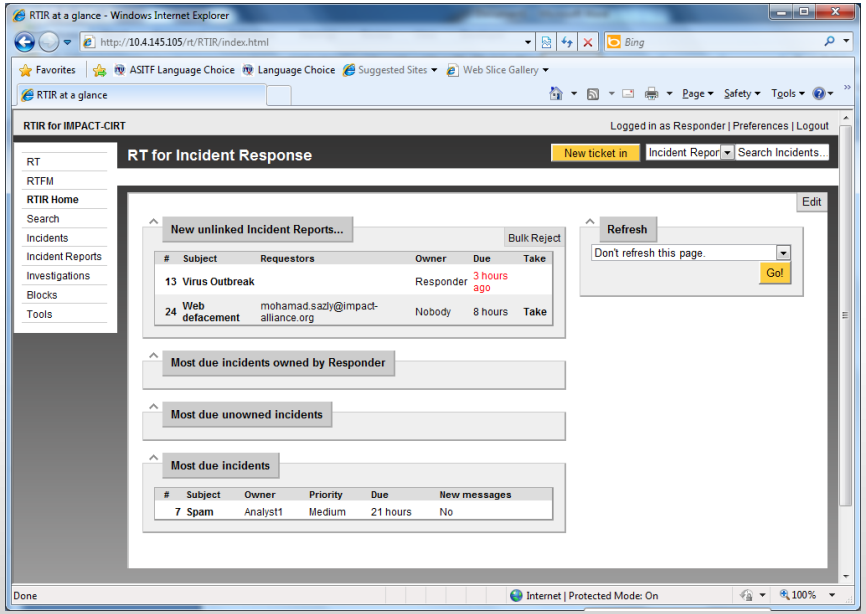
International Telecommunication Union

RTIR FOR INCIDENT MANAGEMENT

What is RTIR?

- RTIR is the premiere open source incident handling system targeted for computer security teams
- Used by over a dozen CERT and CSIRT teams around the world for e.g. JANET CSIRT (UK's National Research and Education Network)
- A Web-based software programmed in Perl.



RTIR Components

- Major components:
  - Web server (Apache + mod_perl-enabled)
  - Database (MySQL, PostgreSQL)
  - An email address to handle incoming tickets
  - An SMTP server to send email out
  - Required Perl modules

RTIR Features

- A workflow designed specifically for incident response
  - Incident reports
  - Incidents
  - Investigations
- A web interface to administer the system
- Reports
  - Generate text, HTML, or spreadsheet reports

Purpose

- To ensure that Computer Incident Response Team (CIRT) members carry out incident handling duties consistently and effectively
- Follow an agreed work-flow pattern for the application Request Tracker for Incident Response (RTIR)

Incident Handling

Detection *(Incident reported/detected)*

Triage *(Incident assessed,categorised, prioritised & queued)*

Analysis *(Research on what happened/who's affected)*

Incident response *(Actions taken to resolve incident)*

RTIR Ticketing System (1)

Incident Reports

- *New reports end up here, with a due date set according to your SLAs, and are displayed on the RTIR dashboard.*

Incidents

- *Valid Incident Reports are turned into new Incidents Ticket or linked to existing ones with one click.*

Investigations

- *Launching further analysis or investigation on the reported case.*

RTIR Ticketing System (2)

Constituency	Responder	Manager	Handler
Incident Reported	Incident Report Ticket	Incident Ticket	Investigation Ticket
	This ticket reaches to the RTIR system via email/portal messages or is created manually by the responder if its lodged via phone or fax.	This ticket is created by the manager after verifying the facts and getting all details from the incident report ticket.	This ticket is created by the handler while doing the investigations and linked to the incident ticket

User Role & Responsibility

There are 3 main people in CIRT:

- **Duty Officer (Responder)**
- **Triage Officer (Manager)**
- **Incident Handler (Analyst)**

User Role & Responsibility

Duty Officer

- Take care of all in-coming requests
- Carry out periodic or ad hoc activities dedicated to this role

User Role & Responsibility

Triage Officer

- Deal with all incident reports that are reported by the duty officer
- Decide whether it is an incident that is to be handled by the team, when to handle it and who is going to be the incident handler according to the triage process.
- Control and monitor the whole incident.

