Carnegie Mellon University
Software Engineering Institute

Triage

Foundations of Incident Management (FIM)

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

Notices

This material is based upon work funded and supported by the Independent Agency under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center sponsored by the United States Department of Defense.

The view, opinions, and/or findings contained in this material are those of the author(s) and should not be construed as an official Government position, policy, or decision, unless designated by other documentation.

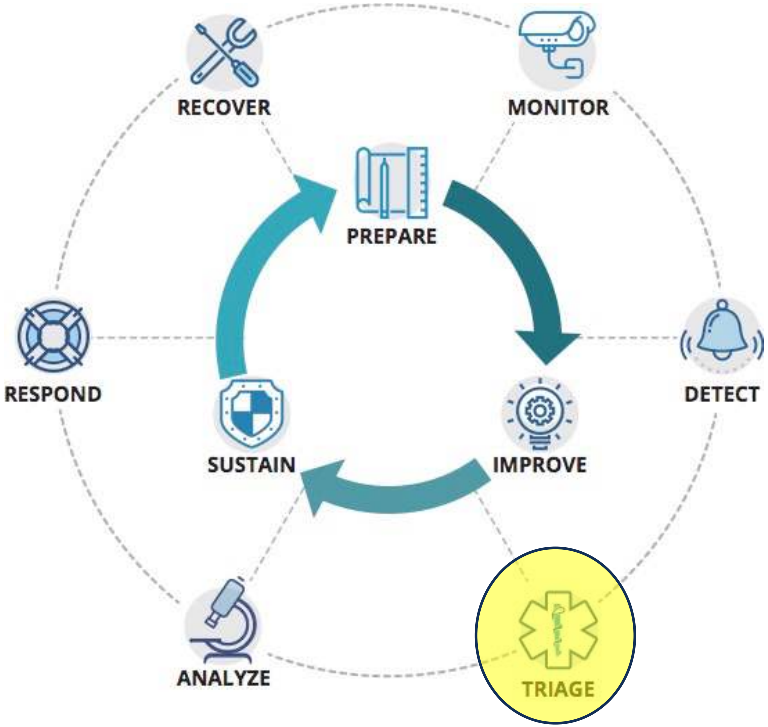
NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN "AS-IS" BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

This material is distributed by the Software Engineering Institute (SEI) only to course attendees for their own individual study.

Although the rights granted by contract do not require course attendance to use this material for U.S. Government purposes, the SEI recommends attendance to ensure proper understanding.

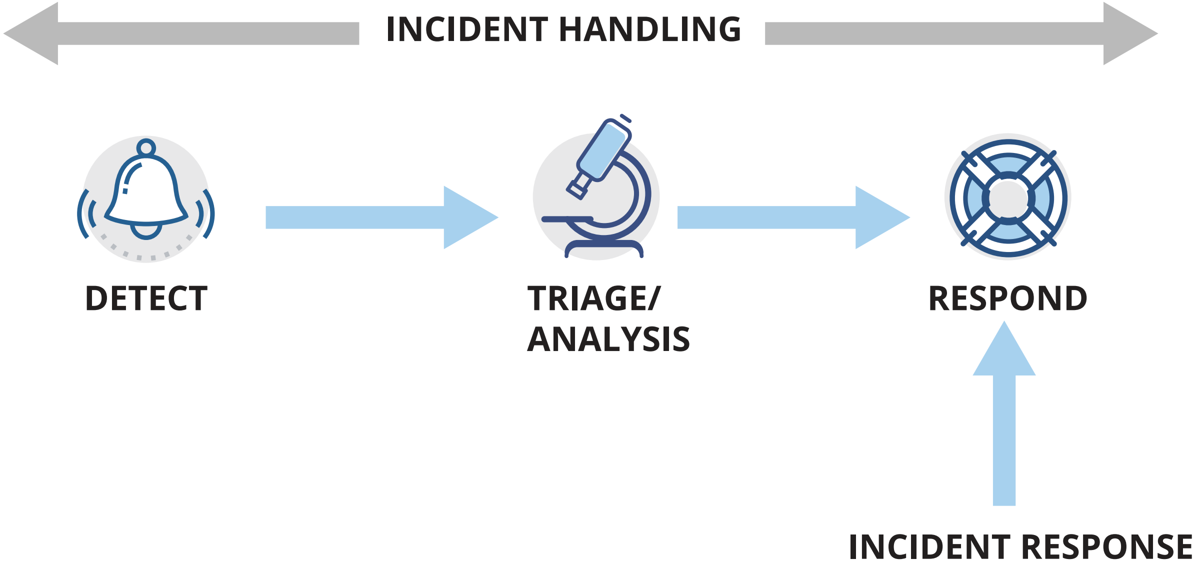
DM19-0875

Overview [Reminder] of Triage in the Incident Management Lifecycle



Terms & Definitions – Triage

Actions taken to categorize, prioritize, and assign events and incidents



Objectives of the Triage Process

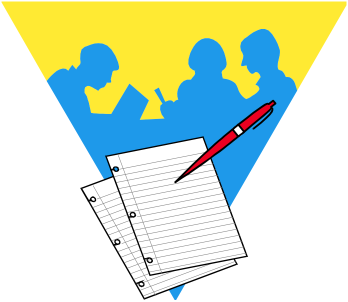
Identify and sort.

