

Request Tracker for Incident Response

Carlos Fuentes IRIS-CERT/RedIRIS

What RT is

- RT is a ticketing system
- Help keep you organized
- Issue tracking
 - Trouble ticketing
 - Workflow
 - Helpdesk
 - Customer Service
 - Process management
 - Bug Tracking

What RTIR is



- RT for Incident Response
- Ticketing system
- Designed for CERT/CSIRT teams
- Originally designed for JANET-CERT
- Generalized for a “standard” process
 - TF-CSIRT RTIR Working Group

Designed for CSIRT Teams



- Metadata
- Workflows
- Views
- Plugins

- RTIR is RT

... with more features, a custom interface and special configuration

What RTIR does



- Keeps track of incidents
- Keeps track of correspondence
- Keeps an uneditable history
- Makes incident research easier
- Tracks your SLA commitments
- Integrates with your other systems
- Takes care of the 'boring' parts of Incidents Response

The RTIR Workflow

RTIR for rediris.es Logged in as root | Preferences | Logout

RT for Incident Response New ticket in Blocks Search Incidents

- RT
- RTFM
- RTIR Home**
- Search
- Incidents
- Incident Reports
- Investigations
- Blocks
- Tools

New unlinked Incident Reports... Bulk Reject

Most due incidents owned by root

#	Subject	Owner	Priority	Due	New messages
2	Problem with RENATER	root	Medium	7 days	No


Most due unowned incidents

Most due incidents

#	Subject	Owner	Priority	Due	New messages
2	Problem with RENATER	root	Medium	7 days	No

Refresh Edit

Don't refresh this page.

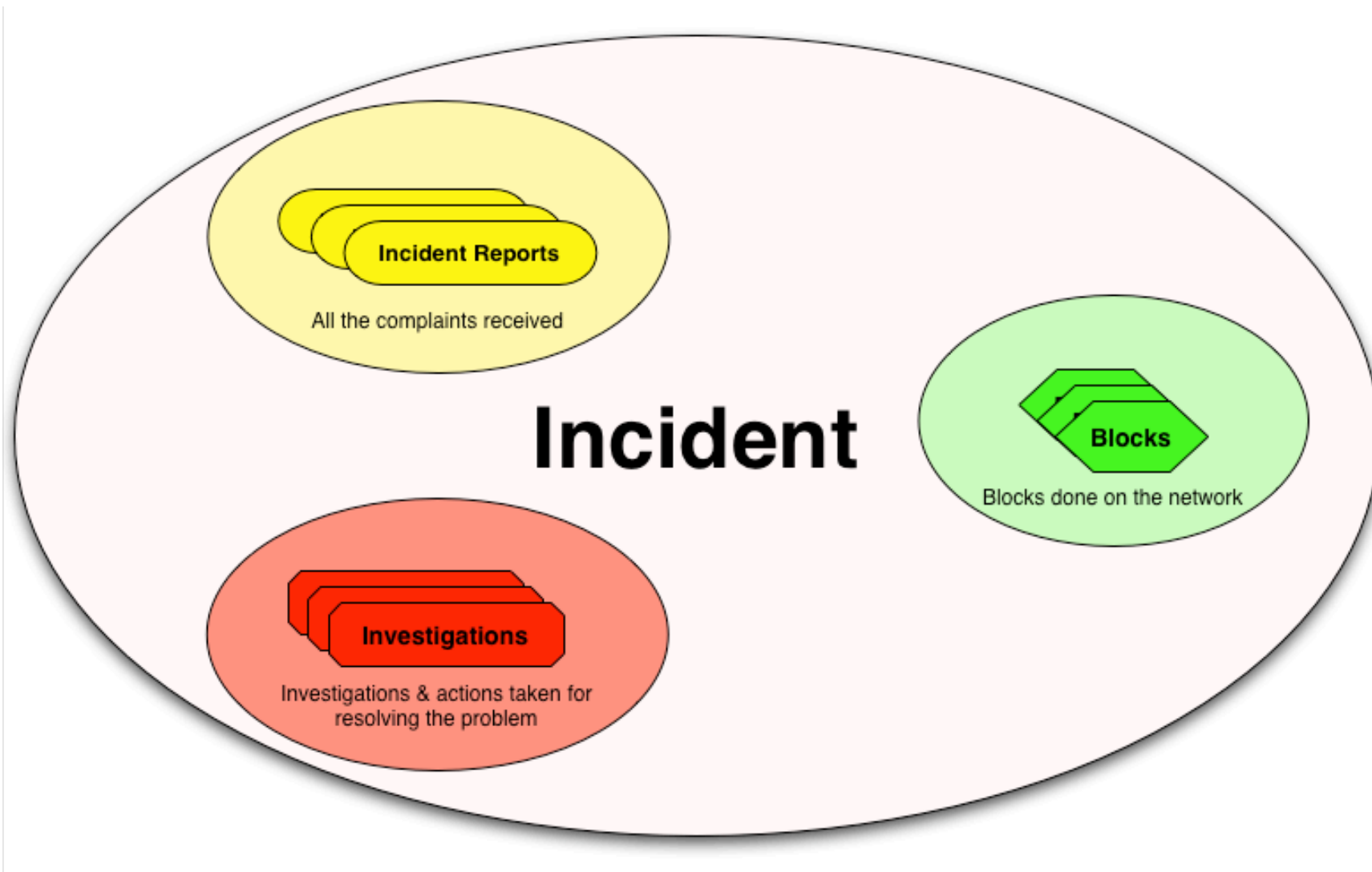


»« RT 3.8.7 Copyright 1996-2009 Best Practical Solutions, LLC.

