

RT and RT for Incident Response

Carlos Fuentes Bermejo

RTIR WG - Primary Technical Contact

RedIRIS IRIS-CERT - Security Specialist

Si habla español

Couldn't be here today :(

Jesse Vincent

Designed RT and RTIR

(It's all my fault)

Founded Best Practical

(It's even more my fault)

No puedo presentar en español. Lo Siento.

WARNING

I represent a
software vendor

We sell support,
training, consulting and
customization for RT,
RTIR and RTFM

This talk could be
dangerously close to a
sales pitch.

I'm not a sales guy

All the software we
make is open source.

We helped create RTIR
to let CERT teams be
more effective.

I want you to use RTIR
for free - forever.

I will be *happy* if you
use it for free.

(Now do you believe
that I'm not a sales guy?)

About RT

RT is a Ticketing System

*RT helps keep you
organized.*

Every conversation gets
a number, a status and
an owner.

*RT helps keep your
customers happy.*

RT sends an autoreply and ticket number when they report a problem.

*RT helps keep your team
from going crazy.*

You know what's been
done, and when.

*RT helps you show your
bosses how hard you work.*

It's easy to run reports
on all kinds of metrics.

*RT builds an ad-hoc
knowledge base.*

(With RTFM, you can
build an explicit
Knowledge Base)

Some RT history...

Created in 1996

First public release in 1997

2.0 released in 1999

Best Practical formed in 2001

RTIR Created in 2003

RTIR WG Started in 2005

RTIR 2.4 Released 2008 (*Last week!*)

What is RT useful for?

Issue Tracking

Trouble Ticketing

Workflow

Helpdesk

Customer Service

Process Management

Bug Tracking

RT Homepage

RT for example.com Logged in as root | Preferences | Logout

Home

- Simple Search
- Tickets
- RTFM
- RTIR
- Tools
- Configuration
- Preferences
- Approval

RT at a glance New ticket in Blocks Search

10 highest priority tickets I own Edit

#	Subject	Priority	Queue	Status
2	Please deploy new logging server	0	General	new

10 newest unowned tickets Edit

#	Subject	Queue	Status	Created	
1	This is a regular RT ticket	General	new	6 min ago	Take

Bookmarked Tickets Edit

Quick ticket creation

Subject:

Queue: Blocks Owner: root

Content:

Create

Reminders Edit

Quick search Edit

Queue	new	open	stalled
General	2	0	0

Dashboards Edit

Refresh

Don't refresh this page. ▾

Go!

Ticket Details

#2: Please deploy new logging server New ticket in Blocks Search

Display · History · Basics · Dates · People · Links · Reminders · Jumbo

Open · Take ... Comment · Reply · Resolve · ☆ · Extract Article

Ticket metadata

The Basics

Id: 2
 Status: new
 Priority: 0/0
 Queue: General

Reminders

New reminder:
 Subject:
 Owner: Enoch Root
 Due: Calendar
Save

People

Owner: Nobody
 Requestors: jesse@bestpractical.com
 Cc: boss@bestpractical.com
 AdminCc:

Dates

Created: Sun Sep 21 16:53:50 2008
 Starts: Not set
 Started: Not set
 Last Contact: Not set
 Due: Not set
 Closed: Not set
 Updated: Sun Sep 21 16:53:51 2008 by root

Links

Depends on: (Create)
 Depended on by: (Create)

Graph

More about jesse@bestpractical.com

Comments about this user:
Autocreated when added as a watcher
 This user's 10 highest priority tickets:

- 2: Please deploy new logging server (new)

Groups this user belongs to:

- Everyone

Ticket History

[Open](#) · [Take ...](#) · [Comment](#) · [Reply](#) · [Resolve](#) · [☆](#) · [Extract Article](#)

^
Brief headers — Full headers

Sun Sep 21 16:53:50 2008 **root - Ticket created**

CC: boss@bestpractical.com

Subject: Please deploy new logging server

We need that new logging server up this week. Please drop everything and head to the data center.

Thanks!

[Reply](#) [Comment](#) [Forward](#)

[Download \(untitled\) / with headers](#)
text/plain 106b

Sun Sep 21 16:53:51 2008 **RT_System - Outgoing email recorded**

[Show](#)

Ticket Update

Update ticket #2 (Please deploy new logging) New ticket in Blocks Search

Display · History · Basics · Dates · People · Links · Reminders · Jumbo

Open · Take ... Comment · Reply · Resolve · ☆ · Extract Article

Status: Owner: Worked:

Update Type:

Subject:

One-time Cc:

One-time Bcc:

Attach:

Sign using Queue's key Encrypt

Message:

Include RTFM article:

▼
Headed out now

Ticket History

Ticket History # 2 Please deploy new logging New ticket in Blocks Search

Display · **History** · Basics · Dates · People · Links · Reminders · Jumbo

Open · Take ... · Comment · Reply · Resolve · ☆ · Extract Article

History Brief headers — Full headers

Sun Sep 21 16:53:50 2008 **root - Ticket created** Reply Comment Forward
CC: boss@bestpractical.com
Subject: Please deploy new logging server

We need that new logging server up this week. Please drop everything and head to the data center.

Thanks!

Download (untitled) / with headers
text/plain 106b

Sun Sep 21 16:53:51 2008 **RT_System - Outgoing email recorded** Show

RT Core Concepts

Tickets

Queues

Custom Fields

Scripts

Access Control

Email Gateway

Internationalization

Tickets

Track issues

Have unique id #s

Keep a history of correspondence

Have one owner

(And a bunch of other metadata)

Queues

High-level grouping of tickets

Each can have its own

- Access Control

- Business Logic (Scripts)

- Custom Fields

Custom Fields

Track your own ticket metadata

Freeform (optional validation)

Select (one or many)

Text block

Upload files or images

Custom data sources

Per-field access control

Scripts

Custom business logic

(Also how RT sends mail)

Each is built from

Condition

Action

Template

Access Control

User, Group or Role based
Global and Per-queue rights

Email Gateway

RT was first made to replace a mailing list

RT is designed for email interaction

(and web. and command line)

RT mediates and tracks all discussions

Internationalization

Fully native UTF8 internally

Speaks 22 languages

Handles inbound and outbound email
encoding

Contribute at

<https://translations.launchpad.net/rt/>

More RT Features

Charts and Reports

Dashboards

Self-service interface

Feeds

RTFM

PGP Support

Themability

Ticket Aging

Ticket Locking

Web API

Perl API

CLI tools

Customizability

The Community

Where to get RT

<http://bestpractical.com/rt>

Questions about RT?

