



## RTIR and AbuseHelper integration

Lee Harrigan-Green

Janet CSIRT Senior Member

## Our Reasons for using AbuseHelper

- >> Too much of our time is spent dealing with issues which can be automated
- >> Successful implementation of automating copyright notifications dealt 3957 in the last year
- >> We are a small team and our resources can be put to better use than distributing and processing abuse data

# How we currently process abuse data

A part manual / part automated process

- >> Report is received via email and a incident handler determines if we should process the information and create incidents
- >> Incident handler runs script that creates new incidents / investigations or appends the data to an existing incident / investigation
- >> Where a new incident is created the customer receives this immediately
- >> Where data is appended to an existing incident / investigation, the next time an incident handler reviews the incident the data is sent
- >> We ask for a response for each notification before closing the incident

## Why this is bad

- >> We ask for a response for each notification before closing the incident
- >> We work Monday to Friday, if a report arrives on Friday after 6pm, It will not get processed until after Monday at 8am
- >> Getting the latest data sent out requires intervention by an incident handler
- >> Due to resource issues we have to choose what we process
- >> Incomplete data is sometimes sent out making investigations difficult
- >> A response is not often required and creates unnecessary work for both parties

## Consultation with our customers

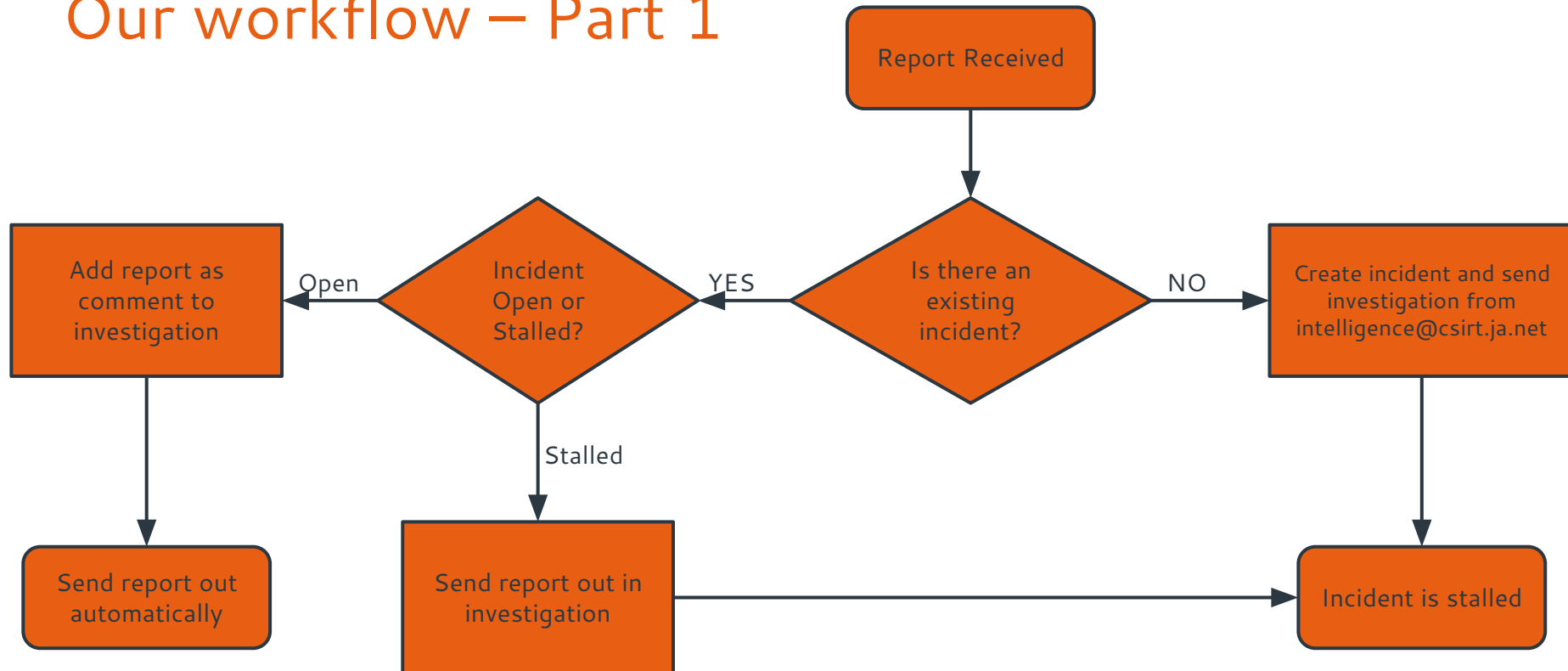
We asked our customers how they wanted us to process data:

