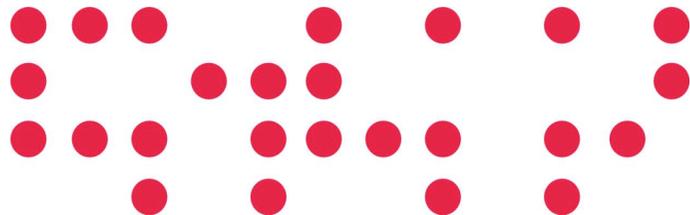




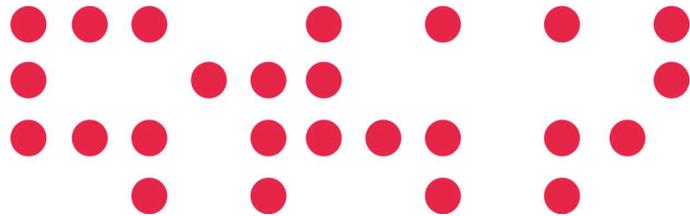
Incident Handling

3rd OSCT Meeting
19th-20th June, 2007 Edinburg

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



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



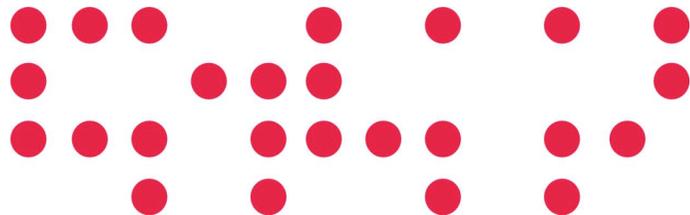
- Actors
 - OSCT member on shift called
 - SfE-A, SfE-F
 - ROC Security Officers
 - SfE-B, SfE-C, SfE-D
 - External user
 - U-E
- The real-time status board
 - Place where information related a problem would be shared
- Malicious patterns or hosts
 - P1 -> Evil Host attacking and trying to get access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

- 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

- SfE-A gets sick, so SfE-F takes over the problem
- SfE-D after checking, it sees not infected
 - So no longer rights 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

