MINISTERIO
DE INDUSTRIA, TURISMO
Y COMERCIO

red.es

Incident Handling

3rd OSCT Meeting

19th-20th June, 2007 Edinburg

Red IRIS

Index

MINISTERIO DE INDUSTRIA, TURISMO Y COMERCIO

red.es

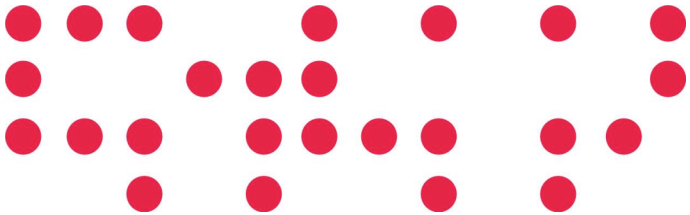
1. Scenario
2. What is RTIR?
3. Using RTIR in Our Scenario
4. Feature for OSCT

Red IRIS

Index

MINISTERIO DE INDUSTRIA, TURISMO Y COMERCIO

red.es



Red IRIS

Scenario (I)

MINISTERIO DE INDUSTRIA, TURISMO Y COMERCIO

red.es

- Actors
  - OSCT member on shift called
    - SfE-A, SfE-F
  - ROC Security Officers
    - SfE-B, SfE-C, SfE-D
  - External user
    - U-E
- The real-time status board
  - Place where information related a problem would be shared
- Malicious patterns or hosts
  - P1 -> Evil Host attacking and trying to get access in EGEE infrastructure
  - P2 -> Suspicious file found on a compromised box

Red IRIS

Scenario (II)

MINISTERIO DE INDUSTRIA, TURISMO Y COMERCIO

red.es

- U-D sends a complaint/warning to EGEE-CSIRT
  - Got some strange flows
  - Got a compromised box where he/she discovers source of the attack (P1) and possible targets
- SfE-A takes the report and starts studying, and looking for related reports
- SfE-A finds a report with P2
  - P2 was a back-door for P1
- A heads-up is sent to EGEE CSIRTS with P1 and P2
  - SfE-B replies with no relevant information
  - SfE-C replies and confirms, it's affected
- SfE-A and SfE-C share information to fix the problems by the real-time status board
- SfE-D has a late reply, confirming it's probably infected
  - So SfE-D gets access to the real-time status board

Scenario (III)

MINISTERIO DE INDUSTRIA, TURISMO Y COMERCIO

red.es

- SfE-A gets sick, so SfE-F takes over the problem
- SfE-D after checking, it sees not infected
  - So no longer rigths for real-time status board
- Incident is contained and resolved
- SfE-F updates the "real-time status board" with all sensitive details (possibly private information), which is available to all involved sites (here: only SfE-C)
- SfE-F post a summary report without sensitive information
- SfE-F resolve the ticket

Red IRIS

Scenario (IV)

MINISTERIO DE INDUSTRIA, TURISMO Y COMERCIO

red.es

- Features asked to a tool for handling our case study
  - No sensitive information has been sent to (and leaked from!) mailing list.
  - Coordinators received much less requests
  - A clear status of the incident was available at all time to all involved sites by the real-time status board
  - Sites that joined the incident later had immediate access to the archive as well as a real-time status, without having to question the coordinator

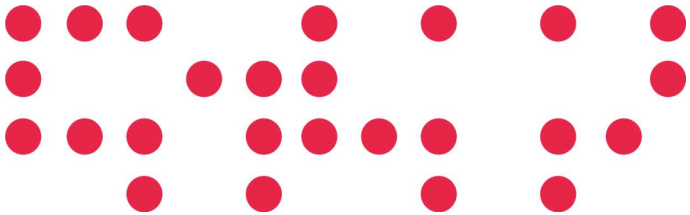
RedIRIS

Index

MINISTERIO DE INDUSTRIA, TURISMO Y COMERCIO

red.es

1. Scenario
2. What is RTIR?
3. Using RTIR in Our Scenario
4. Feature for OSCT



Red IRIS

What is RTIR? (I)

MINISTERIO DE INDUSTRIA, TURISMO Y COMERCIO

red.es

- A tool for incident handling
- Design for IRT workflows.
- Based on Request Tracker RT (http://www.bestpractical.com)
- What we wanted to do?
  - Allow an IRT staff to manage increasing workload effectively
  - Be easily extensible
  - Meet needed features for IRT
    - Care of confidentiality
    - …

RedIRIS

What is RTIR? (II)