User Role & Responsibility

Incident Handler

- Deals with the incidents and its related investigations
- Analyzing data, creating workarounds, resolving the incident and communicating clearly about the progress he has made to his triage officer and constituent(s)

RTIR Basic Functionalities

RTIR Basic Functionalities (2)

Comment	This link puts you in a form where you can **enter a comment**, just as if you had replied to mail from RTIR about a particular ticket. You can Cc: or Bcc: the comment if you wish.
Reply	This link puts you in a similar form to the comment one with two major differences: • You can change the state of the request from the form. • The reply is automatically sent to the requestor.
Take	Taking a Ticket assigns it to the person who takes it initially when it's in an open state. Their ID goes into the Owner field. You may only Take a Ticket if it is unowned -- if someone else already Owns the Ticket, then you have to Steal it from them to gain Ownership.

RTIR Basic Functionalities (3)

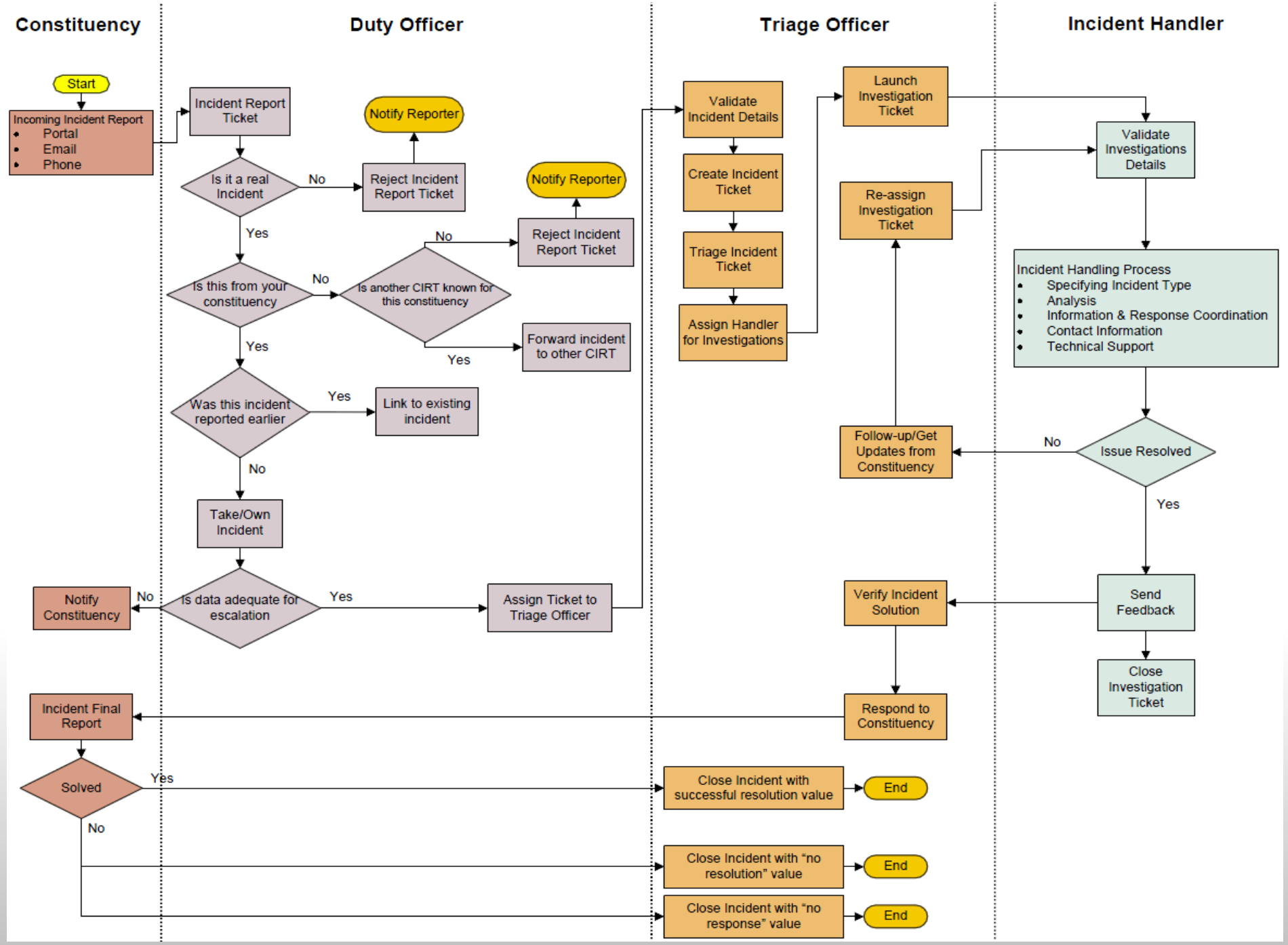
Steal	Stealing a Ticket re-assigns an already Owned ticket to you, instead of to its current Owner. Useful in cases where the original Owner (as compared to you) has become overburdened, under informed, fired, reassigned, amnesiac, promoted, or something else.
Subject	Change the subject of a ticket. Note that RTIR does not keep track of the former subject. If you would like it preserved, you are advised to enter a comment saying that you have changed the subject.
Queue	This is how you move a ticket from one queue to another. Simply select the destination queue from the menu and click. You may move a ticket from any queue you can manipulate into any queue you can create tickets in.