- 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

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

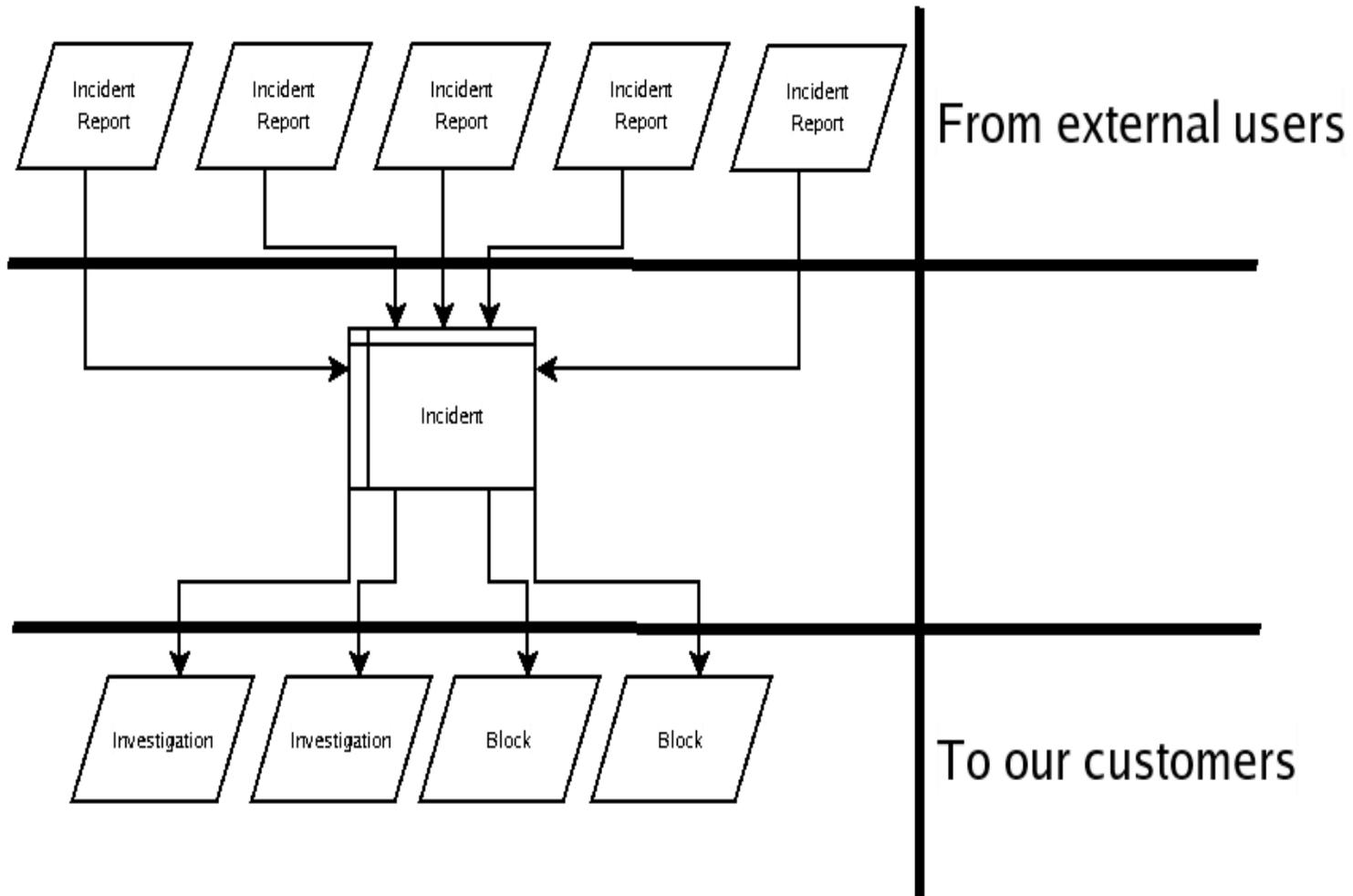


- A tool for incident handling
- Design for IRT workflows.
- Based on Request Tracker RT (<http://www.bestpractical.com>)
- What we wanted to do?
 - Allow an IRT staff to manage increasing workload effectively
 - Be easily extensible
 - Meet needed features for IRT
 - Care of confidentiality
 - ...

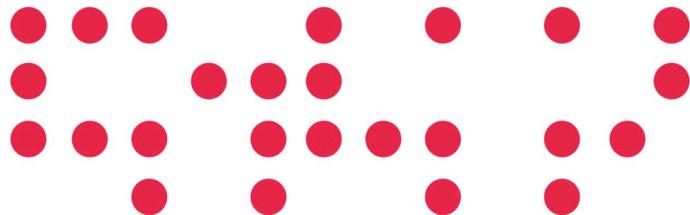
- Why?
 - Increasing volume of incidents
 - Requirement for multiple person triage
 - System struggling to cope
 - Need to increase resilience
 - Increase automation
 - Allow several levels of helpdesk
 - No tools for IH
 - Status now not too different

- 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.