MINISTERIO DE INDUSTRIA, TURISMO Y COMERCIO

red.es

- Why?
  - Increasing volume of incidents
  - Requirement for multiple person triage
  - System struggling to cope
  - Need to increase resilence
  - Increase automation
  - Allow several levels of helpdesk
  - No tools for IH
    - Status now not too different

RedIRIS

What is RTIR? (III)

MINISTERIO DE INDUSTRIA, TURISMO Y COMERCIO

red.es

- Structure
  - Incident Report
    - Someone has a complaint of our constituency
  - Investigations
    - IRT attempts to get the root of the problem
  - Blocks
    - Track network level intervention against threat
  - Incidents
    - Ties it all together. May have many related incident reports, investigations and blocks.

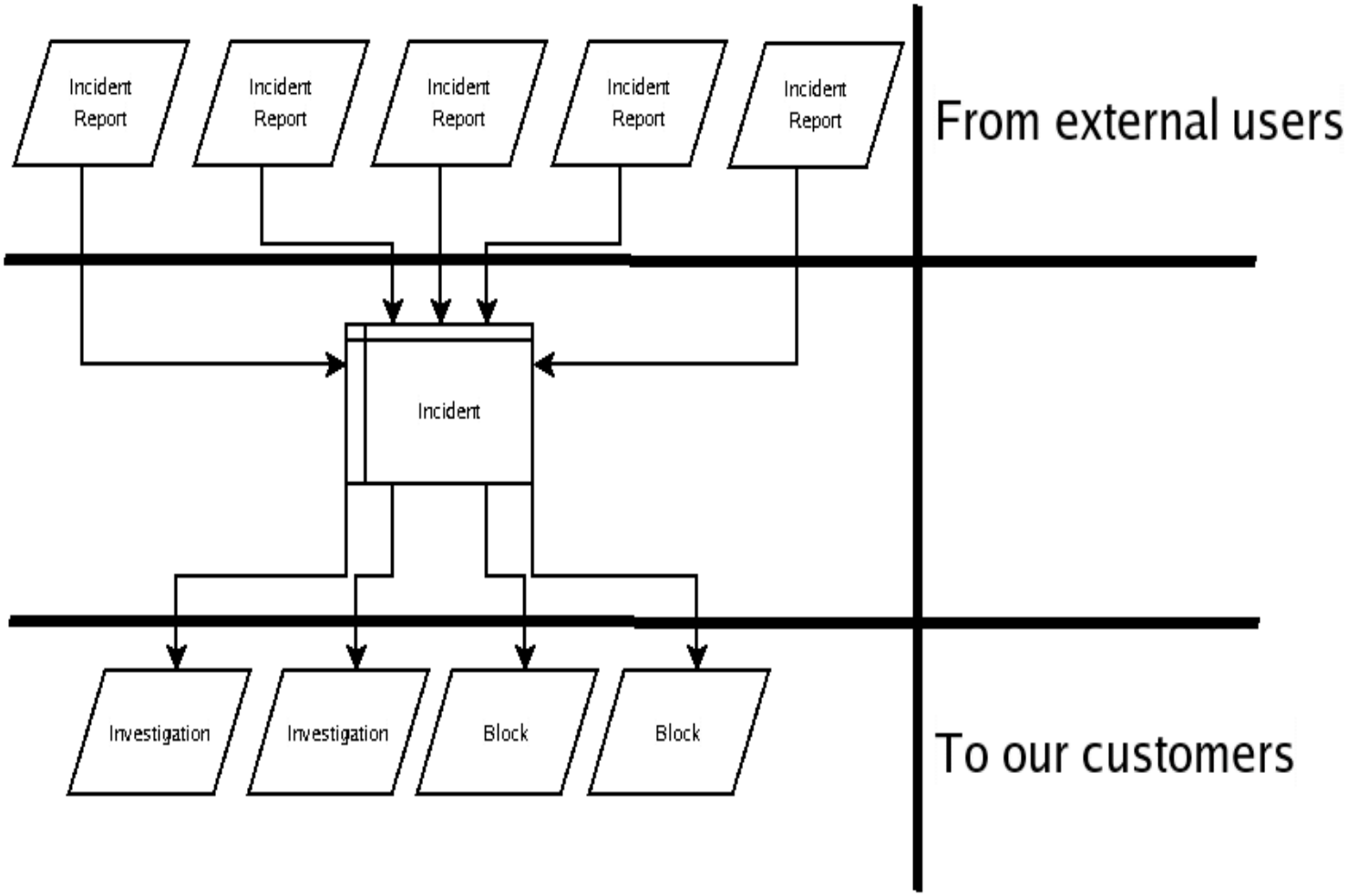
Red IRIS

What is RTIR? (IV)