(Next up: RTIR)

RTIR

RT for Incident Response

What is RTIR?

Ticketing System

RT for Incident Response

Designed for CERT/CSIRT Teams

Designed for *a* CERT team - JANET-CERT

Generalized for a 'standard' process

Differences from RT

RTIR *is* RT

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

Designed for CERT/CSIRT Teams

Metadata

Workflows

Views

Plugins

*We designed RTIR to help you
get your job done.*

RTIR keeps track of
incidents.

RTIR keeps track of
correspondence.

RTIR keeps an
uneditable history.

RTIR makes incident
research easier.

RTIR tracks your
SLA commitments.

RTIR integrates with
your other systems.

RTIR takes care of the
‘boring’ parts of
Incident Response.

The RTIR Workflow

RTIR Homepage

RTIR for example.com Logged in as root | Preferences | About RTIR | Logout

RT for Incident Response New ticket in Blocks Search In

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

[Edit](#)

New unlinked Incident Reports...

#	Subject	Requestors	Owner	Due	Take
7	Someone sent me spam!		root	18 hours	

[Bulk Reject]

Most due incidents owned by root

#	Subject	Owner	Priority	Due	New messages
4	Spammers are attacking customer machines	root	50	16 hours	No

Most due unowned incidents

Most due incidents

#	Subject	Owner	Priority	Due	New messages
4	Spammers are attacking customer machines	root	50	16 hours	No

Refresh

Don't refresh this page.

[Go!](#)