Assign to other roles.

What Questions Are Addressed in Triage?

During the triage process, a number of questions are answered and first steps taken.

- What category and priority should a report or request be assigned?
- Is this a new report or is it related to ongoing activity?
- Are any preliminary actions required?
  - Decrypt information.
  - Virus check any attachments.
  - Distribute information to others on staff related to a hot site or ongoing communications.
- Who should handle this event or incident?



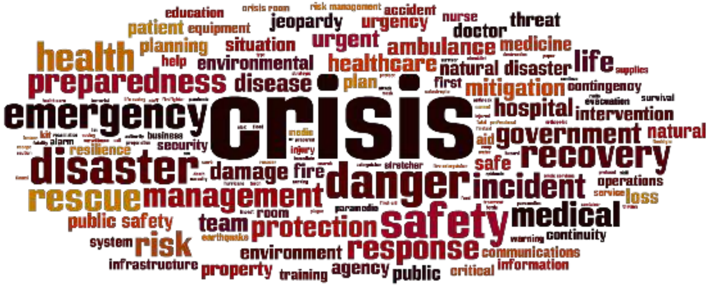
Triage Functions

Categorization

Prioritization

Correlation

Assignment



Categorization

Possible criteria

- type of activity
- impact or severity
- type of report or request
- complexity of incident

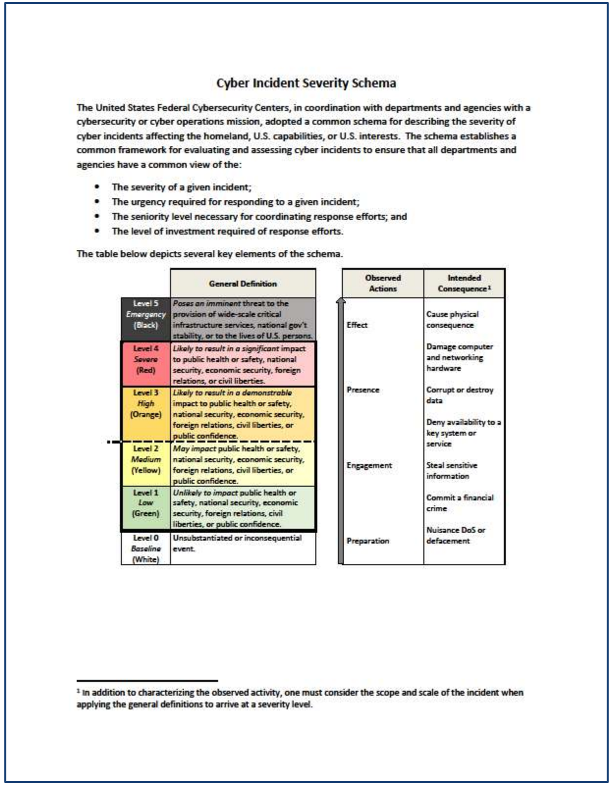
Category	Name
CAT 0	Exercise/Network Defense Testing
CAT 1	Unauthorized Access
CAT 2	Denial of Service (DoS)
CAT 3	Malicious Code
CAT 4	Improper Usage
CAT 5	Scans/Probes/Attempted Access
CAT 6	Investigation

US-CERT Federal Incident Reporting Guidelines (until 2015 Sep 30)

Prioritization

Possible criteria

- type of activity
- severity
  - scope or scale
- who reported or is affected



Cyber Incident Severity Schema

The United States Federal Cybersecurity Centers, in coordination with departments and agencies with a cybersecurity or cyber operations mission, adopted a common schema for describing the severity of cyber incidents affecting the homeland, U.S. capabilities, or U.S. interests. The schema establishes a common framework for evaluating and assessing cyber incidents to ensure that all departments and agencies have a common view of the:

- The severity of a given incident;
- The urgency required for responding to a given incident;
- The seniority level necessary for coordinating response efforts; and
- The level of investment required of response efforts.

The table below depicts several key elements of the schema.

	General Definition
Level 5 *Emergency* (Black)	*Poses an imminent* threat to the provision of wide-scale critical infrastructure services, national gov't stability, or to the lives of U.S. persons.
Level 4 *Severe* (Red)	*Likely to result in a significant* impact to public health or safety, national security, economic security, foreign relations, or civil liberties.
Level 3 *High* (Orange)	*Likely to result in a demonstrable* impact to public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence.
Level 2 *Medium* (Yellow)	*May impact* public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence.
Level 1 *Low* (Green)	*Unlikely to impact* public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence.
Level 0 *Baseline* (White)	Unsubstantiated or inconsequential event.