- >> In real time and aggregated
- >> Within our existing ticketing system
- >> 'high risk' events handled by us and low level automation
- >> Via Email

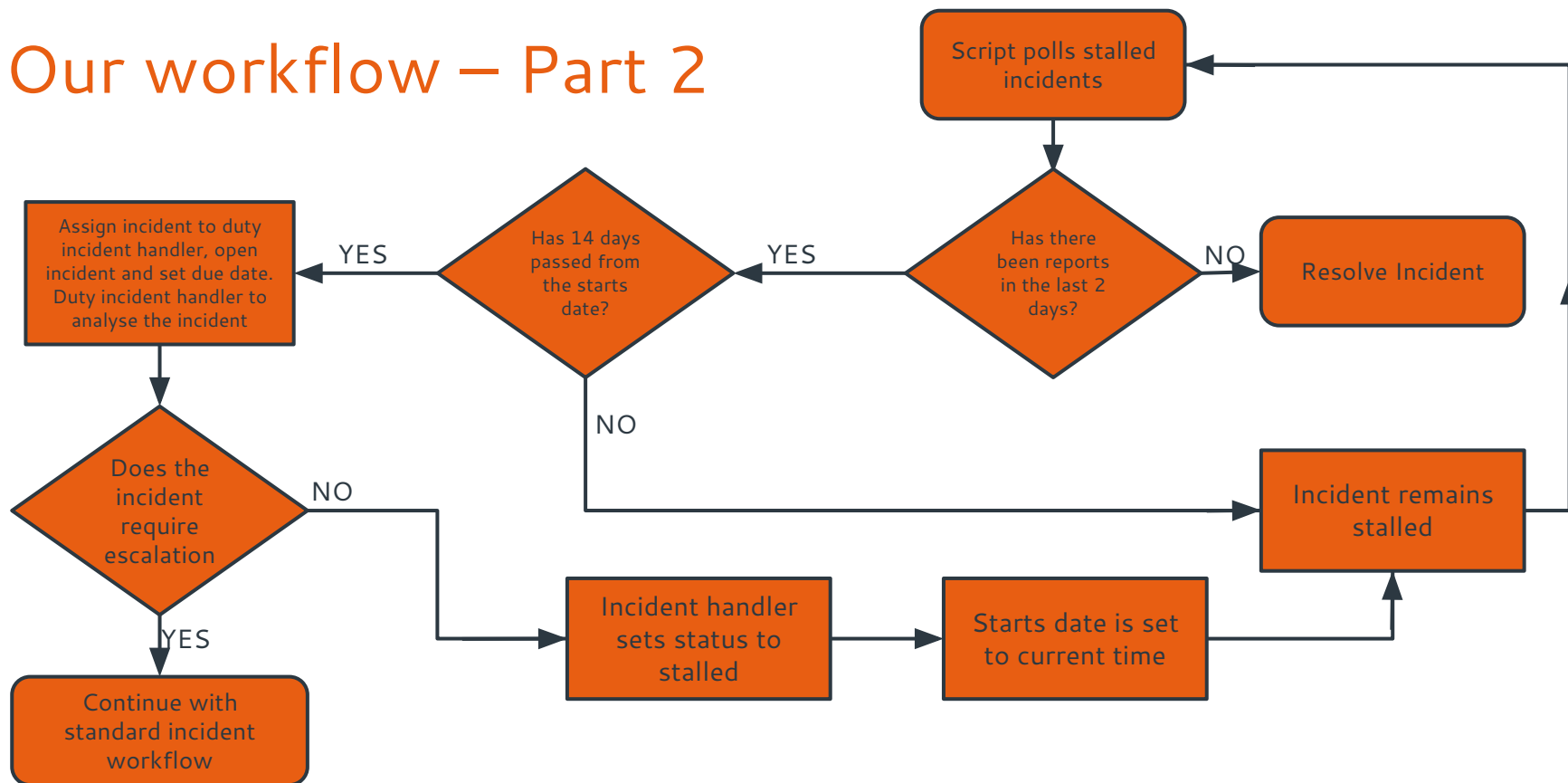
## How we are going to process abuse data