RTIR is built around *Incidents*

Incidents tie everything together

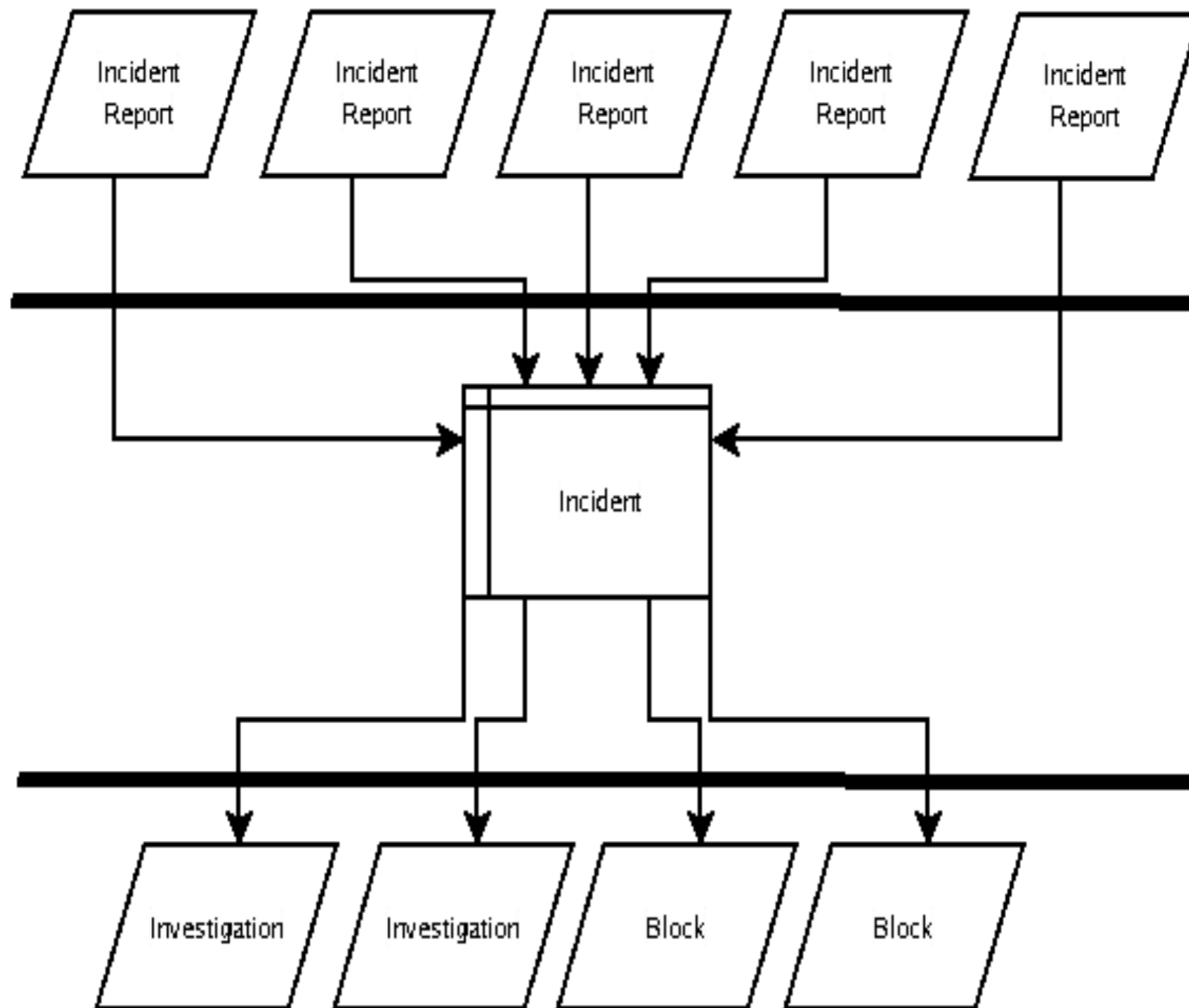
One Incident for

many Incident Reports

many Investigations

many Blocks

RTIR Relationships



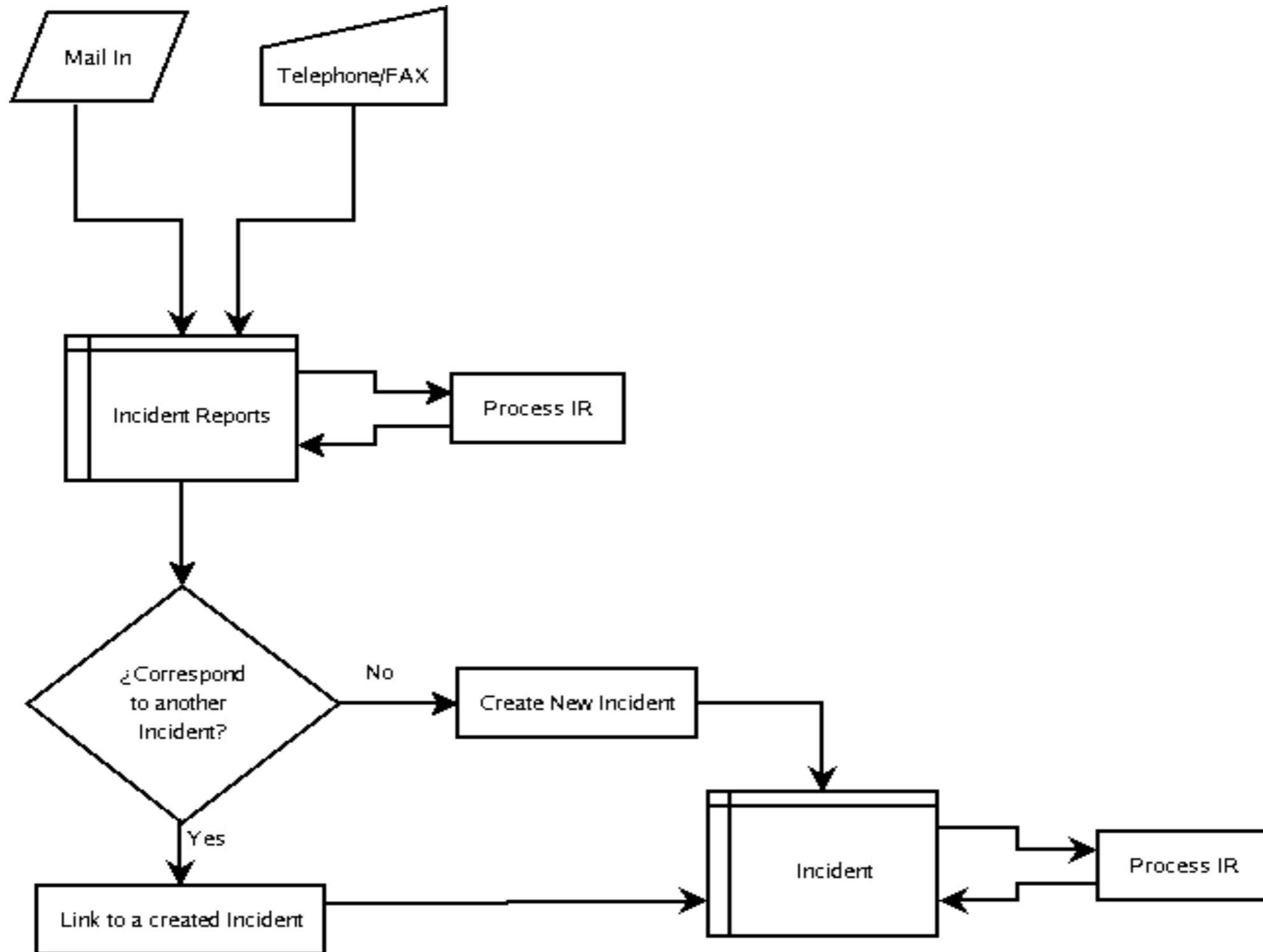
It usually starts with an *Incident Report*