MINISTERIO DE INDUSTRIA, TURISMO Y COMERCIO

red.es

- Structure



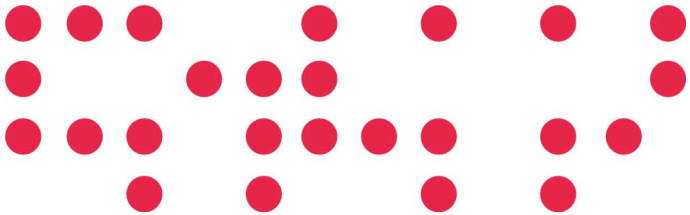
RedIRIS

Index

MINISTERIO DE INDUSTRIA, TURISMO Y COMERCIO

red.es

1. Scenario
2. What is RTIR?
3. Using RTIR in Our Scenario
4. Feature for OSCT



Red IRIS

Using RTIR in our scenario (I)

MINISTERIO DE INDUSTRIA, TURISMO Y COMERCIO

red.es

- U-D sends a complaint/warning to EGEE-CSIRT

RTIR (2 Nuevos Incidents Reports) - Mozilla Firefox

Archivo Editar Ver Ir Marcadores Herramientas Ayuda

http://rt.rediris.es/RTIR/index.html

Work Red Hat, I... Red Hat ... Support Shop Products Training

RTIR (2 Nuevos Incidents Repor... | Barrapunto: La información que t... | Working Links

Red IRIS

Preferences | About RTIR | Logout

Logged in as root

RTIR for IRIS-CERT

Search Incidents

RT

RTIR Home

Incidents

Incident Reports

Investigations

Blocks

Tools

RT for Incident Response (2 Nuevos Incidents Reports)

2 of 2 new unlinked Incident Reports...

#	Subject	From	Owner	Due	
48980	Ticket [TI #159692] Resuelto	cau@uam.es	Nobody	in 2 hours	[Take]
48855	Security breaches from your network [Bulk Reject]	david.adams@ultimateuptime.net	sergior	in 5 days	[Steal]

Refresh

Every 5 minutes Go!

Most due 1 incidents owned by root (and unowned)...

#	Subject	Owner	Priority	Due
48982	Example for E-Coat presentation at 5th Abuse Workshop	root	10	in 2 hours

Most due 46 incidents...

#	Subject	Owner	Priority	Due	
46041	Re bichos project	paco	10	5 weeks ago	[Steal]
43250	[gratisweb.com] URL de contenidos maliciones	paco	10	4 weeks ago	[Steal]
47361	[icac.es] posible router comprometido	paco	10	3 weeks ago	[Steal]
48772	[upf.es] Portscan fr 193.145.38.38	chelo	10	3 hours ago	[Steal]
48452	[csic.es] Escaneos desde 161.111.93.61	chelo	10	2 hours ago	[Steal]
48245	[umh.es] Conexiones TCP 3000 desde 193.147.142.6	chelo	10	107 min ago	[Steal]
47912	[uam.es] Conexiones puerto UDP 80 150.244.65.1	sergior	10	53 min ago	[Steal]
48448	[upc.es] Unauthorized Access Attempts from Your IP - 147.83.156.34	chelo	10	in 52 min	[Steal]