- Structure



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



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

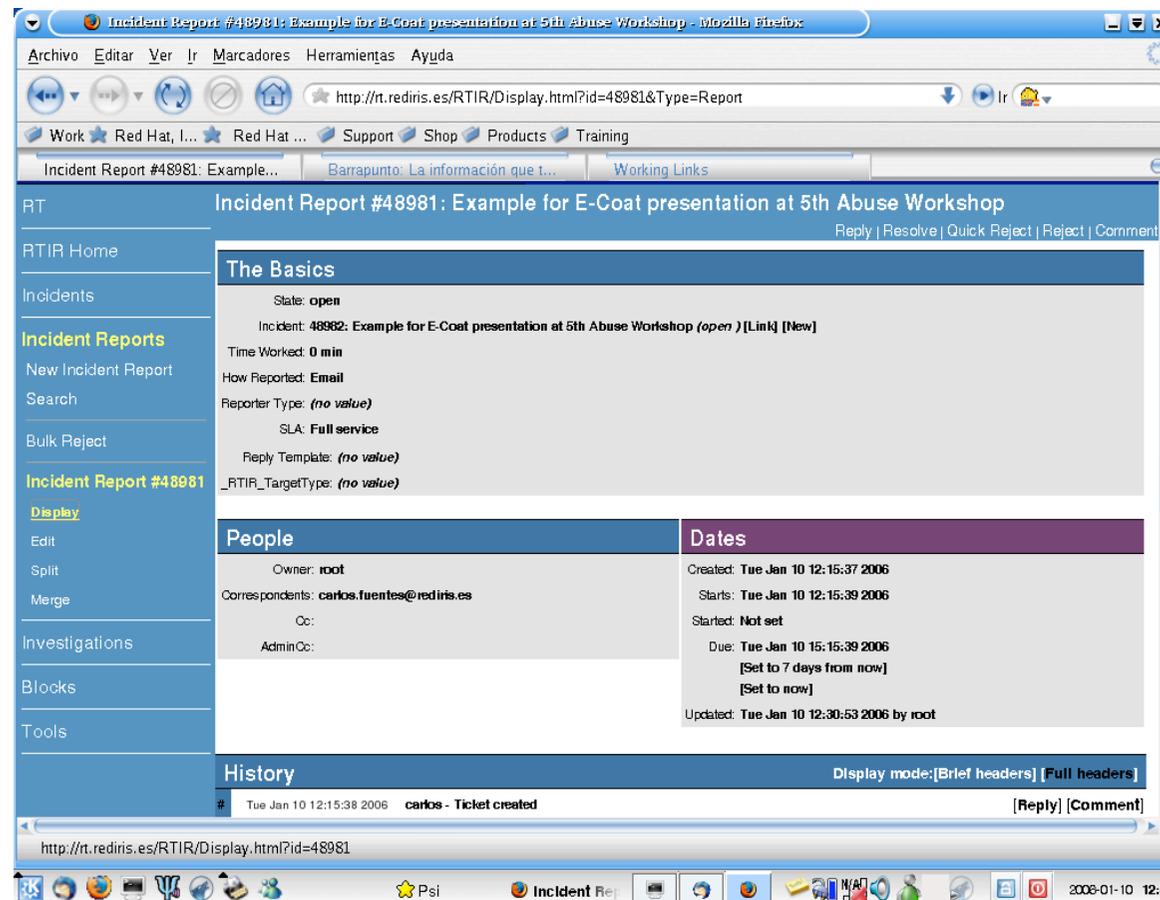
The screenshot shows the RTIR (Red Hat Incident Response) web interface. The browser window title is "RTIR (2 Nuevos Incident Reports) - Mozilla Firefox". The address bar shows "http://rt.rediris.es/RTIR/index.html". The page header includes the Red IRIS logo and navigation links like "Preferences", "About RTIR", and "Logout". The main content area is titled "RTIR for IRIS-CERT" and "RT for Incident Response (2 Nuevos Incident Reports)". It displays a table of incident reports with columns for "# Subject", "From", "Owner", and "Due".

# Subject	From	Owner	Due
48960 Ticket [TI#159692] Resuelto	cau@uam.es	Nobody	in 2 hours [Take]
48865 Security breaches from your network	david.adams@ultimateuptime.net	sergior	in 5 days [Steal]

Below this, there are sections for "Most due 1 incidents owned by root (and unowned)..." and "Most due 46 incidents...". The second table lists various incidents with their subjects, owners, priorities, and due dates.

# Subject	Owner	Priority	Due
46041 Re bichos project	paco	10	5 weeks ago [Steal]
43250 [gratisweb.com] URL de contenidos maliciosos	paco	10	4 weeks ago [Steal]
47361 [icac.es] posible router comprometido	paco	10	3 weeks ago [Steal]
48772 [upf.es] Portscan fr 193.145.36.38	cheb	10	3 hours ago [Steal]
48452 [csic.es] Escaneos desde 161.111.93.61	cheb	10	2 hours ago [Steal]
48245 [umh.es] Conexiones TCP 3000 desde 193.147.142.6	cheb	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	cheb	10	in 52 min [Steal]

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



The screenshot displays the RTIR (Red Hat Ticketing and Reporting Interface) web application. The browser window title is "Incident Report #48981: Example for E-Coat presentation at 5th Abuse Workshop - Mozilla Firefox". The address bar shows the URL: <http://rt.rediris.es/RTIR/Display.html?id=48981&Type=Report>. The page content is organized into a sidebar on the left and a main content area on the right.