The Concept

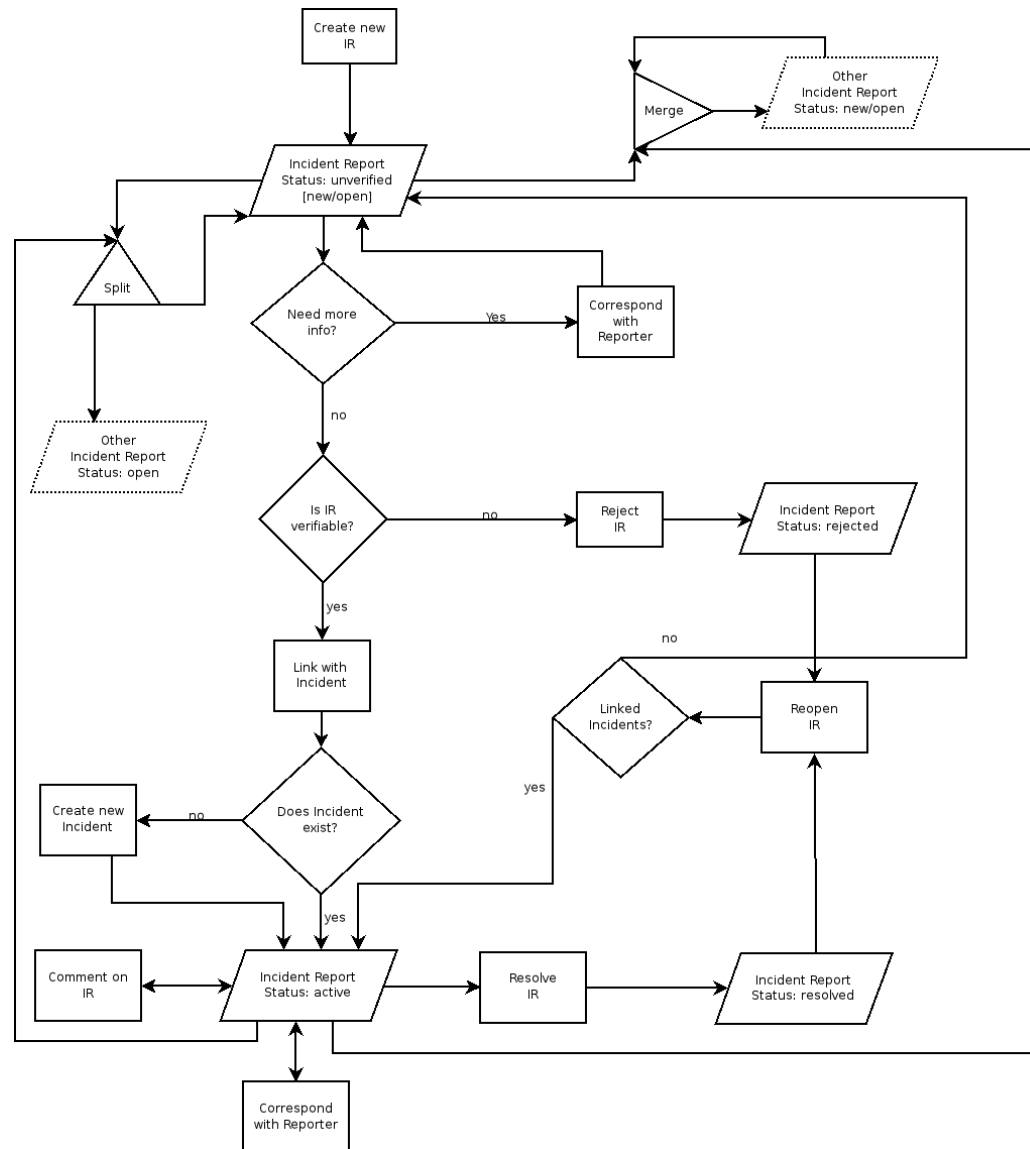


- Incidents tie everything together
- One Incident for
 - Many Incident Reports
 - Someone has a complaint of our constituency
 - Many Investigations
 - IRT attempts to get the root of the problem
 - Many Blocks
 - Track network level intervention against threat