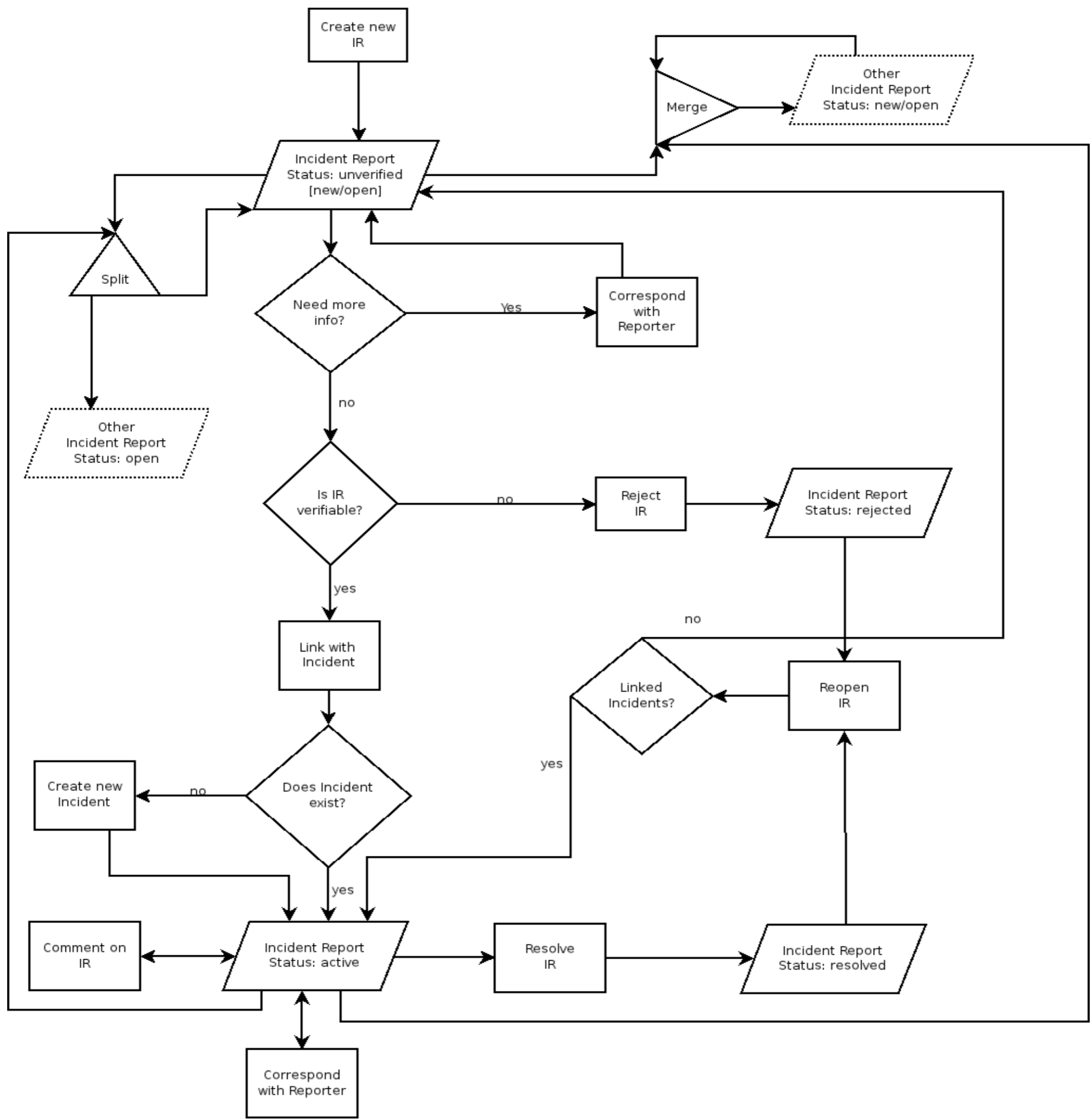
Conversations with Customers

“Something bad happened!”

“Please help me!”

Incident Report





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:

Create an IR #2

How Reported: (no value) Email Telephone Other Reporter Type: (no value) customer external individual other ISP police

IP address: 10.0.0.1 10.0.2.0/24

Attach file: Browse... Add More Files

Sign using Queue's key Encrypt

Message: Customer reports that he woke up this morning to find that his server was sending lots of spam.

IR Details

Incident Report #3: Someone broke into New ticket in Blocks Search In

Display · Edit · Split · Merge · Advanced

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

Results

- Ticket 3 created in queue 'Incident Reports'

The Basics

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

IP Address:

- 10.0.0.1
- 10.0.2.0-10.0.2.255

People

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

Dates

Created: Sun Sep 21 17:07:03 2008
 Starts: Mon Sep 22 09:00:00 2008
 Started: Not set
 Due: Mon Sep 22 11:00:00 2008 [Set to 7 days from now]
 Updated: Sun Sep 21 17:07:05 2008 by root

Articles

| New | Link |

Incident Report Reply

State: new

Update Type:

Owner: Worked: minutes

Subject:

One-time Cc:

One-time Bcc:

Attach file:

Sign using Queue's key Encrypt

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

#	Sun Sep 21 17:07:03 2008	root - Ticket created	Reply Comment Forward
<p>Subject: Someone broke into our server!!!!!!</p> <hr/> <p>Customer reports that he woke up this morning to find that his server was sending lots of spam.</p>			<p>Download (untitled) / with headers text/html 109b</p>
#	Sun Sep 21 17:07:04 2008	RT_System - Outgoing email recorded	Show
#	Sun Sep 21 17:07:04 2008	RT_System - AdminCc DutyTeam EDUNET added	
#	Sun Sep 21 17:07:04 2008	RT_System - Due changed from Not set to Mon Sep 22 11:00:00 2008	
#	Sun Sep 21 17:07:04 2008	RT_System - State new added	
#	Sun Sep 21 17:07:05 2008	RT_System - Starts changed from Not set to Mon Sep 22 09:00:00 2008	
#	Sun Sep 21 17:08:05 2008	root - Correspondence added	Reply Comment Forward
<p>Dearest customer,</p> <p>We're looking into your issue today. Expect to hear from us this evening.</p>			<p>Download (untitled) / with headers text/html 113b</p>
#	Sun Sep 21 17:08:05 2008	RT_System - Due changed from Mon Sep 22 11:00:00 2008 to Mon Sep 22 09:00:00 2008	
#	Sun Sep 21 17:08:05 2008	RT_System - Outgoing email recorded	Show

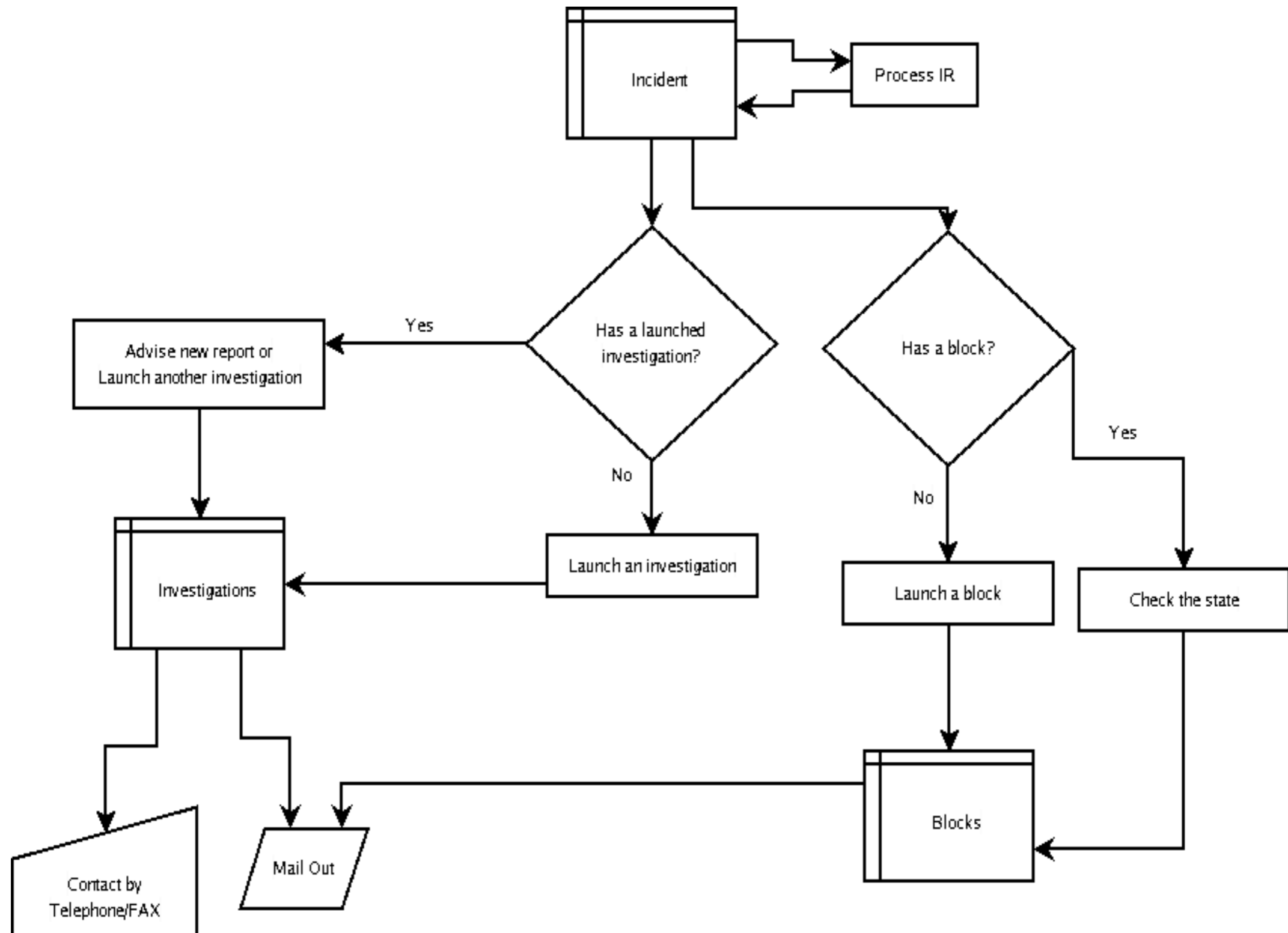
Once reported, the team tracks an *Incident*