Observed Actions	Intended Consequence[1]
Effect	Cause physical consequence
	Damage computer and networking hardware
Presence	Corrupt or destroy data
	Deny availability to a key system or service
Engagement	Steal sensitive information
	Commit a financial crime
Preparation	Nuisance DoS or defacement

[1] In addition to characterizing the observed activity, one must consider the scope and scale of the incident when applying the general definitions to arrive at a severity level.

Correlation

May or may not happen

- during initial triage
- while working through incidents
  - during staff meetings or daily incident handling meetings
- later during incident coordination and response

Assignment

May be based on

- category or priority of the event
- current workload
- current person responsible for handling an existing incident
- incident handler expertise
- responsible functional business unit

What Can Help Perform Efficient Triage?

To perform triage in the most efficient method possible requires some other type of activities to be performed.

Some would be done by other parts of your organization and the outputs provided to the CSIRT including

- risk analysis – to determine the various risks to your critical assets and the resulting impacts
- critical asset inventory and evaluation – that allows you to benchmark the importance and priority of critical assets
- data classification scheme – that identifies what type of data requires what type of protection and classification, this may impact prioritization

Others are processes that should be part of your CSIRT operations such as

- shift handoffs – if CSIRT or helpdesk has multiple shifts for a 24 hour operation
- beginning and end of day reports – that help summarize what has happened and what is left to be done

Elements that Support Triage

Use of reference numbers

Use of a database to record and track information

In-class Discussion: Triage

How does your organization triage cyber events and incidents?

What more should *you* know to help the triage process?

Documentation and Tracking

The Need for Documentation -1

Short term or operational

During an incident, written documentation regarding

- what happened
- impact or significance
- information gathered
- analysis performed
- steps taken
- who is informed

Vital to fully understanding the situation and the successful closing of an incident

The Need for Documentation -2

Long term

- trending
- basic statistics
- repeat offenders
- reports to upper/senior management
- situational awareness

Incident Reports

The term *Incident Report* has different meanings in different contexts.

The initial message from the victim of a cyber incident can be referred to as the *Incident Report.*

The final report detailing a closed incident can legitimately be called the *Incident Report.*

Here we are primarily concerned with the documentation and tracking of activity between the time of the initial incident report to the delivery of the final incident report.

Incident Tracking

What Is a Ticket, Really?

In general, it is the data related to a reported incident.

More importantly, it is a method of tracking the work.

It may be an amorphous collection of fields in a data base related by a key such as the ticket number.

It may be a file or directory containing such data.

It could even be a spreadsheet.

The Need for Incident Tracking

Once an incident has been reported or otherwise detected, it should “enter the system” so its progress can be followed.

Incident tracking is often done with a ticketing system, sometimes called an issue tracking system.

Uses of Ticketing Systems

Ticketing systems are a tool used by many Incident Management teams to manage their cases. Usually

- meant to support operational tasks such as: Open a case, assign pieces of it to different analysts, track their tasks, collect status, close a case, etc.
- key functionality includes Workflow – assigning tasks to different groups to work through a process until completion
- require customization to be used in an IR context
    - Some systems are specific to typical incident management needs.
- integrated with other systems to exchange data such as IT helpdesks, SOC systems, Email (for workflow notifications), Threat Intelligence platforms
- teams store Cross-Reference numbers in their ticketing systems to knowledge and storage resources outside of their ticketing systems
    - such as Wiki pages or storage servers with case or forensic artifacts

What Makes a Good Ticketing System?

Characteristics of ticketing systems include

- front end data entry and query interface
- back end data base
- multiple user roles (for example: query, update, administer)
- methods of automation
  - entry
  - export
- flexible export capabilities

Where Do Ticketing Systems Come From?

These are the most common

- acquired as a commercial product
  - for example, JIRA, ServiceNow, Remedy
- assembled internally from open source software
  - for example, start with RTIR
- written and maintained strictly in house
  - tend not to get a lot of publicity

Acquired as a Commercial Product

Commercial ticketing systems are often repurposed from a different field.

There are arguably more IT Help Desk issue tracking systems than actual incident response ticketing systems.

- Advantages
  - It comes as a mature product.
  - Professional support is available.
- Disadvantages
  - needs lots of configuration
  - can be expensive for what you get
  - If repurposed, it may not have all of the required data fields and features needed.

Assembled Internally from Open Source Software

There are many open source packages for incident response ticketing/tracking.

