] in the subject and contain predefined text to clarify that this is a simulated incident
- Sirtfi obligations, including TLP, should be respected
- Test coordinators should be copied on all communication

### Test Objectives

- Ease of use of security contacts from Metadata
- Necessity of Federation Operators and/or interfederation Support

- Although the aim is to test the process, we may also gain insight into
  - Usefulness of logs
  - Responsiveness of Participants

## Test Scenario - Traceability Exercise

*Scenario: One Service Provider discovers a malicious user and alerts the Identity Provider of this user. Additional affected services are identified and should be able to see activity by the Identity in their logs.*

### Script

1. A “malicious” Identity is used to access SPs across multiple federations
2. The Identity does something suspicious at one SP
3. The SP contacts the IdP of the Identity
4. The IdP checks which other SPs the Identity has accessed
5. The IdP contacts the other SPs directly and requests a response
6. SPs respond with confirmation of the activity

### Roles

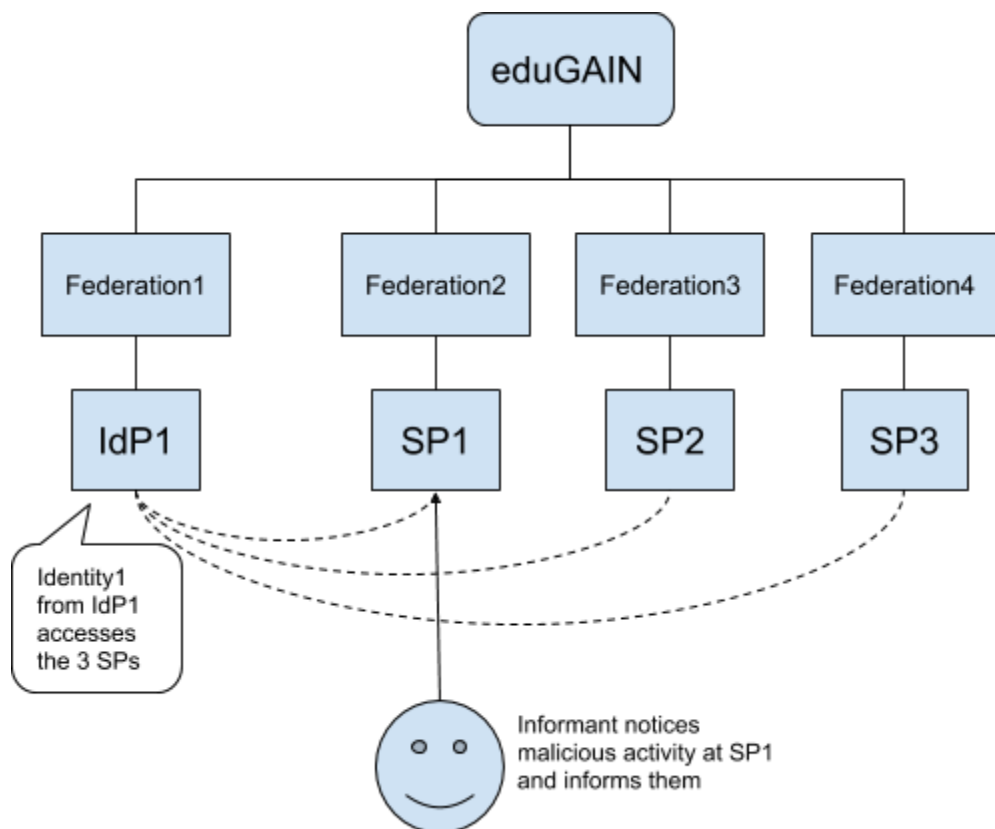
- Identity 1
- SP1
- IdP1
- SP2
- SP3

### Aims

1. All SPs are discovered by the IdP
2. The malicious identity is discovered at each SP
3. SPs and the IdP respond to notifications in a reasonable timeframe

### Test Communicator Actions

1. Ask Identity 1 to authenticate to SP1, 2 and 3 and perform a specific task at SP1 (e.g. create malicious content)
2. Tell SP1 about the specific action
3. Monitor and close the test
4. Post-test Interview



## Incident Response Simulation #2

### Communication Plan

Date	Action	Status
08.10.18	Send instructions to all participants	Complete
15.10.18	Send reminder	Complete
19.10.18	Ask Identity 1 to access SPs and plant logs	Complete
22.10.18	Send trigger email to SP1	Complete