Sidebar (Left):

- RT
- RTIR Home
- Incidents
- Incident Reports**
- New Incident Report
- Search
- Bulk Reject
- Incident Report #48981**
- Display
- Edit
- Split
- Merge
- Investigations
- Blocks
- Tools

Main Content Area (Right):

Incident Report #48981: Example for E-Coat presentation at 5th Abuse Workshop

Reply | Resolve | Quick Reject | Reject | Comment

The Basics

State: **open**

Incident: **48982: Example for E-Coat presentation at 5th Abuse Workshop (open)** [Link] [New]

Time Worked: **0 min**

How Reported: **Email**

Reporter Type: **(no value)**

SLA: **Full service**

Reply Template: **(no value)**

_RTIR_TargetType: **(no value)**

People	Dates
Owner: root	Created: Tue Jan 10 12:15:37 2006
Correspondents: carlos.fuentes@rediris.es	Starts: Tue Jan 10 12:15:39 2006
Cc:	Started: Not set
AdminCc:	Due: Tue Jan 10 15:15:39 2006
	[Set to 7 days from now]
	[Set to now]
	Updated: Tue Jan 10 12:30:53 2006 by root

History

Display mode: [Brief headers] [Full headers]

#	Time	User	Action
1	Tue Jan 10 12:15:38 2006	carlos	Ticket created

[Reply] [Comment]

<http://rt.rediris.es/RTIR/Display.html?id=48981>

- SfE-A finds a report with P2

RTIR for IRIS-CERT

RT: Lookup 130.206.1.130 using server whois.ripe.net

RTIR Home: **Current Report: #48981**

#	Subject	State	Last Updated	Created	Priority
48981	Example for E-Coat presentation at 5th Abuse Workshop	open	56 sec	22 hours	N/A

Requestor(s)	Owner	Last Contact	Due	Left
carlos.fuentes@rediris.es	root	56 sec	in 6 days	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]

Investigations: 130.206.1.130

(no Investigations)

Blocks: 130.206.1.130

(no Blocks)

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]

Look Up Information

WHOIS: 130.206.1.130 at whois.ripe.net

Using RTIR in our scenario (IV)



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

Look Up Information

WHOIS: 130.206.1.130 at whois.ripe.net Go

Traceroute to: 130.206.1.130 Go

WHOIS Results

```
% This is the RIPE Whois query server #1.
% The objects are in RPSL format.
%
% Note: the default output of the RIPE Whois server
% is changed. Your tools may need to be adjusted. See
% http://www.ripe.net/db/news/abuse-proposal-20050331.html (www.ripe.net)
% for more details.
%
% Rights restricted by copyright.
% See http://www.ripe.net/db/copyright.html (www.ripe.net)
%
% Note: This output has been filtered.
%       To receive output for a database update, use the "-B" flag.
%
% Information related to '130.206.0.0 - 130.206.255.255'
inetnum:      130.206.0.0 - 130.206.255.255
netname:      IRIS
descr:        RedIRIS
descr:        Spanish National R&D Network
descr:        Madrid, Spain
country:      ES
admin-c:      ER494-RIPE
tech-c:       IRIS1-RIPE
status:       ASSIGNED PI
mnt-irt:      IRT-IRIS-CERT
remarks:      mail spam reports: abuse@rediris.es (rediris.es)
```