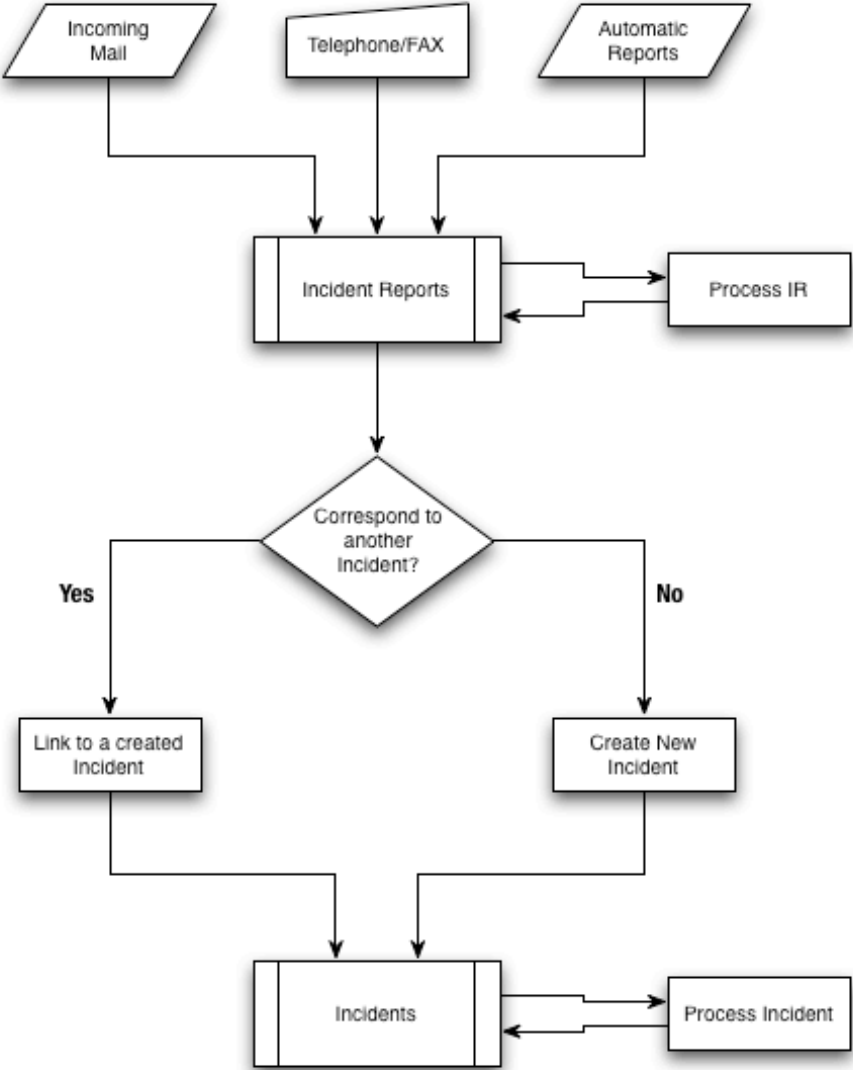


- It usually starts with a Incident Report
 - Conversations with complainers
 - Something bad happened
 - Please help me
 - Related to our constituency
 - Coming from
 - Mail
 - Telephone
 - FAX
 - Internal/External Automatic Detection System

Incident Reports LifeCycle



Incident Reports Workflow



Create an IR

Create a new Incident Report

Incident:

Owner:

Subject:

Time Worked: Time Left:

Correspondents: Don't send any emails to correspondents.

Cc: (Sends a carbon-copy of this update to a comma-delimited list of email addresses. These people **will** receive future updates.)

Admin Cc: (Sends a carbon-copy of this update to a comma-delimited list of administrative email addresses. These people **will** receive future updates.)

Constituency:

SLA:

Customer:

How Reported:

Reporter Type:

Create an IR #2

IP address:

Age
Select one value

- (no value)
- Active
- Finished
- Dead
- Extinct

Attach file:

Search for RTFM articles matching

Include RTFM article:

Message:

Starts:

Due:

Incident Report #6:

New ticket in

Blocks

Search Incidents

Display · Edit · Split · Merge · Advanced

Reply · Resolve · Quick Resolve · Reject · Quick Reject · Comment · Lock · ☆ · Extract Article

Results

- Ticket 6 created in queue 'Incident Reports'

The Basics

State: new
Incident: *(no Incidents)* [Link] [New]
Constituency: EDUNET
Time Worked: 0 min
SLA: Full service
Customer: no value
How Reported: Telephone
Reporter Type: external individual

IP Address:

- 10.0.0.1
- 10.1.11.2

Age: *(no value)*

People

Owner: Enoch Root
Correspondents: customer@customer.example.com
Cc:
AdminCc: Group: DutyTeam EDUNET

Dates

Created: Mon Feb 08 16:05:40 2010
Starts: Mon Feb 08 16:05:42 2010
Started: Not set
Due: Mon Feb 08 17:05:41 2010 [Set to 7 days from now]
Updated: Mon Feb 08 16:05:42 2010 by root

Articles

| New | Link |

History Brief headers — Full headers

Mon Feb 08 16:05:40 2010 **Enoch Root - Ticket created** Reply Comment Forward

Customer reports that he woke up this morning to find that his server was sending lots of spam Download (untitled) / with headers
text/html 100b

Mon Feb 08 16:05:41 2010 **The RT System itself - Outgoing email recorded** Show

Mon Feb 08 16:05:41 2010 **The RT System itself - AdminCc DutyTeam EDUNET added**

Mon Feb 08 16:05:41 2010 **The RT System itself - Due changed from Not set to Mon Feb 08 17:05:41 2010**

Mon Feb 08 16:05:42 2010 **The RT System itself - State new added**

Mon Feb 08 16:05:42 2010 **The RT System itself - Starts changed from Not set to Mon Feb 08 16:05:42 2010**

Incident Report Reply

State: new

Update Type:

Owner: Worked: minutes

Subject:

One-time Cc:

One-time Bcc:

Attach file:

Message: Search for RTFM articles matching

Include RTFM article:

Dearest Customer,

We're looking into your issue today. Expect to hear from us this evening.