- Advantages
  - It has a low initial cost.
  - Most of the work is done.
  - It is designed for Incident Response not IT Help Desk.
- Disadvantages
  - still needs to be configured
    - by you
    - perhaps with “help” from the entire Internet community
  - questionable long term stability
  - often supported by volunteers on their own schedule

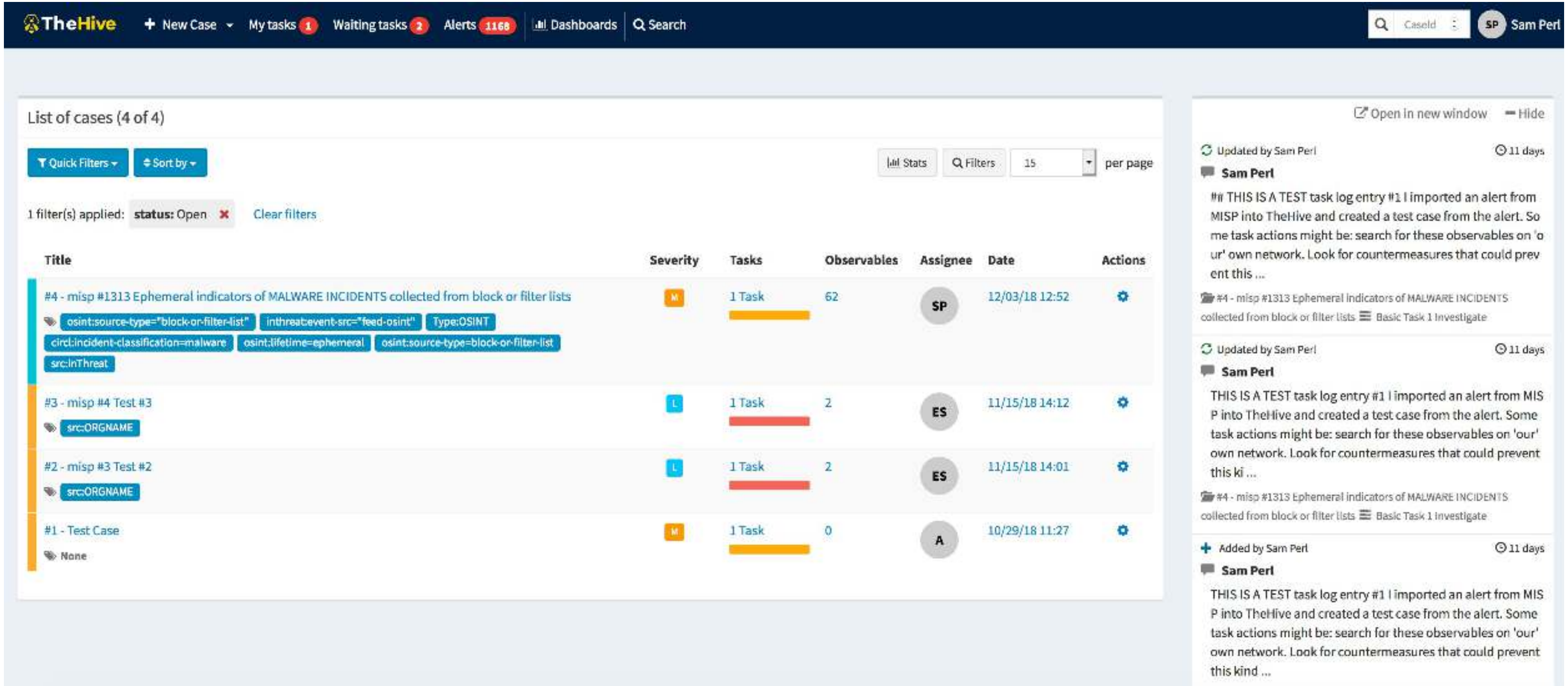
Written and Maintained Strictly In-house

In-house systems often start small and evolve with the organization.

- Advantages
  - can be tailored to the needs of the response team
  - may cost less than a commercial system
  - in-house support
- Disadvantages
  - requires a skilled development team
  - turnover of developers
  - may suffer from growing pains as it is coded to do more

Example Ticketing Systems

TheHive



List of cases (4 of 4)

1 filter(s) applied: **status:** Open ✖ Clear filters

Title	Severity	Tasks	Observables	Assignee	Date	Actions
#4 - misp #1313 Ephemeral indicators of MALWARE INCIDENTS collected from block or filter lists osint:source-type="block-or-filter-list" inthreat:event-src="feed-osint" Type:OSINT circl:incident-classification=malware osint:lifetime=ephemeral osint:source-type=block-or-filter-list src:InThreat	M	1 Task	62	SP	12/03/18 12:52	⚙
#3 - misp #4 Test #3 src:ORGNAME	L	1 Task	2	ES	11/15/18 14:12	⚙
#2 - misp #3 Test #2 src:ORGNAME	L	1 Task	2	ES	11/15/18 14:01	⚙
#1 - Test Case None	M	1 Task	0	A	10/29/18 11:27	⚙

Updated by Sam Perl — 11 days

Sam Perl

THIS IS A TEST task log entry #1 I imported an alert from MISP into TheHive and created a test case from the alert. Some task actions might be: search for these observables on 'our' own network. Look for countermeasures that could prevent this ...