## Security Contacts

The following is a list of security contacts for Federation and Interfederation participants (who do not otherwise have an available list of contacts):

Entity	Security Contact
eduGAIN	support@edugain.org
Incommon	+17343527045 or security@incommon.org
AAF	security@aaf.edu.au
UK Federation	security@ukfederation.org.uk
DFN-AAI	security@aai.dfn.de <a href="https://www.aai.dfn.de/en/security/">https://www.aai.dfn.de/en/security/</a>
Haka	security@csc.fi, for support contact haka@csc.fi
SURFconext	cert@surfnet.nl or support@surfconext.nl

## Instructions to Participants

Hello,

You have agreed to be a volunteer to test Incident Response in Identity Federations, following Incident Response Procedures proposed by AARC and the wider community.

A simulation will take place during the week of **October 22nd**. A short list of questions will be sent afterwards to collect your feedback. Please let us know if you are unavailable.

Please note the following guidelines for email communication during this simulation:

- Please keep the coordinator hannah.short@cern.ch in Cc on all communication
- Message subjects should include [TEST]

- Message bodies should include the boilerplate text **\*\*\*THIS IS A SIMULATED INCIDENT COORDINATED BY AARC\*\*\***
- Security contacts for federation and interfederation will be listed at <https://wiki.geant.org/display/AARC/Temp%3A+Security+Contacts+List>
- The following **procedures** should be read in advance and followed:
  - For IdPs/SPs: <https://wiki.geant.org/display/AARC/Procedure+for+Federation+Participants>
  - For Federation Operators: <https://wiki.geant.org/display/AARC/Procedure+for+Federations>
  - For eduGAIN: <https://wiki.geant.org/display/AARC/Procedure+for+Interfederation>

The following are recommended for all incidents, including this simulation:

- All Sirtfi obligations, including TLP, should be respected
- Timed notes should be taken to aid with postmortem

The simulation will begin by someone from the AARC project sending an email to alert a participant of a security incident. From that point it is up to the volunteers to use Security Contacts to fully explore the scope of the incident. The simulation will end after a week.

**\*\*Please remember that we are not interested in tricking you or analysing how well your organisation completes the test - the aim is to simulate incident response communication and understand where we need to concentrate effort.\*\***

Thanks for your participation!

## Post-test Follow-up

Many thanks for participating in the simulation, please **consider the incident closed**. Particular thanks to those who were not aware and were included in the simulation by surprise - thank you for your willingness to pitch in without notice!

We'd appreciate if you could spend a few minutes to answer the following questions, **by next Friday**, which will be used in a report about the incident:

1. What went well?
2. What didn't go well?
3. Were people responsive?
4. Were you able to get the information you needed?
5. Did you follow the Incident Response Procedure?
6. Was federation operator involvement needed? Please Comment

7. Was the eduGAIN support service needed? Please Comment
8. Would any tools have helped this process?
9. Are there any “lessons learnt” that you would like to share?
10. Do you require the incident report to be anonymous?

If you would like to participate in a post-simulation video conference, to discuss and identify action points, please fill the following Doodle <https://doodle.com/poll/s8665kr79y73pfv8>

Please ensure that any emails where I was not in Cc are sent to me in order to build up a full timeline.

Thanks again and I hope this contributes to protecting our shared infrastructure :)

## Participants

Participant	Federation	IdP/SP	Role Test 1
User	UK Fed	Jisc	Identity 1
Jisc	UK Fed	IdP	IdP1
ORCID	Incorrectly identified as Incommon (registrar is actually SURFconext)	SP <a href="https://orcid.org/signin">https://orcid.org/signin</a>	SP1
CSC	Haka	SP <a href="https://lbr.csc.fi/shibboleth">https://lbr.csc.fi/shibboleth</a>	SP3
MWA Telescope Collaboration	AAF	SP <a href="https://wiki.mwatelescope.org">https://wiki.mwatelescope.org</a>	SP2
UK Fed		Federation	
Haka		Federation	
AAF		Federation	
Incommon		Federation	
eduGAIN		Interfederation	



## Instructions for Compromised User

Please perform the following steps between now and Monday morning, and let me know when you're finished.

- Log in to <https://orcid.org/signin> with your IdP
- Log in to <https://zenodo.org/> with ORCID (signed in through your IdP) and upload something with the text “[TEST] this document is part of a security incident simulation”
- Log in to <https://wiki.mwatelescope.org> - and register as a user
- Log in to <https://lbr.csc.fi> and download a few documents

Your background story, when you are asked for details: you re-used your email and password on Facebook and believe it was compromised.