Incident Report History

History Brief headers — Full headers

Mon Feb 08 16:05:40 2010 **Enoch Root - Ticket created** Reply Comment Forward

Customer reports that he woke up this morning to find that his server was sending lots of spam Download (untitled) / with headers
text/html 100b

Mon Feb 08 16:05:41 2010 **The RT System itself - Outgoing email recorded** Show

Mon Feb 08 16:05:41 2010 **The RT System itself - AdminCc DutyTeam EDUNET added**

Mon Feb 08 16:05:41 2010 **The RT System itself - Due changed from Not set to Mon Feb 08 17:05:41 2010**

Mon Feb 08 16:05:42 2010 **The RT System itself - State new added**

Mon Feb 08 16:05:42 2010 **The RT System itself - Starts changed from Not set to Mon Feb 08 16:05:42 2010**

Mon Feb 08 16:08:58 2010 **Enoch Root - Correspondence added** Reply Comment Forward

Dearest Customer,

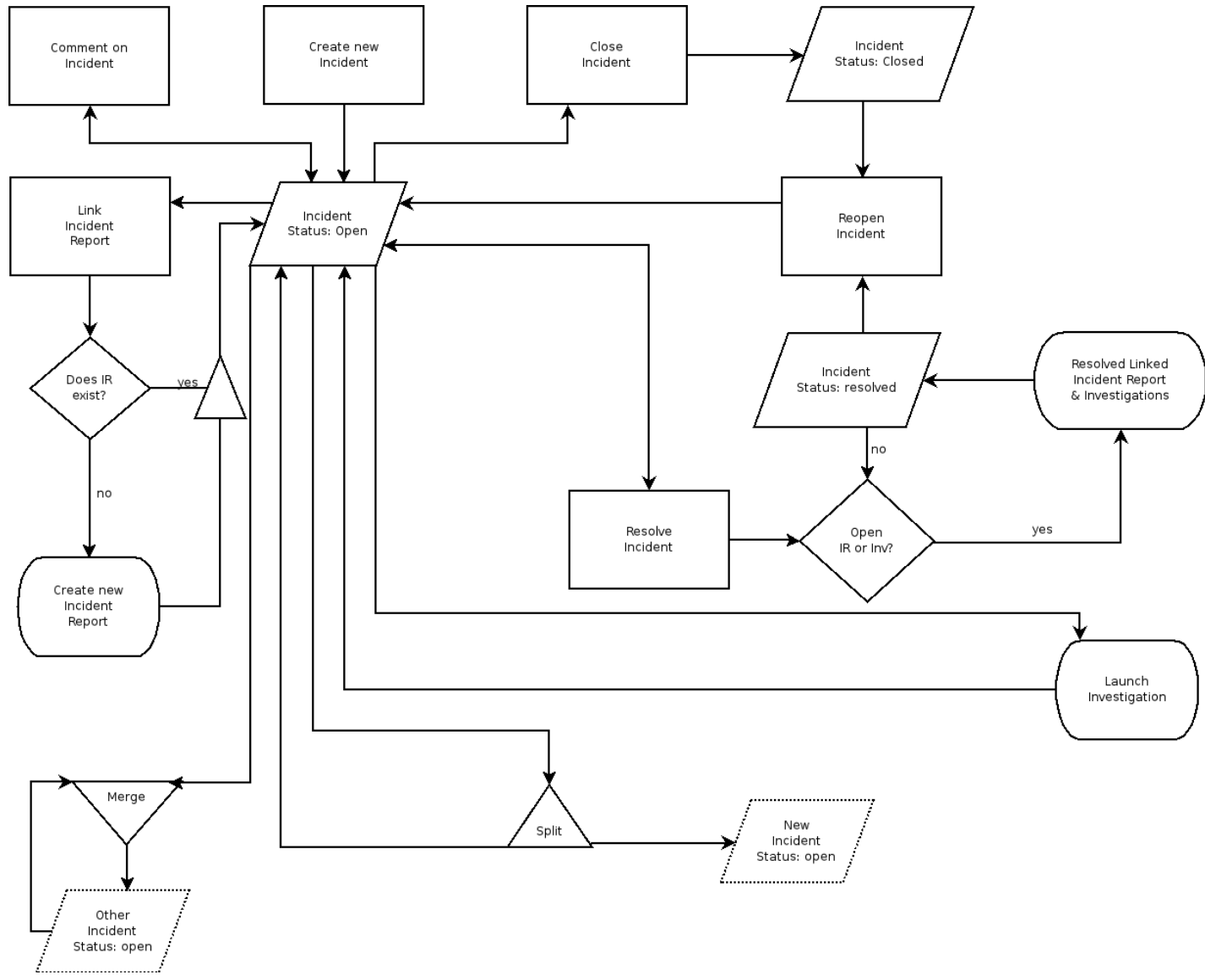
We're looking into your issue today. Expect to hear from us this evening. Download (untitled) / with headers
text/html 117b

Mon Feb 08 16:08:59 2010 **The RT System itself - Due changed from Mon Feb 08 17:05:41 2010 to Mon Feb 08 16:08:59 2010**