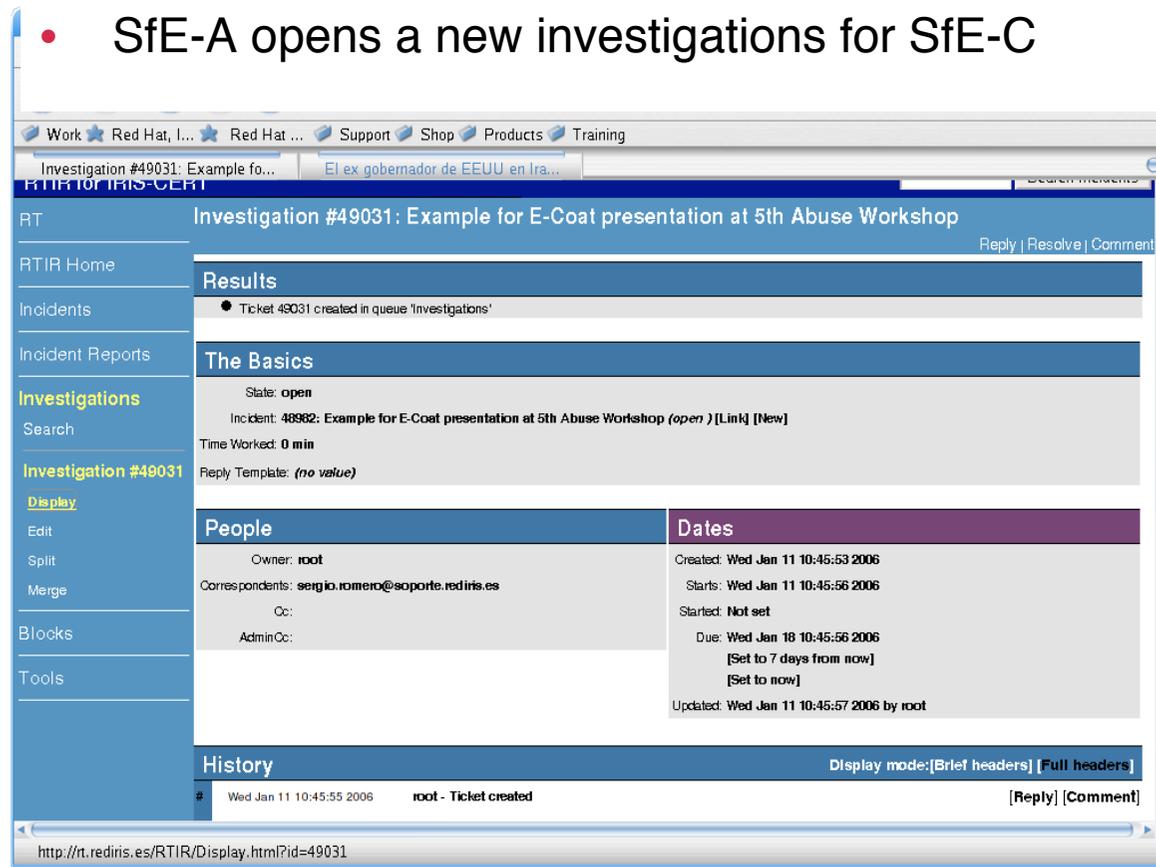
- A heads-up is sent to EGEE CSIRTs with P1 and P2

The screenshot shows a web browser window displaying the RTIR interface. The main content area shows the details for investigation #49031, titled "Example for E-Coat presentation at 5th Abuse Workshop". The interface includes a sidebar with navigation options like "RTIR Home", "Incidents", "Incident Reports", "Investigations", "Search", "Investigation #49031", "Display", "Edit", "Split", "Merge", "Blocks", and "Tools". The main content area is divided into sections: "Results" (Ticket 49031 created in queue 'Investigations'), "The Basics" (State: open, Incident: 48982: Example for E-Coat presentation at 5th Abuse Workshop (open) [Link] [New], Time Worked: 0 min, Reply Template: (no value)), "People" (Owner: root, Correspondents: sergio.romero@soporte.rediris.es, Cc:, AdminCc:), "Dates" (Created: Wed Jan 11 10:45:53 2006, Starts: Wed Jan 11 10:45:56 2006, Started: Not set, Due: Wed Jan 18 10:45:56 2006 [Set to 7 days from now] [Set to now], Updated: Wed Jan 11 10:45:57 2006 by root), and "History" (Wed Jan 11 10:45:55 2006 root - Ticket created). The browser address bar shows "http://rt.rediris.es/RTIR/Display.html?id=49031".