## AARC Pilot Report # 2

### Timeline

Day	Time (CEST)	Action (orange text indicates entity's first action within the incident)
<b>Monday 22nd</b>	11:00	<b>CERN Computer Security</b> informed <b>Zenodo</b> about malicious content [CERN: RQF1143915]
	11:54	Zenodo identifies that the user was authenticated through ORCID
	15:00	Zenodo contacts <b>ORCID</b> with account identifier
	15:44	ORCID replies <ul style="list-style-type: none"> <li>• Disables the ORCID account</li> <li>• Loops in the <b>Jisc IdP</b> (Cc)</li> <li>• Loops in the <b>Surfconext Federation</b> (Cc)</li> </ul>
	15:56	ORCID receives a bounce from Jisc so included the <b>UK Federation</b>
	17:17	ORCID contacts User to say that they believe his account is compromised

	17:45	UK Federation contacts ORCID to acknowledge receipt and says they are investigating
	17:55	UK Federation contacts IdP operator to contact the user and, if necessary, disable the account
<b>Tuesday 23rd</b>		
	09:00	UK Federation speaks with Jisc Infosec team
	09:00	UK Federation calls the User
	11:28	UK Federation compiles list of who to contact
	14:07	UK Federation contacts <b>CSC</b> (TLP:AMBER)
	14:09	UK Federation contacts <b>MWA</b> (TLP:AMBER)
	14:19	UK Federation contacts ORCID to provide additional information (TLP:AMBER)
	14:23	Jisc Security Team updates Federation and IdP operator that the incident should be considered in progress
	14:33	ORCID disconnects Jisc ID from ORCID account
	14:55	CSC Security replies to UK Federation to say that they will act
	15:47	CSC sends transaction logs to UK Federation
<b>Wednesday 24th</b>		
	02:28	MWA responds to UK Federation
	02:53	MWA includes their local university contact, <b>eduGAIN</b> , <b>Incommon</b> , UK Federation
	02:53	MWA responds with information about user activity
	09:32	eduGAIN looks for discussion channel for the team
	11:39	AAF asks whether they should have been contacted. Asked to allow the

		incident to continue naturally.
	13:38	eduGAIN replies to UK Federation asking whether the User identity has been disabled
	14:32	eduGAIN confirms with MWA that no services behind the proxy were contacted
	16:21	UK Federation informs <b>AAF</b> that one of their SPs was involved in an Incident and that it has been resolved
	16:32	UK Federation informs <b>DFN</b> that a CSC service has been involved in an incident but that incident is closed
	16:39	UK Federation informs <b>Surfnet</b> that one of their SPs was involved in an Incident and that it has been resolved
	22:22	AAF thanks UK Federation
<b>Thursday 25th</b>		
	09:06	SURFcert responds to UK Federation to say that they have no additional information and do not seem to be needed
	10:15	eduGAIN thanks MWA for clarification and is piecing together the puzzle
	16:37	eduGAIN checks with SURFconext to try and elicit a response
<b>Friday 26th</b>		
	10:49	eduGAIN begins incident closure with draft report. Includes UK Federation, IdP, MWA.
	11:39	UK Federation provides additional information from DFN, HAKA, SURFconext
	13:41	eduGAIN asks UK Federation for further information r.e.
	14:28	eduGAIN asks UK Federation for further information r.e. CSC
	16:25	eduGAIN sends report to UK Federation, Jisc, MWA, AAF, DFN, SURFnet, SURFconext