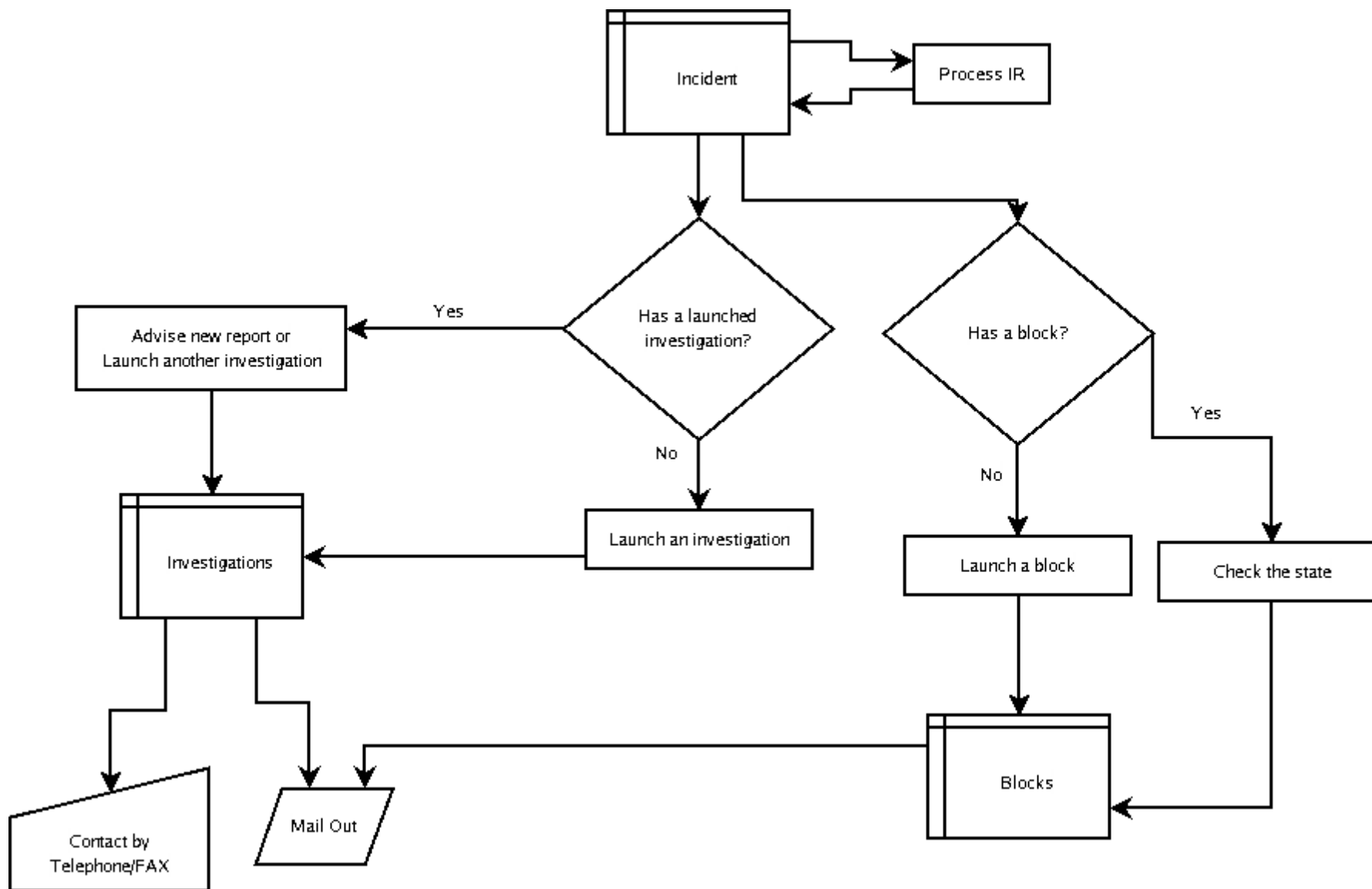
Mon Feb 08 16:09:00 2010 **The RT System itself - Outgoing email recorded** Show

- Once reported, the team tracks an Incident
 - Tracking what actually happened
 - Private / Internal
 - Tie everything together

Incident Lifecycle



Incident Workflow



Create an Incident

Create a new Incident

New ticket in Blocks Search Incidents

[New Incident](#) · [Results](#) · [Refine](#) · [Report](#) · [Bulk Abandon](#)

You have locked Ticket #6.

Create a new Incident

Link with: Report #6:
Owner: Enoch Root

Subject:

Description:

Constituency: EDUNET

Function: (no value)

Classification: (no value)

Resolution: (no value)

IP:
10.0.0.1
10.1.11.2

Age
Select one value
(no value)
Active
Finished
Dead
Extinct

Attach file:

Message:
Customer reports that he woke up this morning to find that his server was sending lots of spam
Dearest Customer,
We're looking into your issue today. Expect to hear from us this evening.