http://rt.rediris.es/RTIR/index.html

Psi RTIR (2 Nue 2008-01-10 12:31

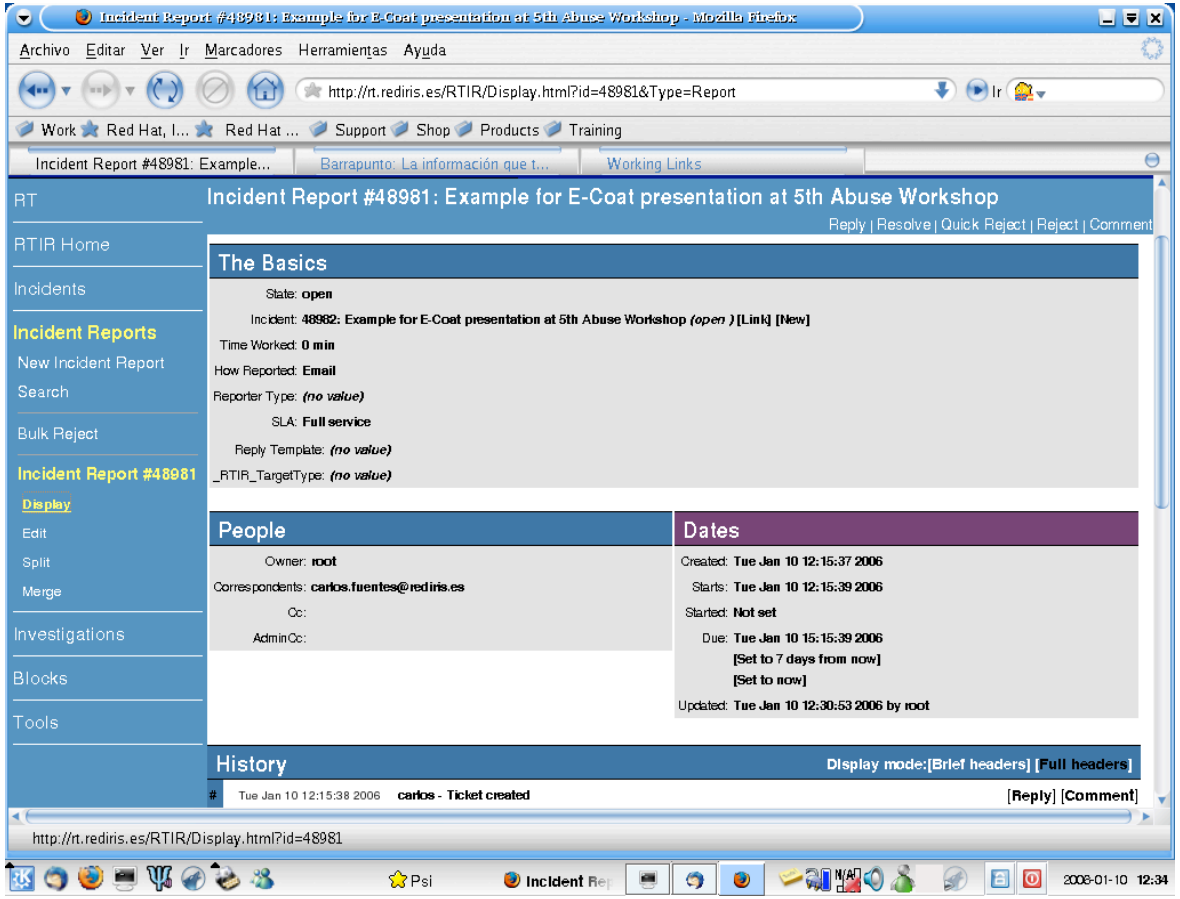
Red IRIS

Using RTIR in our scenario (II)

MINISTERIO DE INDUSTRIA, TURISMO Y COMERCIO

red.es

- SfE-A takes the report and starts studying, and looking for related reports



RedIRIS

Using RTIR in our scenario (III)

MINISTERIO DE INDUSTRIA, TURISMO Y COMERCIO

red.es

- SfE-A finds a report with P2

Lookup 130.206.1.130 using server whois.ripe.net - Mozilla Firefox

Archivo Editar Ver Ir Marcadores Herramientas Ayuda

http://rt.rediris.es/RTIR/Tools/Lookup.html?ticket=48981&type=ip&q=130.206.1.130

Work | Red Hat, I... | Red Hat ... | Support | Shop | Products | Training

Lookup 130.206.1.130 using serv... | El ex gobernador de EEUU en Ira...

Preferences | About RTIR | Logout

Logged in as root

RTIR for IRIS-CERT

Search Incidents

RT
RTIR Home
Incidents
Incident Reports
Investigations
Blocks
Tools
Lookup
Reporting
Scripted Action
By Email address
By IP address

Lookup 130.206.1.130 using server whois.ripe.net

Current Report: #48981

#	Subject / Requestor(s)	State / Owner	Last Updated / Last Contact	Created / Due	Priority / Left
48981	Example for E-Coat presentation at 5th Abuse Workshop / carlos.fuentes@rediris.es	open / root	56 sec / 56 sec	22 hours / in 6 days	N/A / 0

Incidents: 130.206.1.130

id	Subject	State	Priority	Actions
48982	Example for E-Coat presentation at 5th Abuse Workshop	open	10	[Link] [Investigate]

[New] [Refine Search]

Investigations: 130.206.1.130

id	Subject	State	Priority	Actions
(no Investigations)				

[Refine Search]

Incident Reports: 130.206.1.130

id	Subject	State	Priority	Actions
48981	Example for E-Coat presentation at 5th Abuse Workshop	open	0	

[Refine Search]

Blocks: 130.206.1.130

id	Subject	State	Priority	Actions
(no Blocks)				

[Refine Search]

Look Up Information

WHOIS: 130.206.1.130 at whois.ripe.net Go

Esperando a rt.rediris.es...