	16:35	Incident Closed
--	-------	-----------------

## Questionnaire Results

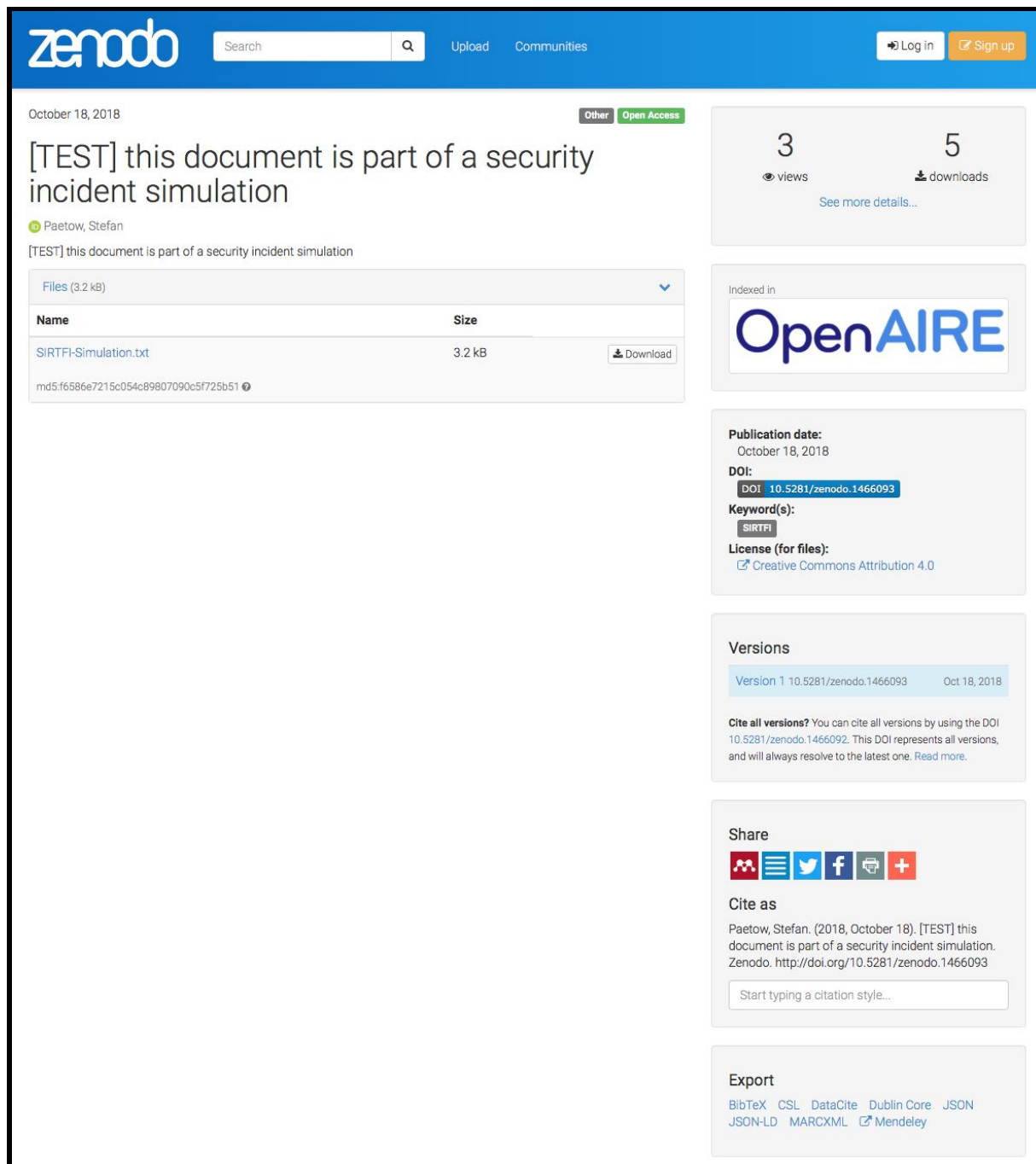
A follow up questionnaire was sent. Some participants responded via email and others during a video conference. This is a summary of responses, excluding feedback regarding the organisation of the simulation itself.

Question	Summarised Answers
What went well?	<ul style="list-style-type: none"> <li>● The incident was resolved and a report produced</li> <li>● The user appreciated being contacted by various parties</li> <li>● Information collection and ticketing systems worked well</li> </ul>
What didn't go well?	<ul style="list-style-type: none"> <li>● Some Entities did not loop in their Federation</li> <li>● Some email communication bounced due to sender restrictions</li> <li>● eduGAIN was looped in late</li> <li>● The report was not shared with all affected participants</li> <li>● The originating SP (ORCID) did not receive follow-up</li> <li>● MET was used to find contacts and gave unreliable answers</li> <li>● The procedures were not always followed closely</li> </ul>
Were people responsive?	<ul style="list-style-type: none"> <li>● Mostly</li> <li>● An acknowledgement of receipt of an incident notification would have been appreciated</li> </ul>
Were you able to get the information you needed?	<ul style="list-style-type: none"> <li>● Yes</li> <li>● All requested information was gathered</li> <li>● No encryption was attempted</li> </ul>
Did you follow the Incident Response Procedure?	<ul style="list-style-type: none"> <li>● All attempted to follow the procedure (excluding those who were not warned previously)</li> <li>● Certain mistakes were made, e.g.               <ul style="list-style-type: none"> <li>○ Not including Federations</li> <li>○ Not including eduGAIN</li> <li>○ Not using TLP</li> </ul> </li> </ul>
Was federation operator involvement needed? Please Comment	<ul style="list-style-type: none"> <li>● Yes</li> </ul>
Was the eduGAIN support service	<ul style="list-style-type: none"> <li>● Yes</li> </ul>