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

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

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

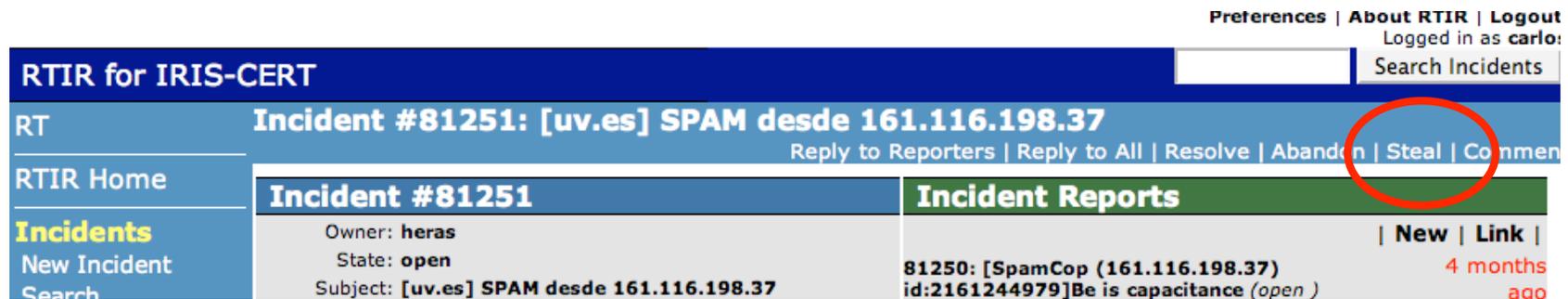


The screenshot displays the RTIR web interface for investigation #49031. The page title is "Investigation #49031: Example for E-Coat presentation at 5th Abuse Workshop". The interface includes a left sidebar with navigation options like "RTIR Home", "Incidents", "Incident Reports", "Investigations", "Search", "Investigation #49031", "Display", "Edit", "Split", "Merge", "Blocks", and "Tools". The main content area is divided into several sections: "Results" (Ticket 49031 created in queue 'Investigations'), "The Basics" (State: open, Incident: 48982: Example for E-Coat presentation at 5th Abuse Workshop (open) [Link] [New], Time Worked: 0 min, Reply Template: (no value)), "People" (Owner: root, Correspondents: sergio.romero@soporte.rediris.es, AdminCc:), "Dates" (Created: Wed Jan 11 10:45:53 2006, Starts: Wed Jan 11 10:45:56 2006, Started: Not set, Due: Wed Jan 18 10:45:56 2006 [Set to 7 days from now] [Set to now], Updated: Wed Jan 11 10:45:57 2006 by root), and "History" (Wed Jan 11 10:45:55 2006 root - Ticket created). The URL at the bottom is http://rt.rediris.es/RTIR/Display.html?id=49031.

- 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...



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



The screenshot shows the RTIR for IRIS-CERT interface. At the top right, there are links for 'Preferences', 'About RTIR', and 'Logout', along with the text 'Logged in as carlo:'. Below this is a search bar labeled 'Search Incidents'. The main header displays 'RT Incident #81251: [uv.es] SPAM desde 161.116.198.37'. A red circle highlights the 'Steal' button in the navigation bar. The left sidebar contains 'RTIR Home', 'Incidents', 'New Incident', and 'Search'. The main content area is divided into two columns: 'Incident #81251' and 'Incident Reports'. The 'Incident #81251' column shows 'Owner: heras', 'State: open', and 'Subject: [uv.es] SPAM desde 161.116.198.37'. The 'Incident Reports' column shows a report for '81250: [SpamCop (161.116.198.37) id:2161244979]Be is capacitance (open)' with a 'New | Link |' link and a timestamp of '4 months ago'.

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

Using RTIR in our scenario (IX)



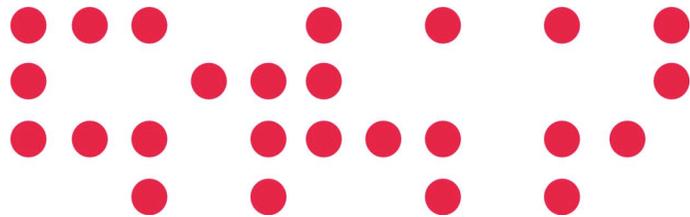
- Incident is contained and resolved
- SfE-F updates the "real-time status board" with all sensitive details (possibly private information), which is available to all involved sites (here: only SfE-C)
- SfE-F resolve the ticket

The screenshot displays the RTIR (Real-time Incident Reporting) interface for incident #91770. The interface is divided into several sections:

- RTIR Home:** Shows the incident title: "Incident #91770: [cesga.es] GGUS-Ticket-ID: #23376 TICKET SUBMITTED - Security Service Challenge (SSC_2) for SouthWesternEurope/cesga".
- Incident #91770:** A detailed view of the incident with fields for Owner (carlos), State (open), Subject, Description, Priority (10), Time Worked (0 min), Constituency (RedIRIS), and Function (IncidentCoord). It also shows the classification as "Sondeo/Probe".
- Investigations:** A table listing investigation entries. One entry is visible: "91779: [cesga.es] GGUS-Ticket-ID: #23376 TICKET SUBMITTED - Security (open)" with a status of "21 hours (no Blocks)" and "ago".
- Dates:** A section showing the incident's timeline: Created: Thu Jun 14 16:35:54 2007, Starts: Thu Jun 14 16:35:56 2007, Updated: Thu Jun 14 16:36:12 2007 by sergior.
- History:** A log of actions taken on the ticket. Key entries include: "Thu Jun 14 16:35:55 2007 sergior - Ticket created", "Thu Jun 14 16:35:56 2007 RT_System - Starts changed from Not set to Thu Jun 14 16:35:56 2007", and "Thu Jun 14 16:35:56 2007 RT_System - State open added".



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



- 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

¿¿¿Questions???



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