#4 - misp #1313 Ephemeral indicators of MALWARE INCIDENTS collected from block or filter lists ☰ Basic Task 1 Investigate

Updated by Sam Perl — 11 days

Sam Perl

THIS IS A TEST task log entry #1 I imported an alert from MISP into TheHive and created a test case from the alert. Some task actions might be: search for these observables on 'our' own network. Look for countermeasures that could prevent this ki ...

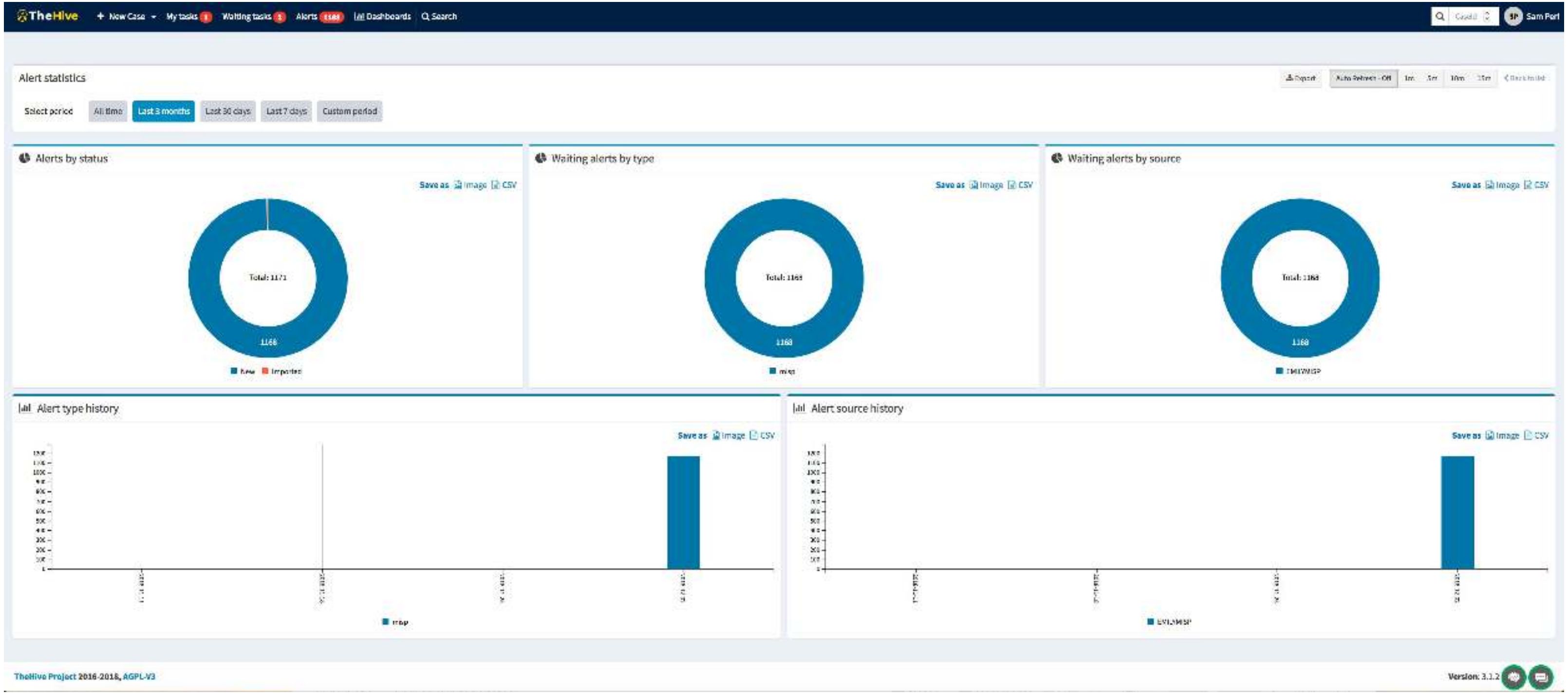
#4 - misp #1313 Ephemeral indicators of MALWARE INCIDENTS collected from block or filter lists ☰ Basic Task 1 Investigate

Added by Sam Perl — 11 days

Sam Perl

THIS IS A TEST task log entry #1 I imported an alert from MISP into TheHive and created a test case from the alert. Some task actions might be: search for these observables on 'our' own network. Look for countermeasures that could prevent this kind ...