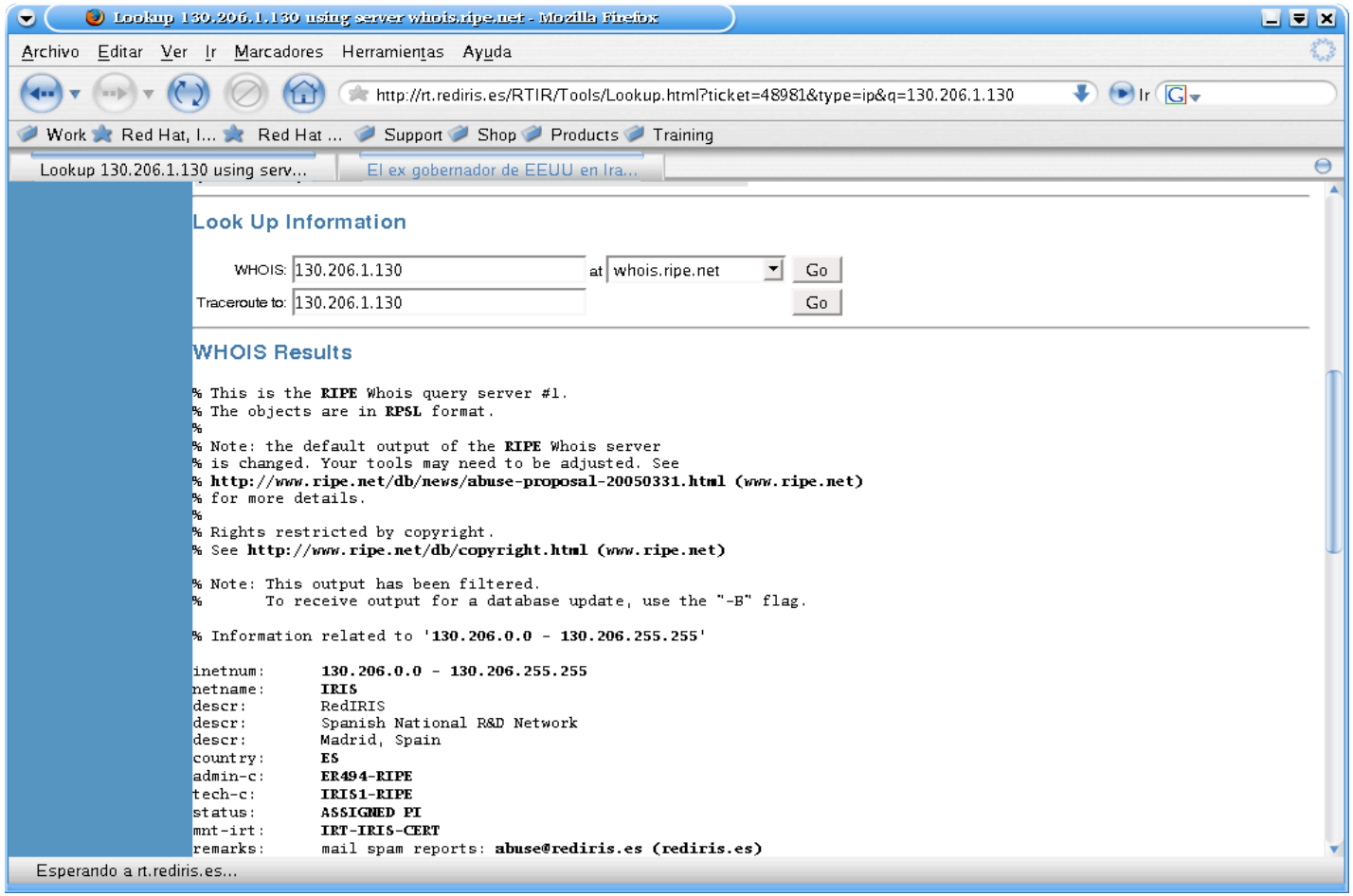
RedIRIS

Using RTIR in our scenario (IV)