<p>needed? Please Comment</p>	<ul style="list-style-type: none"> <li>● General agreement that having the overall perspective was useful, particularly for coordinating and producing the report</li> </ul>
<p>Would any tools have helped this process?</p>	<p>Email and ticketing systems were the primary tools used. Tools that may be of interest include:</p> <ul style="list-style-type: none"> <li>● A chat where all affected participants could discuss</li> <li>● The ability to send encrypted or signed information and verify identities would have been appreciated by some participants</li> <li>● A central place for accessing the incident response procedure</li> <li>● A platform for storing incident reports</li> </ul>
<p>Are there any “lessons learnt” that you would like to share?</p>	<ul style="list-style-type: none"> <li>● Many “lessons learnt” internally at organisations, e.g. communication improvements</li> <li>● Direct contact with the affected entity is preferred, in parallel to looping in the federation operator and interfederation, for the sake of efficiency</li> <li>● Suggestion to consider Trusted Introducer as a trust building mechanism</li> <li>● Feedback for the procedure includes <ul style="list-style-type: none"> <li>○ Guidance on implementation on specific steps, e.g. announcing suspension of service</li> <li>○ Highlighting requirements to follow up with affected Users</li> <li>○ Clarity on how to inform people who is the coordinator, and how the transition of the coordinator role should work</li> <li>○ TLP is not considered a strong control, suggestion to include guidance on when to use encryption</li> </ul> </li> <li>● General consensus that this exercise was useful</li> <li>● In reality the line between IdP operator, Federation, Sirtfi contact, Organisation Security Team and other parties is often blurred. The procedures should be suitable flexible.</li> </ul>
<p>Do you require the incident report to be anonymous?</p>	<ul style="list-style-type: none"> <li>● Agreement to send this report around all participants prior to publishing</li> </ul>

## Screenshots

“Malicious” content on Zenodo:



The screenshot shows a Zenodo record page for a document. The document title is "[TEST] this document is part of a security incident simulation" and it was published on October 18, 2018, by Paetow, Stefan. The document is 3.2 kB in size and is available for download. The record is indexed in OpenAIRE and has 3 views and 5 downloads. The publication date is October 18, 2018, and the DOI is 10.5281/zenodo.1466093. The keyword is SIRTPI and the license is Creative Commons Attribution 4.0. The record has one version, Version 1, published on October 18, 2018. The record is shared on various social media platforms and can be cited as: Paetow, Stefan. (2018, October 18). [TEST] this document is part of a security incident simulation. Zenodo. <http://doi.org/10.5281/zenodo.1466093>. The record can be exported in various formats including BibTeX, CSL, DataCite, Dublin Core, JSON, JSON-LD, MARCXML, and Mendeley.

zenodo Search Upload Communities Log in Sign up

October 18, 2018 Other Open Access

### [TEST] this document is part of a security incident simulation

Paetow, Stefan

[TEST] this document is part of a security incident simulation

Files (3.2 kB)

Name	Size	
SIRTPI-Simulation.txt	3.2 kB	Download

md5:f6586e7215c054c89807090c5f725b51

3 views 5 downloads See more details...

Indexed in OpenAIRE

**Publication date:** October 18, 2018  
**DOI:** DOI 10.5281/zenodo.1466093  
**Keyword(s):** SIRTPI  
**License (for files):** Creative Commons Attribution 4.0

**Versions**

Version 1 10.5281/zenodo.1466093 Oct 18, 2018

**Cite all versions?** You can cite all versions by using the DOI 10.5281/zenodo.1466092. This DOI represents all versions, and will always resolve to the latest one. Read more.

**Share**

**Cite as**

Paetow, Stefan. (2018, October 18). [TEST] this document is part of a security incident simulation. Zenodo. <http://doi.org/10.5281/zenodo.1466093>

Start typing a citation style...