RTIR Basic Functionalities (4)

Priority	You may change the current and/or Final Priority to reflect changes in the Ticket's importance in the grand scheme of things.
Rejecting tickets	A number of legitimate incoming messages, are for information only and once Taken and examined need no further attention. If an Incident ticket is rejected you will have to key in the details about the rejection and submit it to the system. The [Quick Reject] button at the top of the Incident Report will change the report's state to Rejected immediately. Rejected tickets are still searched for IP address matches, and can be linked to Incidents although they will only be displayed if their state is Open or Resolved.
Resolving Incidents	When an Incident requires no further action it can be closed. Children of Incidents (Incident Reports, Investigations and Blocks) can be individually closed during the lifecycle of an Incident once each has run its course.

RTIR Incident Handling Process

- Receiving an Incident
- Validating the Incident Report
- Rejecting the Ticket
- Checking Whether the Incident was reported earlier
- Assigning Incident Report Ticket to the Triage Officer
- Creating an Incident Ticket
- Incident priority and classification
- Linking to an Existing Incident
- Replying to the Incident Report
- Triage Process
- Creating an Investigation Ticket
- Closing an Incident Ticket
- Reporting


Constituency
Duty Officer
Triage Officer
Incident Handler
Start
Incoming Incident Report
Portal
Email
Phone
Incident Report Ticket
Is it a real Incident
No
Notify Reporter
Reject Incident Report Ticket
Yes
Is this from your constituency
No
Is another CIRT known for this constituency
No
Notify Reporter
Reject Incident Report Ticket
Yes
Forward incident to other CIRT
Yes
Was this incident reported earlier
Yes
Link to existing incident
No
Take/Own Incident
Is data adequate for escalation
No
Notify Constituency
Yes
Assign Ticket to Triage Officer
Validate Incident Details
Create Incident Ticket
Triage Incident Ticket
Assign Handler for Investigations
Launch Investigation Ticket
Re-assign Investigation Ticket
Validate Investigations Details
Incident Handling Process
Specifying Incident Type
Analysis
Information & Response Coordination
Contact Information
Technical Support
Issue Resolved
No
Follow-up/Get Updates from Constituency
Yes
Send Feedback
Close Investigation Ticket
Verify Incident Solution
Respond to Constituency
Incident Final Report
Solved
Yes
Close Incident with successful resolution value
End
No
Close Incident with "no resolution" value
End
Close Incident with "no response" value
End

Thank you

For any enquiry forward your email to *grc@impact-alliance.org*