TheHive – Dashboards



Alert statistics

Select period: Last 3 months

Alerts by status

Waiting alerts by type

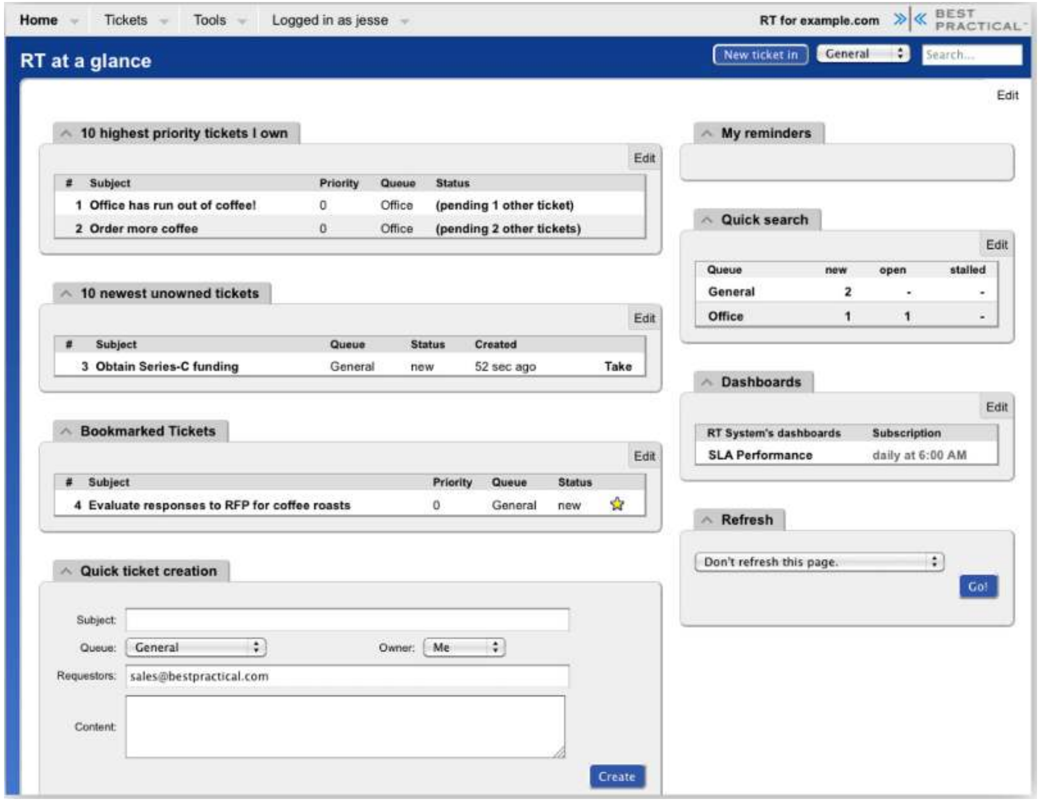
Waiting alerts by source

Alert type history

Alert source history

TheHive Project 2016-2018, AGPL-V3

RT



RT at a glance

10 highest priority tickets I own

#	Subject	Priority	Queue	Status
1	Office has run out of coffee!	0	Office	(pending 1 other ticket)
2	Order more coffee	0	Office	(pending 2 other tickets)

10 newest unowned tickets

#	Subject	Queue	Status	Created	
3	Obtain Series-C funding	General	new	52 sec ago	Take

Bookmarked Tickets

#	Subject	Priority	Queue	Status	
4	Evaluate responses to RFP for coffee roasts	0	General	new	☆

Quick ticket creation

Subject:

Queue: General

Owner: Me

Requestors: sales@bestpractical.com

Content:

Create

My reminders

Quick search

Queue	new	open	stalled
General	2	-	-
Office	1	1	-

Dashboards

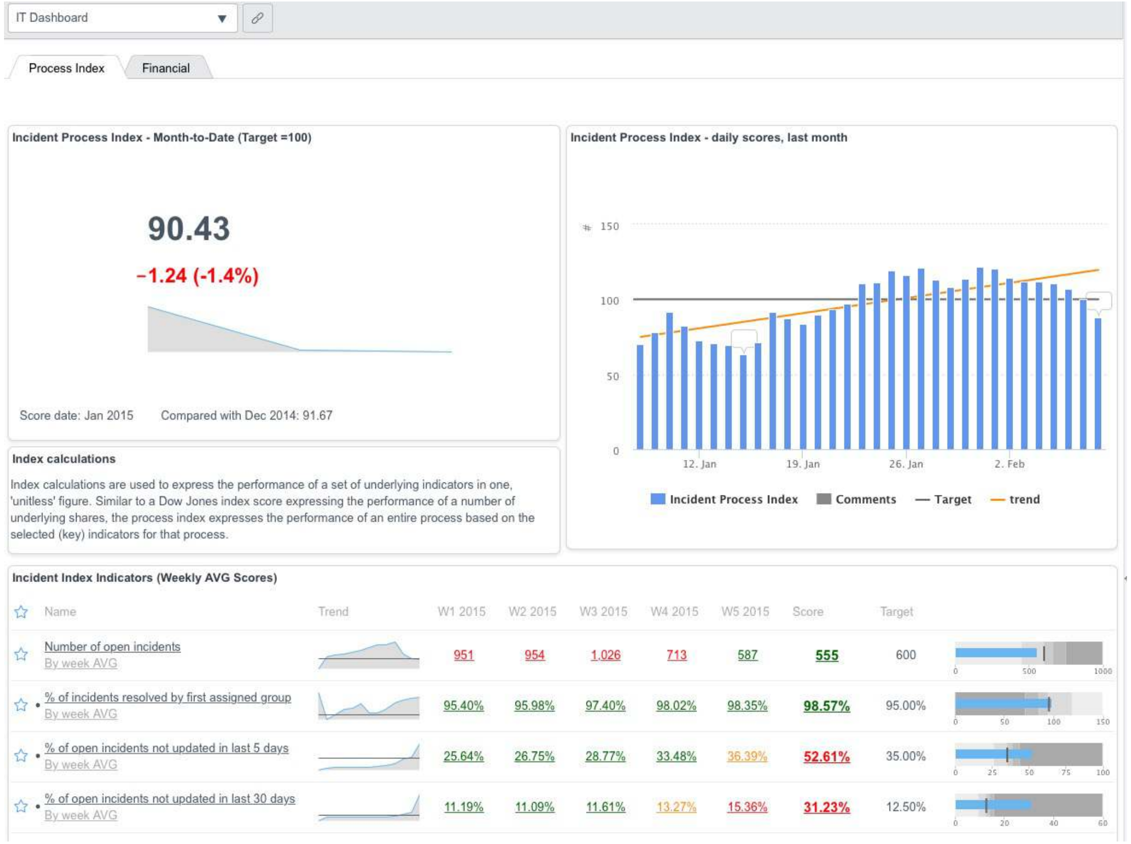
RT System's dashboards	Subscription
SLA Performance	daily at 6:00 AM

Refresh

Don't refresh this page.

Go!

ServiceNow



Incident Process Index - Month-to-Date (Target =100)

90.43

-1.24 (-1.4%)

Score date: Jan 2015 Compared with Dec 2014: 91.67

Incident Process Index - daily scores, last month

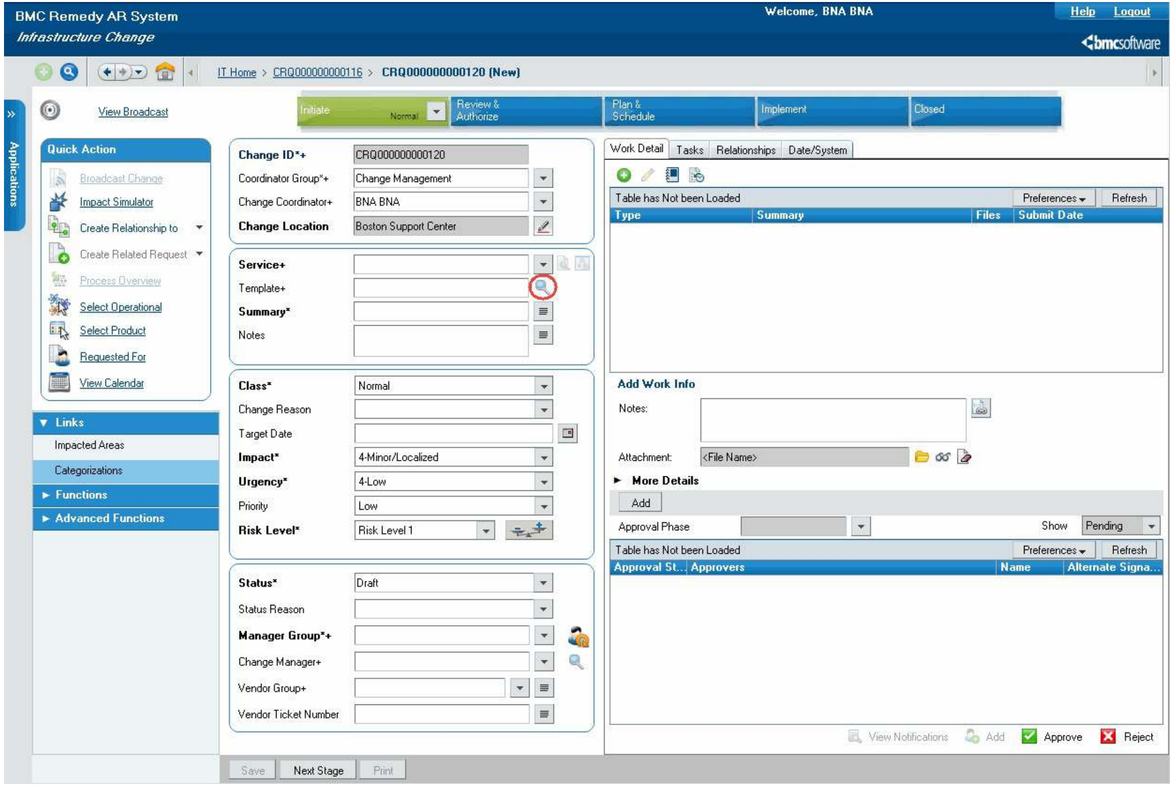
Index calculations

Index calculations are used to express the performance of a set of underlying indicators in one, 'unitless' figure. Similar to a Dow Jones index score expressing the performance of a number of underlying shares, the process index expresses the performance of an entire process based on the selected (key) indicators for that process.