MINISTERIO DE INDUSTRIA, TURISMO Y COMERCIO

red.es

- If RTIR is connected to GOCDB, it could give info related to that IP



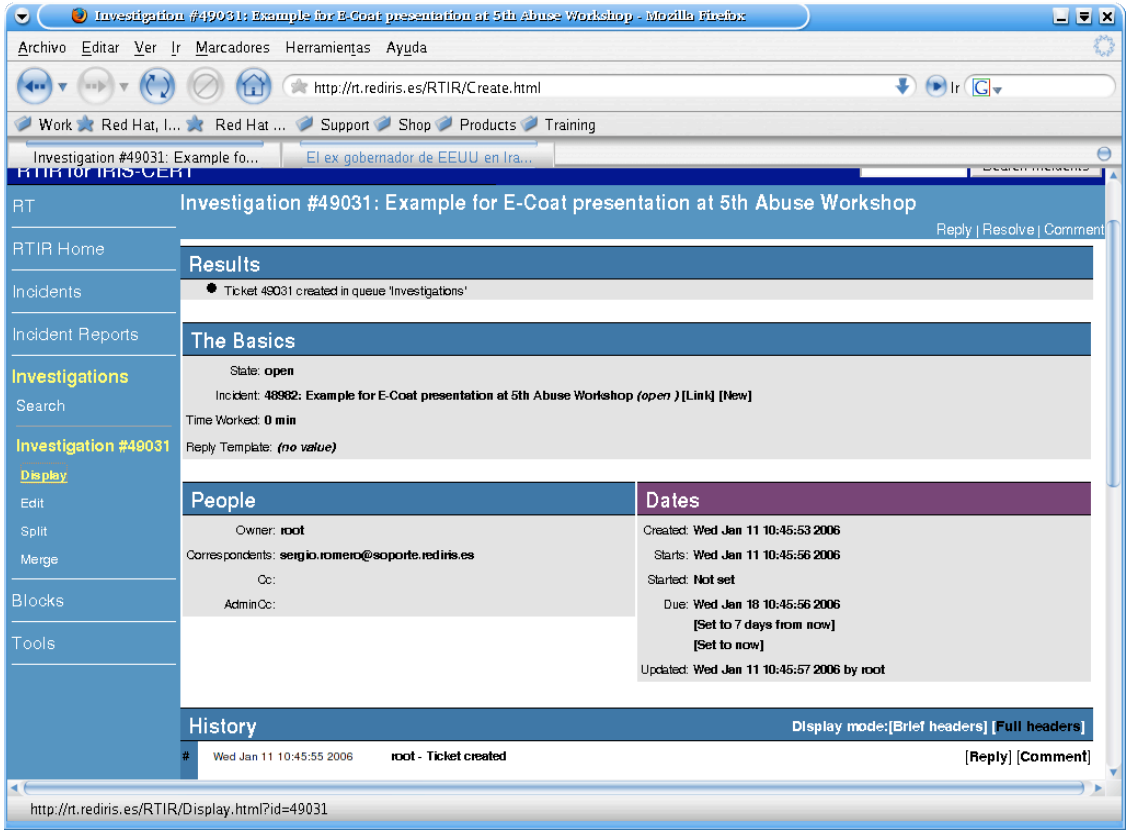
RedIRIS

Using RTIR in our scenario (V)