Incident Details

Incident #8: Spammers are attacking customer machines

New ticket in | Blocks | Search Incidents

Display · Edit · Split · Merge · Advanced

Reply to Reporters · Reply to All · Resolve · Quick Resolve · Abandon · Comment · Lock · ☆ · Extract Article

Results

- Ticket 8 created in queue 'Incidents'

Incident #8

Owner: Enoch Root
State: open
Subject: Spammers are attacking customer machines
Description: no value
Priority: Low/None
Time Worked: 0 min
Constituency: EDUNET
Function: IncidentCoord
Classification: Spam
Resolution: no value

IP Address:

- 10.0.0.1
- 10.1.11.2

Age: (no value)

Incident Reports

| New | Link |

6 Someone broke into our server!!!!	open	7 days
-------------------------------------	------	--------

(No inactive Incident Reports)

Investigations

Blocks

Incident Details #2

Incident #8

Owner: Enoch Root
State: open
Subject: Spammers are attacking customer machines
Description: no value
Priority: Low/None
Time Worked: 0 min
Constituency: EDUNET
Function: IncidentCoord
Classification: Spam
Resolution: no value

IP Address:

- 10.0.0.1
- 10.1.11.2

Age: (no value)

Incident Reports | [New](#) | [Link](#) |

6	Someone broke into out server!!!!	open	7 days
---	-----------------------------------	------	--------

(No inactive Incident Reports)

Investigations | [Launch](#) | [Link](#) |

(No active Investigations)
(No inactive Investigations)

Blocks | [New](#) | [Link](#) |

(No active Blocks)
(No inactive Blocks)

Dates

Created: Mon Feb 08 16:29:05 2010
Starts: Mon Feb 08 16:29:07 2010
Due: Mon Feb 15 16:25:37 2010
Updated: Mon Feb 08 16:29:07 2010 by root

Articles | [New](#) | [Link](#) |

Incident History

History Brief headers — Full headers

- # Mon Feb 08 16:29:06 2010 **The RT System itself - Due changed from Not set to Mon Feb 15 16:25:37 2010**
- # Mon Feb 08 16:29:06 2010 **Enoch Root - Ticket created** Reply Comment Forward
Subject: Spammers are attacking customer machines

Attacker is compromising customer servers. Need to track them down and turn them over to the relevant authority

Download (untitled) / with headers
text/html 117b
- # Mon Feb 08 16:29:07 2010 **The RT System itself - AdminCc DutyTeam EDUNET added**
- # Mon Feb 08 16:29:07 2010 **The RT System itself - State open added**
- # Mon Feb 08 16:29:07 2010 **The RT System itself - Starts changed from Not set to Mon Feb 08 16:29:07 2010**

Incident → Investigation

Launch a new Investigation

Incident: 8
Owner: Enoch Root
Subject: Spammers are attacking customer machines
Time Worked: Time Left:
Correspondents: Don't send any emails to correspondents.
Cc: (Sends a carbon-copy of this update to a comma-delimited list of email addresses. These people will receive future updates.)
Admin Cc: (Sends a carbon-copy of this update to a comma-delimited list of administrative email addresses. These people will receive future updates.)
Constituency: EDUNET
GOVNET
Customer: (no value)
IP address: 10.0.0.1
10.1.11.2
Age: (no value)
Active
Finished
Dead
Extinct
Select one value
Attach file:

Attach Reports

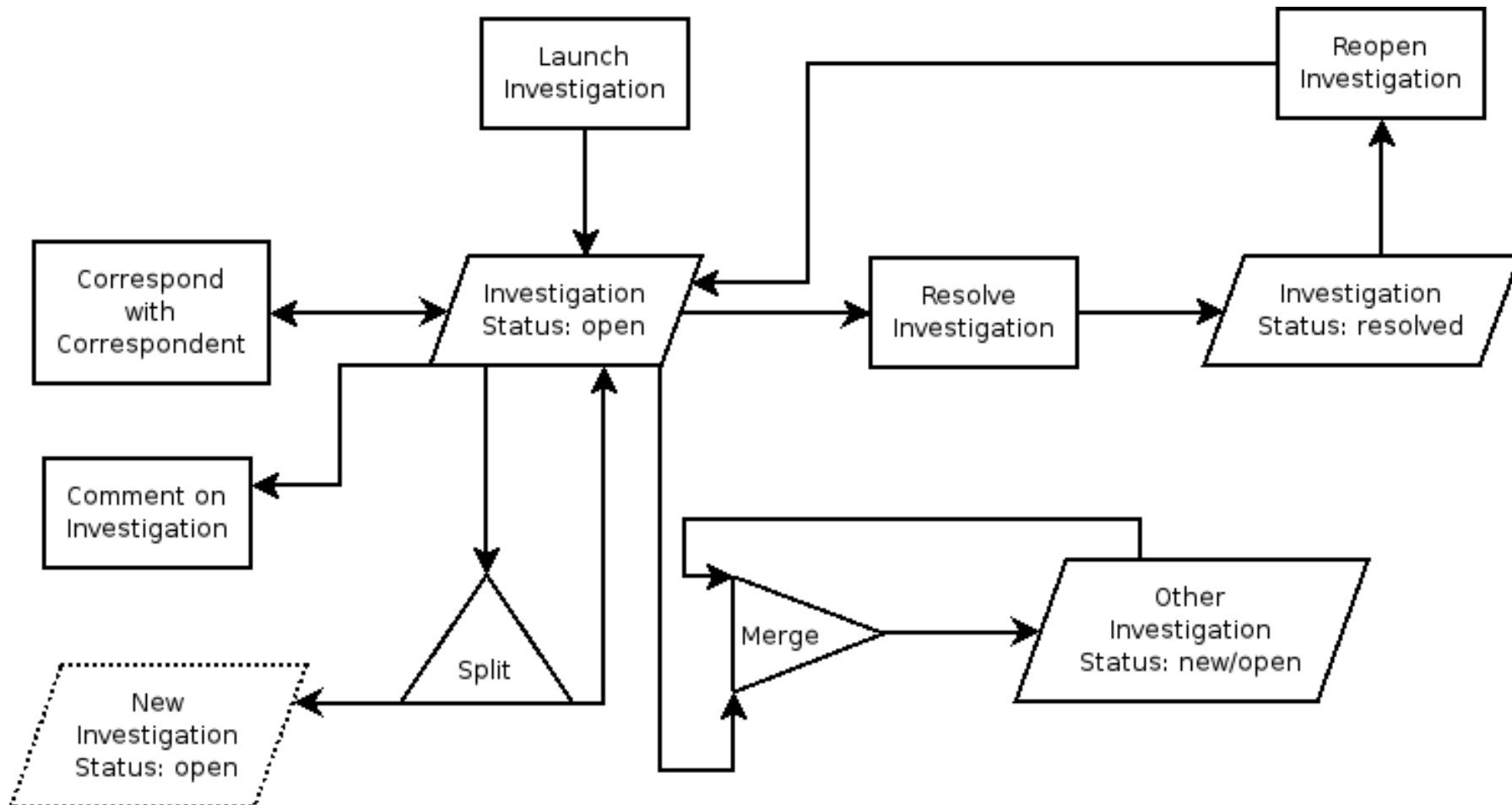
#	Subject	State	Last Updated	Created
6	Someone broke into our server!!!!	open	5 min ago	28 min ago