Track what actually happened

Private / Internal

Tie everything together

Incident Lifecycle



Create an Incident

Create a new Incident New ticket in Blocks Search In

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

Create a new Incident

Link with: Report #3: Someone broke into our server!!!!

Owner: Enoch Root

Subject: Spammers are attacking customer machines

Description:

Constituency: EDUNET

Function: IncidentCoord

Classification: System Compromise

Resolution: (no value)

IP: 10.0.0.1
10.0.2.0-10.0.2.255

Attach file: Browse... Add More Files

Sign using Queue's key Encrypt

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 #4: Spammers are attacking

Display · Edit · Split · Merge · Advanced

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

Results

- Ticket 4 created in queue 'Incidents'
- 70280b873d05396b782b7fa5c6e37342

Incident #4

Owner: Enoch Root
 State: open
 Subject: Spammers are attacking customer machines
 Description: no value
 Priority: 50
 Time Worked: 0 min
 Constituency: EDUNET
 Function: IncidentCoord
 Classification: System Compromise
 Resolution: no value

IP Address:

- 10.0.0.1
- 10.0.2.0-10.0.2.255

Incident Reports

| New | Link |

3 Someone broke into our server!!!!!!	open 16 hours
--	---------------

(No inactive Incident Reports)

Investigations

| Launch | Link |

Blocks

| New | Link |

Incident Details #2

Function: IncidentCoord
Classification: System Compromise
Resolution: no value

IP Address:

- 10.0.0.1
- 10.0.2.0-10.0.2.255

Investigations | Launch | Link |

(No active Investigations)
(No inactive Investigations)

Blocks | New | Link |

(No active Blocks)
(No inactive Blocks)

Dates

Created: Sun Sep 21 17:13:24 2008
Starts: Sun Sep 21 17:13:25 2008
Due: Mon Sep 22 09:00:00 2008
Updated: Sun Sep 21 17:13:25 2008 by root

Articles | New | Link |

Incident History

History Brief headers — Full headers

- # Sun Sep 21 17:13:25 2008 **RT_System - Due changed from Not set to Mon Sep 22 09:00:00 2008**
- # Sun Sep 21 17:13:25 2008 **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 118b
- # Sun Sep 21 17:13:25 2008 **RT_System - AdminCc DutyTeam EDUNET added**
- # Sun Sep 21 17:13:25 2008 **RT_System - State open added**
- # Sun Sep 21 17:13:25 2008 **RT_System - Starts changed from Not set to Sun Sep 21 17:13:25 2008**

Incident ⇒ Investigation

Run Investigation

Subject:

Time Worked: Time Left:

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.)

Customer:

Sign Encrypt

Message:

[Create Incident and run Investigation](#)