MINISTERIO DE INDUSTRIA, TURISMO Y COMERCIO

red.es

- A heads-up is sent to EGEE CSIRTS with P1 and P2



An Investigation has been launched for keeping track the Heads-up

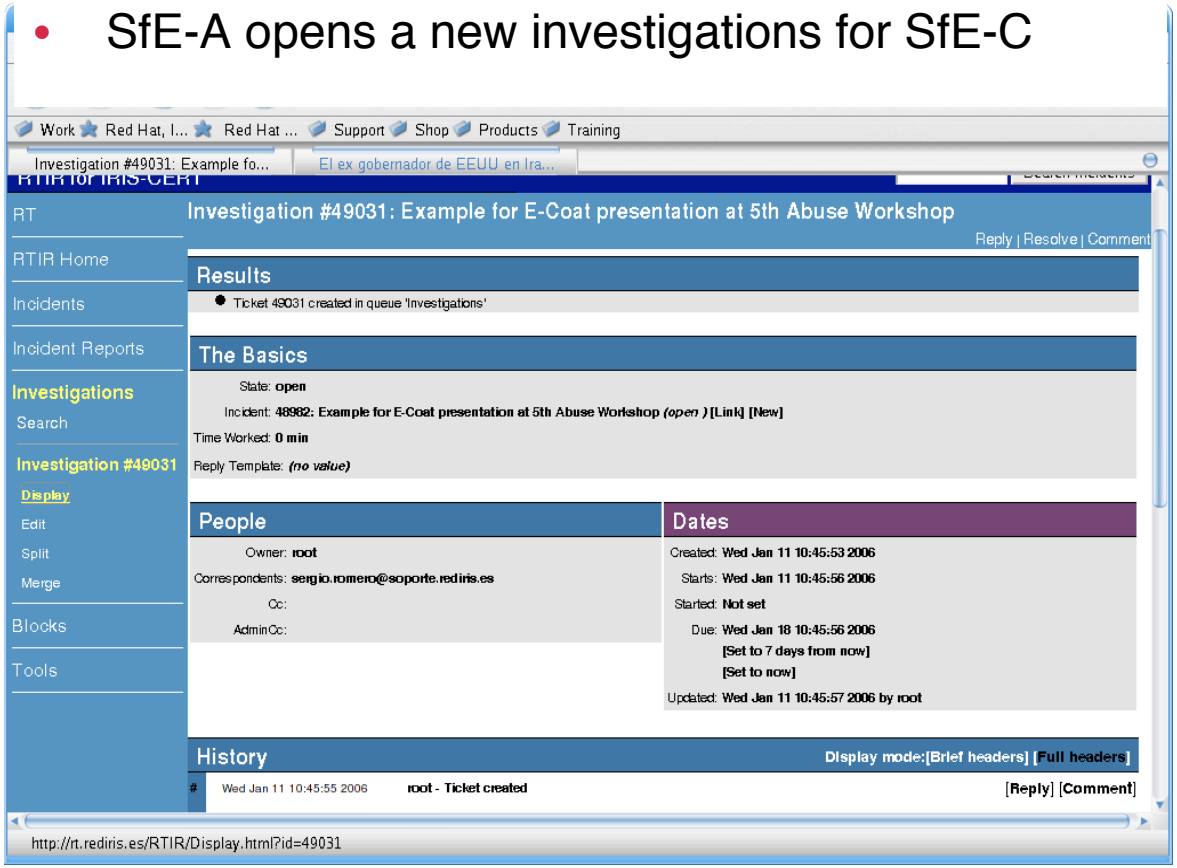
RedIRIS

Using RTIR in our scenario (VI)

MINISTERIO DE INDUSTRIA, TURISMO Y COMERCIO

red.es

- SfE-B replies with no relevant information
- SfE-C replies and confirms, it's affected



- SfE-A opens a new investigations for SfE-C

RedIRIS

Using RTIR in our scenario (VII)

MINISTERIO DE INDUSTRIA, TURISMO Y COMERCIO

red.es

- SfE-A and SfE-C share information to fix the problems by the real-time status board
  - SfE-A would modify the ACLs for giving to SfE-C enc ent.

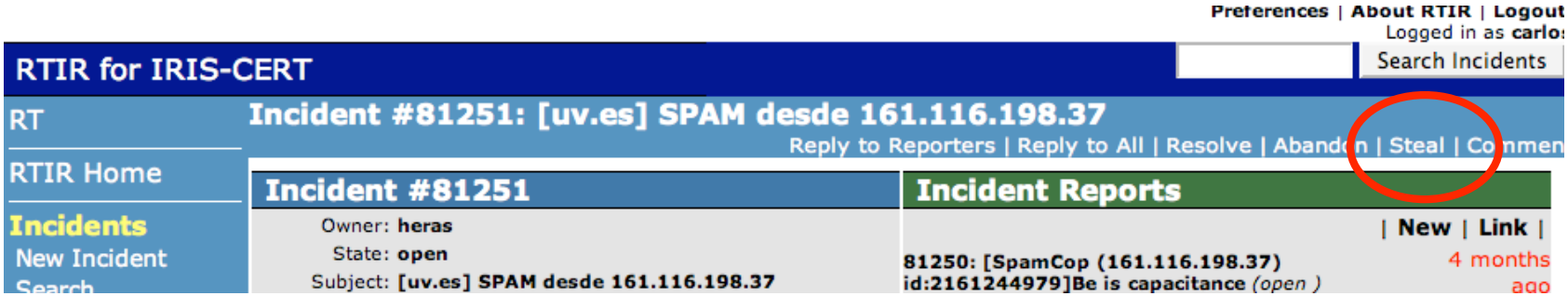
RedIRIS

Using RTIR in our scenario (VIII)