Search for RTFM articles matching
Include RTFM article:

Message:
On Mon Feb 08 16:29:06 2010, root wrote:
> Attacker is compromising customer servers. Need to track them down and turn
> them over to the relevant authority

- The teams starts an Investigation
 - Internal Research and Discovery
 - Conversations with external partners
 - Law Enforcements
 - Network Providers
 - Experts
 - Other CSIRTs
 - Everyone who acts for resolving the issue

Investigation Lifecycle



Launch Investigation



Launch a new Investigation New ticket in Blocks Search Incidents

Display · Edit · Split · Merge · Advanced · **Create linked Investigation**

Reply to Reporters · Reply to All · Resolve · Quick Resolve · Abandon · Comment · Lock · ☆ · Extract Article

Launch a new Investigation

Incident: 8

Owner:

Subject:

Time Worked: Time Left:

Correspondents: Don't send any emails to correspondents.

Cc: (Sends a carbon-copy of this update to a comma-delimited list of email addresses. These people **will** receive future updates.)

Admin Cc: (Sends a carbon-copy of this update to a comma-delimited list of administrative email addresses. These people **will** receive future updates.)

Constituency:

Customer:

IP address:

Age Select one value:

Launch Investigation

Attach Reports

<input type="checkbox"/>	#	Subject	State	Last Updated	Created
<input type="checkbox"/>	6	Someone broke into out server!!!!	open	5 min ago	28 min ago

Search for RTFM articles matching

Include RTFM article: **Go**

Message:

Jim,
Can you help us track down netflow data for the customer's issue. He says he first started seeing weird behaviour at about 4.10am
Thanks!!!

Dates

Starts:

Due:

Investigations Details

Investigation #9: Track down netflow data of attack on customer server

[New ticket in](#) [Blocks](#) [Search Incidents](#)

[Display](#) · [Edit](#) · [Split](#) · [Merge](#) · [Advanced](#)

[Reply](#) · [Resolve](#) · [Quick Resolve](#) · [Comment](#) · [Lock](#) · [☆](#) · [Extract Article](#)

Results

- Ticket 9 created in queue 'Investigations'

The Basics

State: open

Incident:

- 8: Spammers are attacking customer machines (*open*) [Unlink]

[\[Link\]](#) [\[New\]](#)

Constituency: EDUNET

Time Worked: 0 min

Customer: no value

IP Address:

- 10.0.0.1
- 10.1.11.2

Age: (no value)

Articles

[New](#) | [Link](#) |

People

Owner: Enoch Root

Correspondents: sec-institution@isp.example.com

Cc:

AdminCc: Group: DutyTeam EDUNET

Dates

Created: Mon Feb 08 16:37:48 2010

Starts: Mon Feb 08 16:37:49 2010

Started: Mon Feb 08 16:37:48 2010

Due: Mon Feb 15 16:37:49 2010 [Set to 7 days from now]

Updated: Mon Feb 08 16:37:49 2010 by root

Investigations History

History Brief headers — Full headers

Mon Feb 08 16:37:48 2010 **Enoch Root - Ticket created** Reply Comment Forward
Subject: Track down netflow data of attack on customer server

Jim,

Can you help us track down netflow data for the customer's issue. He says he first started seeing weird behaviour at about 4.10am

Thanks!!!