- » All abuse reports will be automated
- » All reports originate from a separate email address to our incident handling system
- » All reports will still be associated with an RTIR reference
- » Customers can choose an aggregate or real time report
- » We no longer require a response from our customers
- » If reports persist for an institution an incident is brought to our attention for us to see if further assistance may be required

# Our workflow – Part 1



## Our workflow – Part 2





## Changes to RTIR

A number of customisations were required to RTIR in order to facilitate our automated workflow:

- >> Customised source e-mail addresses
- >> New stalled incident state
- >> A reply to an investigation within a stalled incident opens the incident
- >> Utilizing the starts date in an unexpected way
- >> Reports are sent in 2 different formats, aggregated & real time

## Customised source e-mail addresses

As we have a number of different types of information passing through RTIR it was deemed that the best way for Janet customers to receive this was by separating the source e-mail addresses.

Currently we use 3 separate source email addresses within RTIR:

[irt@csirt.ja.net](mailto:irt@csirt.ja.net) – Standard Incident handling

[copyright@csirt.ja.net](mailto:copyright@csirt.ja.net) – Copyright automation

[intelligence@csirt.ja.net](mailto:intelligence@csirt.ja.net) – Abusehelper automation

The benefits of separating these different reports is our customers can easily identify the different requirements upon them for dealing with the issues that we send. It also makes it easier for them to manage these reports internally.

A reply to any of these addresses with the appropriate RTIR reference in will open the investigation.

## New stalled incident state

The main driver for this automation is to reduce the workload within our team and to provide additional information to our customers.

In order to keep this data within our primary instance of RTIR it is required for us to easily filter out incidents that we do not currently require any work from us this new state enables that process.

The stalled state is an intermediary state between open and resolved.

A stalled incident does not require any action by an incident handler.

When a customer replies to an investigation contained within a stalled incident a scripted action then brings the stalled incident to open.

## RTIR Starts date

The RT starts date is a date variable that can be used to identify when actions may need to be taken on an incident.

We found that we were not using this variable anywhere within our current workflow.

We are using this as a variable to identify when an incident was set as stalled. When an incident is set as stalled it updates this variable with the current date.

As you have seen from the previous workflow this data is used to identify if an incident needs to be escalated or not.

# Aggregated or Real Time reports

Working with Codenomicon we have developed as requested by our customers 2 different reporting styles.

## **Aggregated reports**

Collate data over a period of time (Currently set to 1 Day) and will report all the information to the customer within a single RTIR Incident.

## **Real time reports**

As soon as the data arrives within AbuseHelper it then follows the initial workflow, this means we have a separate incident per source IP address.

Our customers can select between these 2 reporting styles based upon individual AbuseHelper feeds.

## Where we are currently with development

We have gone live with a select number of customer sites and are in a final testing and development phase prior to switching the service on for all customers.

We are also developing an web based interface where our customers can select the AbuseHelper feeds that they want to receive and the reporting style of them.

# Any questions?



Lee Harrigan-Green  
Senior CSIRT Member  
[lee.harrigan-green@jisc.ac.uk](mailto:lee.harrigan-green@jisc.ac.uk)  
PGP: 16BC0AEB  
Tel: +44 1235 822 340