**Export**

BibTeX CSL DataCite Dublin Core JSON JSON-LD MARCXML Mendeley

## Incident Report:

```
** AMBER Information - Limited Distribution **
** see https://www.us-cert.gov/tlp for distribution restrictions **

Summary of incident (eduGAIN-2018102434000027)
-----
A compromise account was detected by an SP registered in eduGAIN. The incident
was handled by the user's IdP who blocked the user and notified the SPs that
were used by the offenders to check their systems and possibly suspend the user
during the incident resolution.

The incident is closed now. The user's credentials have been re-set and the
user account shall be activated on systems that decided to suspend it before.

Details
-----
On 23rd of Oct 2018 an SP (identified as https://orcid.org/saml2/sp/1, from
SURConext) alerted the Jisc IdP (https://idp.jisc.ac.uk/idp/shibboleth, UK
federation) about unauthorised access by an account from the IdP. In response
to the alert the IdP suspended the user account and identified the SPs that
were accessed by the offender. The SPs and corresponding federations were
subsequently contacted by the IdP who shared details about the users and
accesses.

Three SPs were involved:
https://proxy.mwatelescope.org/sp (AAF)
- provided detailed response, including activities, access times and IP
  addresses used by the offender
- suspended the user account

https://orcid.org/saml2/sp/1 (SURConext)
- reported initially the incident
- suspended the user account

https://lbr.csc.fi/shibboleth (DFN-AAI / HAKA)
- logs checked, simulated suspension

Timeline (as per OTRS)
-----
2018-10-23 Compromised account detected by ORCID SP, reported to Jisc IdP. Jisc
contacts affected SPs.
2018-10-23 13:32 (UTC) User suspended at ORCID SP
2018-10-23 14:01 (UTC) User suspension (simulated) at lbr.csc.fi SP
2018-10-23 20:09 (UTC) UK federation warns MWATelescope SP about compromised
account.
2018-10-24 00:53 (UTC) MWATelescope responds, notifying eduGAIN, too.
2018-10-24 00:53 (UTC) User suspended at MWATelescope.
2018-10-24 13:12 (UTC) Details provided by Jisc to eduGAIN (user suspended at
IdP, confirmed SPs that were contacted)
2018-10-24 15:21 - 15:40 (UTC) Jisc informs federations of affected SP about
the incident
2018-10-26 User's credentials reset, user unbanned at IdP
```

## Simulation Improvements

Certain improvements in the simulation execution were identified. These should be taken into account

- As far as possible, all participants should be aware in advance of the procedure and planned dates
- The malicious activity should take place during the week of the simulation to avoid potential confusion
- In this case, the incorrect Federation was identified for one SP. Care should be taken to avoid this in future.

## Summary

This second simulation was more successful than the first<sup>1</sup>, in terms of incident resolution. At the same time, there are significant lessons that can be learnt from the points of failure. Key results of this simulation include:

1. The availability of Federation and Interfederation security contact details should be addressed as a priority
2. Identifying the correct Sirtfi contact for Federated Entities is non trivial due to federation overlap
3. Further thought is required into how and where the Incident Reports should be made available to those affected, either directly or as part of the wider community
4. Regarding the proposed Incident Response Procedures:
  - a. Involving Federation Operators and Interfederation appears to be the correct approach
  - b. Guidance is required on how to identify, or nominate yourself as, the Incident Coordinator
  - c. A procedure step to “acknowledge” incident response communication should be considered
5. The community’s capability to send encrypted or authenticated (signed) messages should be understood and provision made for secure exchange of information

---

<sup>1</sup> <https://aarc-project.eu/wp-content/uploads/2018/04/20180326-Incident-Simulation-Report.pdf>



## Conclusion and Next Steps

This simulation provided input into the proposed Security Incident Response Procedures<sup>2</sup>. The procedures will be reviewed within the context of the REFEDS Sirtfi Working Group<sup>3</sup>, improved, and a community wide consultation will be undertaken. It is suggested that the final procedures be well circulated and published on the REFEDS Sirtfi website.

Simulation participants were in agreement that simulations were useful, particularly for exposing improvements within their organisation. It is suggested that these simulations be coordinated in future through WISE, the community for Wise Information Security for e-Infrastructures<sup>4</sup>.

---

<sup>2</sup>

<https://aarc-project.eu/wp-content/uploads/2017/02/DNA3.2-Security-Incident-Response-Procedure-v1.0.pdf>

<sup>3</sup> <https://wiki.refeds.org/display/GROUPS/SIRTFI>

<sup>4</sup> <https://wise-community.org>