MINISTERIO DE INDUSTRIA, TURISMO Y COMERCIO

red.es

- SfE-A gets sick, so SfE-F takes over the problem



- SfE-D after checking, it sees not infected
  - So no longer rigths for real-time status board

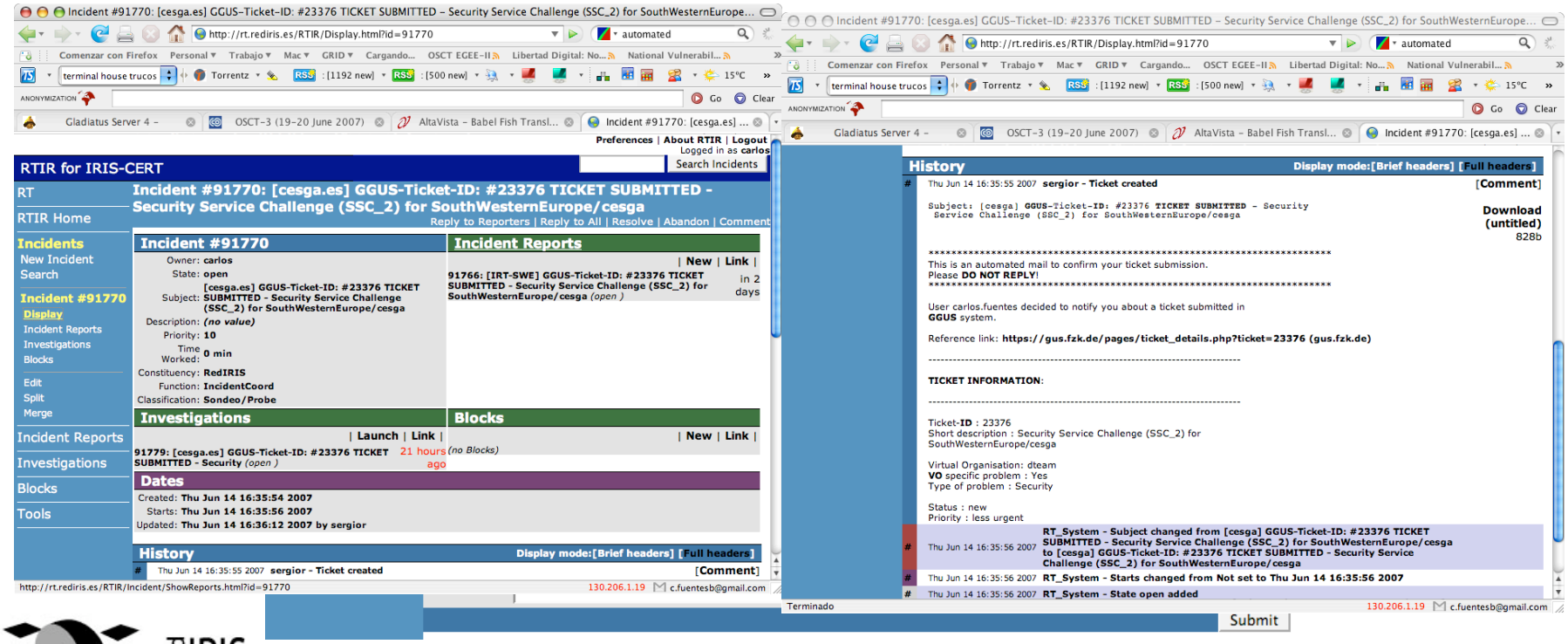
Red IRIS

Using RTIR in our scenario (IX)

MINISTERIO DE INDUSTRIA, TURISMO Y COMERCIO

red.es

- Incident is contained and resolved
- SfE-F updates the "real-time status board" with all sensitive details (possibly private information), which is available to all involved sites (here: only SfE-C)
- SfE-F resolve the ticket



RedIRIS

Index

RTIR offering to OSCT

MINISTERIO DE INDUSTRIA, TURISMO Y COMERCIO

red.es

- Archiving
  - Each issue/complaint/behaviour is stored in the DB
- Searching
  - By Customer
  - By IP/NetRange
  - …
  - By everything which is saved in the DB
- Association of incident and users from GOCDB
  - Even this would be able to be automated
- An acknowledge database
  - RTIR is linked to RTFM
- Allows to run multiple constituencies
  - Several teams can use same infrastructure

RedIRIS

¿¿¿Questions???

red.es

Red IRIS

Edificio Bronce
Plaza Manuel Gómez Moreno s/n
28020 Madrid. España

Tel.: 91 212 76 20 / 25
Fax: 91 212 76 35
www.red.es