The team starts an *Investigation*

Internal Research and Discovery

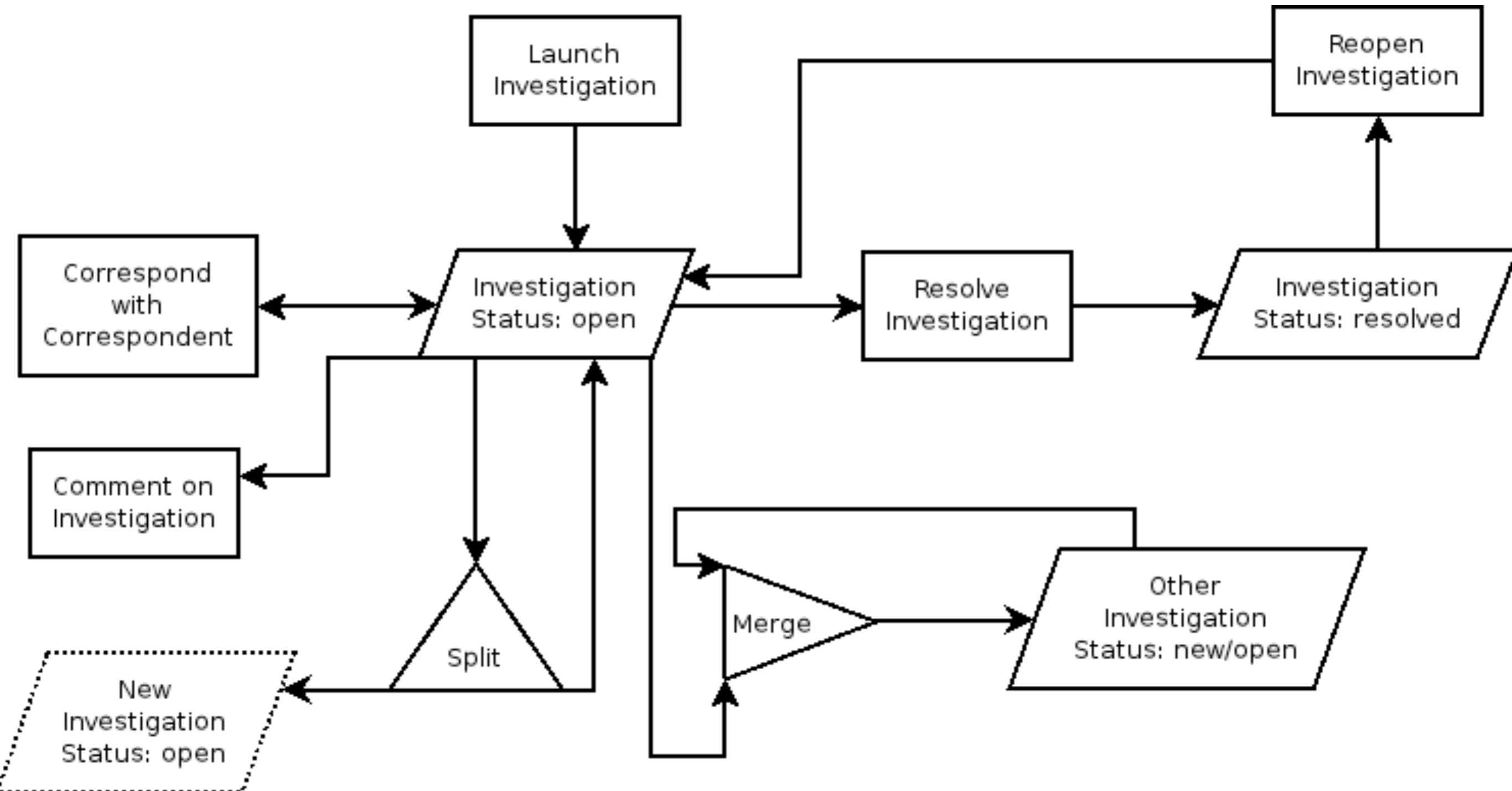
Conversations with external partners

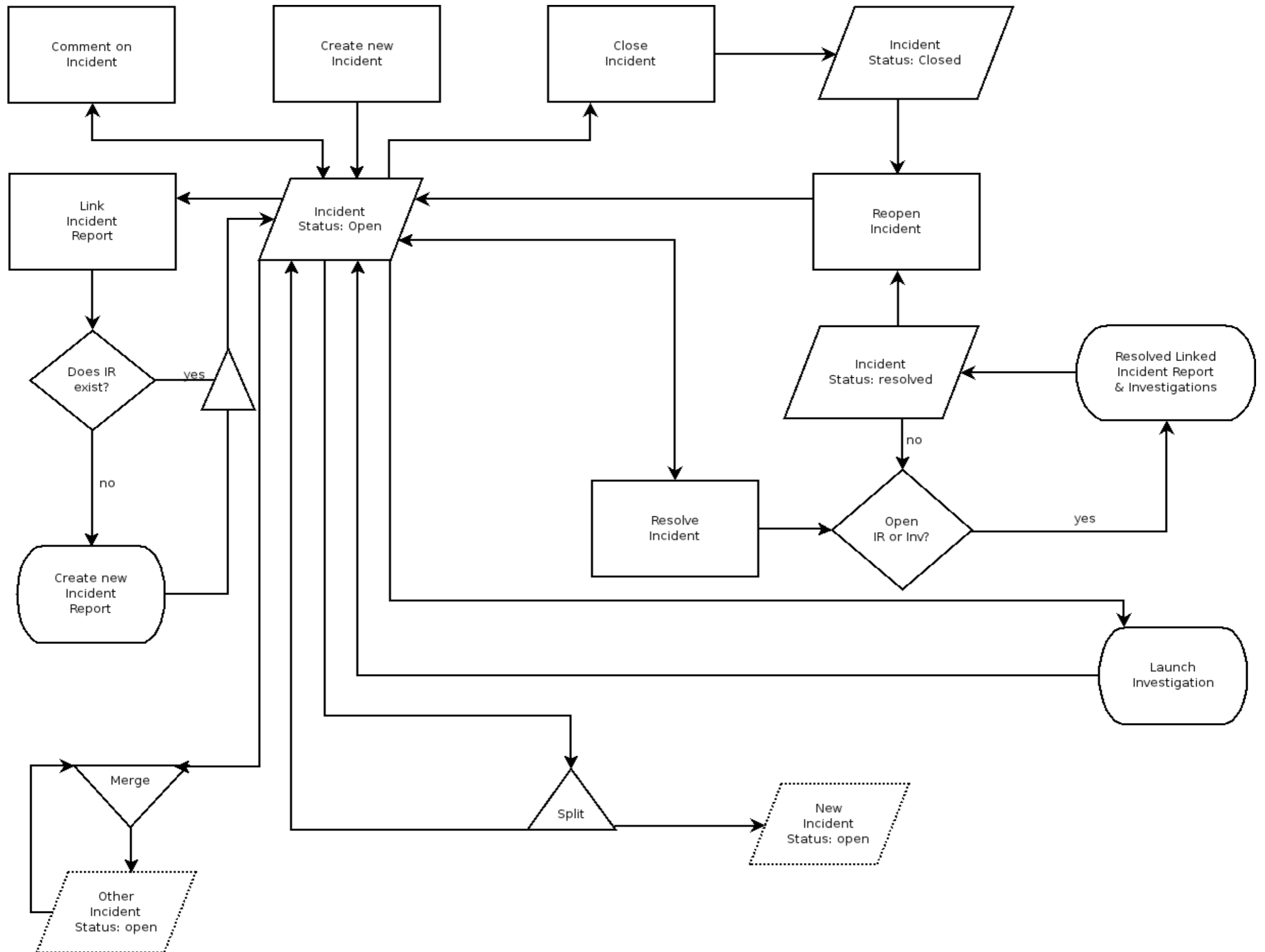
Law Enforcement

Network Providers

Experts

Investigation Lifecycle





Launch Investigation

Launch a new Investigation New ticket in Blocks Search In

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

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

Launch a new Investigation

Incident: 4

Owner: Enoch Root

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: EDUNET
GOVNET

Customer: (no value)

IP address:

Launch Investigation

^ Attach Reports

<input type="checkbox"/>	#	Subject	State	Last Updated	Created
<input checked="" type="checkbox"/>	3	Someone broke into our server!!!!!!	open	1 min ago	7 min ago

Sign using Queue's key Encrypt

Message:

Jim,
Can you help us track down router logs for this customer's issue. He says he first started seeng weird behaviour at about 4:10am
Thanks!