Download (untitled) / with headers
text/html 183b

Mon Feb 08 16:37:49 2010 **The RT System itself - Outgoing email recorded** Show

Mon Feb 08 16:37:49 2010 **The RT System itself - AdminCc DutyTeam EDUNET added**

Mon Feb 08 16:37:49 2010 **The RT System itself - Due changed from Not set to Mon Feb 15 16:37:49 2010**

Mon Feb 08 16:37:49 2010 **The RT System itself - State open added**

Mon Feb 08 16:37:49 2010 **The RT System itself - Starts changed from Not set to Mon Feb 08 16:37:49 2010**

Data Detectors

History Brief headers — Full headers

Mon Feb 08 16:48:11 2010 **Enoch Root - Ticket created** Reply Comment Forward

Subject: under attack!!!

help! I'm being attacked by 127.0.0.1 [lookup IP][Add IP] Download (untitled) / with headers
text/html 130b

And my server keeps trying to connect to a.gtld-servers.net [lookup host]

Incident Report #11: under attack!!!

Display · Edit · Split · Merge · Advanced

The Basics

State: new

Incident: *(no Incidents)* [Link] [New]

Constituency: EDUNET

Time Worked: 0 min

SLA: Full service

Customer: Spanish Customer

How Reported: Telephone

Reporter Type: customer

IP Address: 127.0.0.1

Age: *(no value)*

Data Detectors

History Brief headers — Full headers

Mon Feb 08 16:48:11 2010 **Enoch Root - Ticket created** Reply Comment Forward

Subject: under attack!!!

help! I'm being attacked by 127.0.0.1 [lookup IP][Add IP] Download (untitled) / with headers
text/html 130b

And my server keeps trying to connect to a.gtld-servers.net [lookup host]

Lookup '127.0.0.1' using server localhost

[New ticket in](#)Blocks [Search Incidents](#)

Lookup · Reporting · Scripted Action

Current Report: #11

#	Subject Requestors	State Owner	Last Updated Told	Created Due	Time Left
11	under attack!!! sec-institution@isp.example.com	new root	2 min ago	5 min ago 55 min	

Incidents: 127.0.0.1

id	Subject	State	Priority	Actions
<i>(no incidents)</i>				
[New] [Refine Search]				

Investigations: 127.0.0.1

id	Subject	State	Priority	Actions
<i>(no Investigations)</i>				
[Refine Search]				

Incident Reports: 127.0.0.1

id	Subject	State	Priority	Actions
11	under attack!!!	new	0	
[Refine Search]				

Blocks: 127.0.0.1

id	Subject	State	Priority	Actions
<i>(no Blocks)</i>				
[Refine Search]				

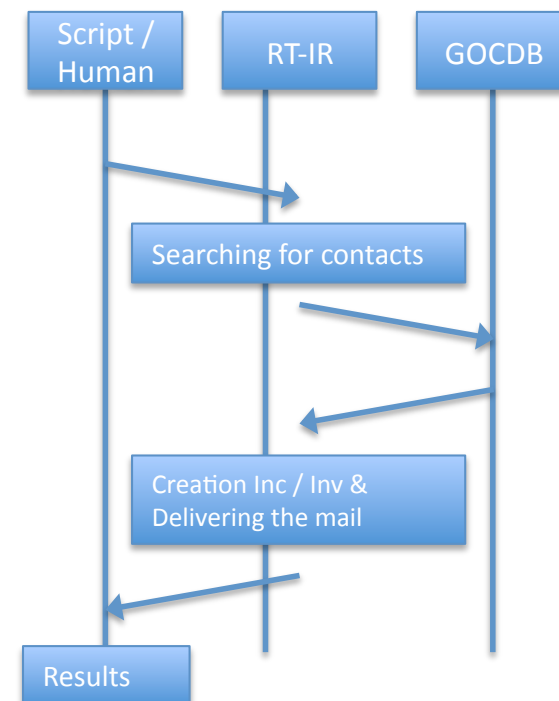
Look Up Information

WHOIS: at Traceroute to:

WHOIS Results

SSC & RT-IR Integration

- New features developed:
 - Integration with GOCDB
 - Customer CF's values: List of the sites
 - Incident Report & Investigations
 - Web Service for Investigation Creation
 - Allows us to launch an investigation for a site
 - Using a predefined RTFM template
 - Deliver to Site Security Officer and NGI Security officer
 - Params required:
 - Exact name of the site
 - Template ID



- Update SSC DB Script Action
 - Allows us to store the answers from site in the SSC DB

Using RTIR

- Cost of RTIR: \$0
- Cost of required software: \$0
- Cost of required hardware: ???
- Operating System
 - Unix/Linux FreeBSD/MacOS X/Solaris/etc ...
- Database
 - MySQL 4.1 or 5.0, PostgreSQL 8.x, Oracle 9.x or 10.x, SQLite (for testing)
- Web Server
 - Apache, lighthttpd, Standalone pure-perl server

- <http://bestpractical.com/rtir>
- <ftp://ftp.rediris.es/rediris/cert/rtir/CentOSRTIR.tgz>
 - Vmware image for testing
 - Provided by RedIRIS

- <http://wiki.bestpractical.com> - <http://www.rtir.org>
- rtir-subscribe@list.bestpractical.com
- rt-users-subscribe@list.bestpractical.com
- rt-devel-subscribe@list.bestpractical.com

Spanish Research & Academic Network



red.es



red.es