^ Dates

Starts:

Due:

Investigation Details

Investigation #5: Track down router logs

Display · Edit · Split · Merge · Advanced

Reply · Resolve · Quick Resolve · Comment · Extract Article

Results

- Ticket 5 created in queue 'Investigations'

The Basics

State: open

Incident:

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

 [Link] [New]

Constituency: EDUNET

Time Worked: 0 min

Customer: no value

IP Address:

- 10.0.0.1
- 10.0.2.0-10.0.2.255

People

Owner: Enoch Root

Correspondents: isp-router-team@customer-isp.example.com

Cc:

AdminCc: Group: DutyTeam EDUNET

Dates

Created: Sun Sep 21 17:16:00 2008

Starts: Mon Sep 22 09:00:00 2008

Started: Sun Sep 21 17:16:00 2008

Due: Mon Sep 29 09:00:00 2008 [Set to 7 days from now]

Updated: Sun Sep 21 17:16:02 2008 by root

Articles

| New | Link |

Investigation History

History
Brief headers — Full headers

Sun Sep 21 17:16:01 2008 **root - Ticket created** Reply Comment Forward

Subject: Track down router logs of attack on customer servers

Jim,

Can you help us track down router logs for this customer's issue. He says he first started seeing weird behaviour at about 4:10am

Thanks!

Download (untitled) / with headers
text/html 176b

Sun Sep 21 17:16:01 2008 **RT_System - Outgoing email recorded** Show

Sun Sep 21 17:16:01 2008 **RT_System - AdminCc DutyTeam EDUNET added**

Sun Sep 21 17:16:01 2008 **RT_System - Due changed from Not set to Mon Sep 29 09:00:00 2008**

Sun Sep 21 17:16:02 2008 **RT_System - State open added**

Sun Sep 21 17:16:02 2008 **RT_System - Starts changed from Not set to Mon Sep 22 09:00:00 2008**

Sometimes the easiest answer is just a *Block*

(Optional Feature)

Tied to an Incident

Records of network blockades

Could autoupdate firewalls

Create a Block

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

Create a new Block

Incident: 4

Owner: Enoch Root

Subject: 192.168.0.23 is attacking our customer. Please block them off

Time Worked: Time Left:

Correspondents: Don't send any emails to correspondents.
(Sends a carbon-copy of this update to a comma-delimited list of email addresses. These people will receive future updates.)

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

Admin Cc:

Constituency: EDUNET
GOVNET

Netmask: 192.168.0/24

Port: All

Where Blocked:

IP address: 10.0.0.1
10.0.2.0-10.0.2.255

Attach file:

Sign using Queue's key Encrypt

Data Detectors

The screenshot shows a 'History' window with a single entry. The entry is a ticket created on Wednesday, September 24, 2008, at 09:51:28, by the user 'root'. The subject of the ticket is 'under attack!'. The main text of the ticket contains two lines of information: 'help! I'm being attacked by 127.0.0.1' followed by a yellow highlight containing the text '[lookup IP][Add IP]', and 'Adn my server keeps trying to connect to a.gtld-servers.net' followed by a yellow highlight containing the text '[lookup host]'.

History

Wed Sep 24 09:51:28 2008 root - Ticket created

Subject: under attack!

help! I'm being attacked by 127.0.0.1 [lookup IP][Add IP]

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

Automatic IP Detection

Incident Report #9: under attack!

Display · Edit · Split · Merge · Advanced

Reply · F

Results

- Ticket 9 created in queue 'Incident Reports'

The Basics

State: new

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

Constituency: EDUNET

Time Worked: 0 min

SLA: Full service: out of hours

Customer: no value

How Reported: Email

Reporter Type: no value

IP Address: 127.0.0.1

Data Detectors

The screenshot shows a 'History' window with a single entry. The entry is a ticket created on Wednesday, September 24, 2008, at 09:51:28, by the user 'root'. The subject of the ticket is 'under attack!'. The main body of the ticket contains two lines of text: 'help! I'm being attacked by 127.0.0.1' and 'Adn my server keeps trying to connect to a.gtld-servers.net'. The IP address '127.0.0.1' and the domain 'a.gtld-servers.net' are highlighted in yellow, with data detector labels '[lookup IP][Add IP]' and '[lookup host]' respectively.

History

Wed Sep 24 09:51:28 2008 root - Ticket created

Subject: under attack!

help! I'm being attacked by 127.0.0.1 [lookup IP][Add IP]

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

Research Tools

Lookup '127.0.0.1' using server whois-

Lookup · Reporting · Scripted Action

Current Report: #9

#	Subject Requestors	State Owner	Last Updated Told	Created Due	Time Left
9	under attack!	new root	1 min ago	1 min ago 2 hours	0

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
8	Help! I'm being attacked.	new	0	[Merge]
9	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

RTIR History

RTIR 1.0

Sponsored by JANET-CERT

Replaced a homebuilt Remedy system

Built on RT 3.0

2003

RTIR 1.0 Features

Clickable 'Data Detectors'

IP/Domain/Address Lookup Tool

RTIR Automated Rules

SLA Monitoring

Business-Hours Logic

RTIR 2

Sponsored by TERENA RTIR WG

Initial vision by JANET-CERT

Design collaboration between RTIR WG
and Best Practical

Built on RT 3.8

RTIR 2.4 released September 2008

RTIR WG Members

JANET CSIRT/UKERNA
(Chair of project)

IRIS-CERT/RedIRIS
(Technical contact)

CERT POLSKA

CERT.PT

GOVCERT.NL

ACOnet-CERT

LITNET CERT

SUNet CERT

SWITCH-CERT

RTIR 2.4 New Features

PGP Integration

Message Forwarding

Ticket Locking

Bulk Actions

Ticket Aging

Quick Actions

Database Pruning

Per-User Timezones

RTFM Integration

IP Address Range Fields

RTIR 2.4 New Features

Improved Automation

Improved UI

Improved Searching

More flexible workflow

Improved Customization

More user preferences

Improved Reporting

Easier Integration

Improved Testing

Improved Performance

Using RTIR

Cost of RTIR: \$0

Cost of required
software: \$0

Cost of required
hardware: \$0?

Operating System

Unix/Linux/FreeBSD/MacOS X/Solaris/etc

(We don't do Windows)

Database

MySQL 4.1 or 5.0

PostgreSQL 8.x

Oracle 9x or 10.x

SQLite (for testing)

Web Server

Apache

mod_perl or FastCGI

lighttpd

FastCGI

Standalone pure-perl server

Getting RTIR

<http://bestpractical.com/rtir>

RT & RTIR Community

<http://wiki.bestpractical.com> - <http://rtir.org>

rtir-subscribe@lists.bestpractical.com

rt-es-subscribe@lists.bestpractical.com

rt-users-subscribe@lists.bestpractical.com

rt-devel-subscribe@lists.bestpractical.com

Muchas gracias!

Questions?

<http://bestpractical.com/rtir>

Jesse Vincent

jesse@bestpractical.com

+1 617 812 0745

Bonus!

Institution - IP correlation

Aim

Correlate automatically the IPs of the IRs, Invs and Blocks with its institutions

Allow us an easiest way to address an investigation

Statistic by institution

What institution got more complaints at the end of the year 😊

When I say institution, it could be department

Requirements and Installation

Requirements

!!!Main one!!! database which associates every institution or department with its IP allocation space

LDAP, MySQL, ... , even a whois server

Modify the "Customer" CustomField of IR and Invs queues to support external values

You have to create your own library

Has to have three functions:

SourceDescription

ExternalValues

GetInstitutionByIP

Requirements and

Install

Download

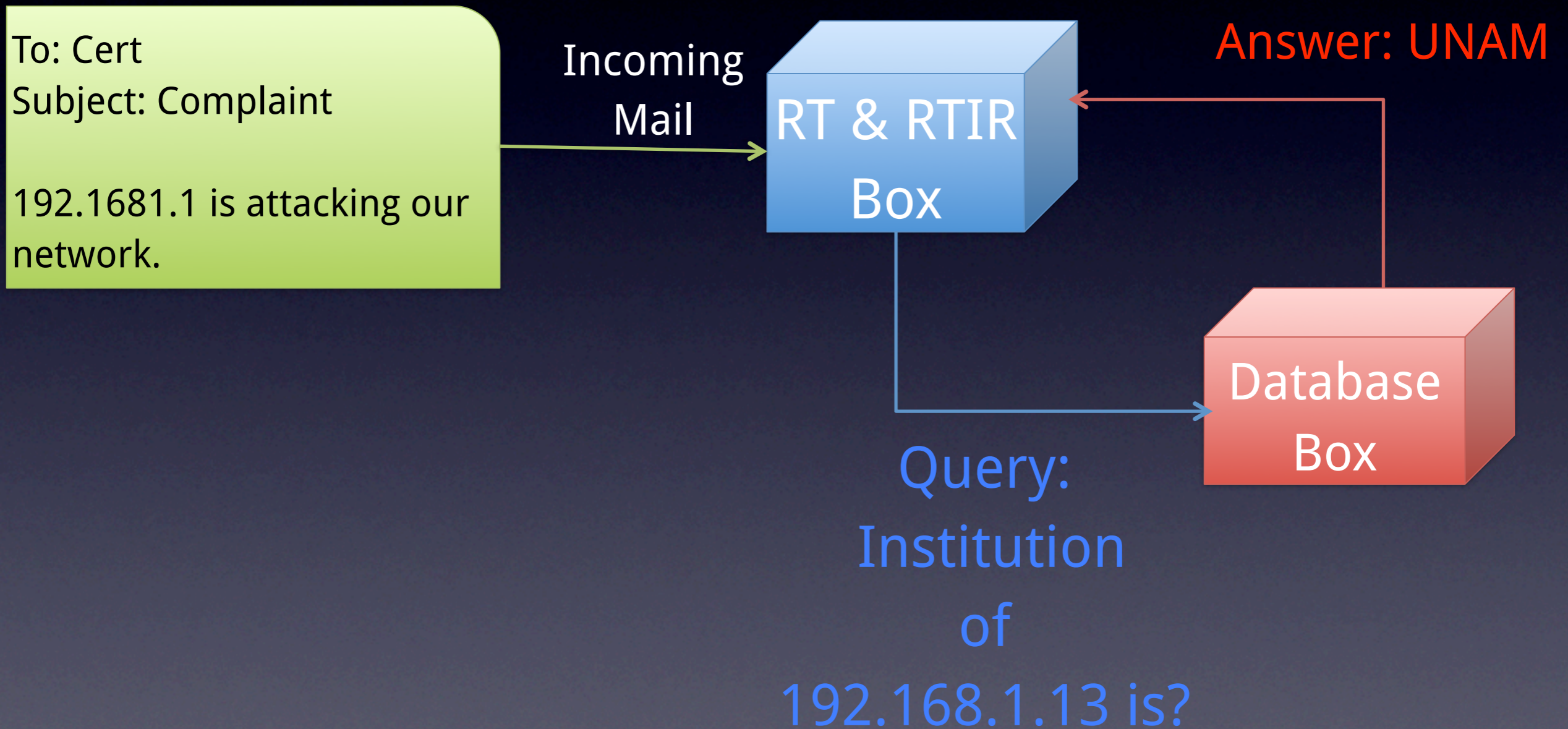
It will be in <http://www.rtir.org>,

Extensions area

Condition OnIPCreate

Condition OnIPDelete

Workflow



^ **The Basics**

State: resolved

Incident: [Conexiones en el puerto TCP 22 desde \(open \)](#)

[\[Steal\]](#)

Constituency: RedIRIS

Time Worked: 0 min

SLA: Full service: out of hours

Customer: UNAM

How Reported: Email

Reporter Type: other

IP Address: 192.168.1.12

Target Type: RedIRIS Customer

Age: (no value)