Incident Index Indicators (Weekly AVG Scores)

☆	Name	Trend	W1 2015	W2 2015	W3 2015	W4 2015	W5 2015	Score	Target
☆	Number of open incidents By week AVG		951	954	1,026	713	587	555	600
☆ •	% of incidents resolved by first assigned group By week AVG		95.40%	95.98%	97.40%	98.02%	98.35%	98.57%	95.00%
☆ •	% of open incidents not updated in last 5 days By week AVG		25.64%	26.75%	28.77%	33.48%	36.39%	52.61%	35.00%
☆ •	% of open incidents not updated in last 30 days By week AVG		11.19%	11.09%	11.61%	13.27%	15.36%	31.23%	12.50%

BMC Remedy



Change ID*+ CRQ000000000120

Coordinator Group*+ Change Management

Change Coordinator+ BNA BNA

Change Location Boston Support Center

Service+

Template+

Summary*

Notes

Class* Normal

Change Reason

Target Date

Impact* 4-Minor/Localized

Urgency* 4-Low

Priority Low

Risk Level* Risk Level 1

Status* Draft

Status Reason

Manager Group*+

Change Manager+

Vendor Group+

Vendor Ticket Number

Incident Reporting Forms

Feeding the Ticketing System

Now that we have a ticketing system, we need to populate it.

A popular way to do this includes the use of an incident reporting form.

They tend to range from **too simple**, through **just right,** to **too big**.

Considerations include

- What form does it take?
- How is the information transmitted?
- Who provides the information?
- How does the information get into the ticketing system?

What Goes into an Incident Reporting Form?

The range of possibilities is quite wide.

- free form: no guidance other than “just the facts please”
  - probably rare in mature organizations
- general guidance: “what happened to which system”
  - may be all you get from a user
- specific items: required and optional
  - who, what, when, where, how, how bad
  - generally keyed to the fields in the ticketing system

How the Information Is Transmitted

- Telephone
- Email
- Web
- Direct Transfer

Incident Report by Telephone -1

Suggestions

- Maintain a log of all telephone calls.
  - Get caller’s contact information.
  - Verify (read back) the spelling of names, email addresses, and hostnames using a phonetic alphabet.
- Prepare a list.
  - of the information needed
  - a way to capture it
    - local online form
    - directly into the ticketing system
    - pre-printed list of questions and space for answers
    - (last resort) pencil and paper

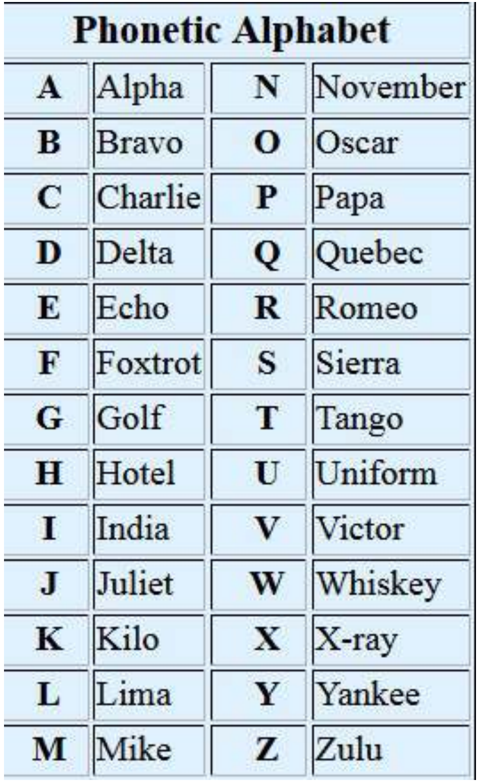
Incident Report by Telephone -2

Advantages

- tends to be more timely
- can ask for clarification immediately
- Get a better sense of urgency.
- Get to know the person reporting.

Disadvantages

- may be less considered or thought out
- can be difficult to ask questions and thoroughly document the answers
- fast/urgent writing – hard to read later
- ephemeral



Phonetic Alphabet

A	Alpha	**N**	November
B	Bravo	**O**	Oscar
C	Charlie	**P**	Papa
D	Delta	**Q**	Quebec
E	Echo	**R**	Romeo
F	Foxtrot	**S**	Sierra
G	Golf	**T**	Tango
H	Hotel	**U**	Uniform
I	India	**V**	Victor
J	Juliet	**W**	Whiskey
K	Kilo	**X**	X-ray
L	Lima	**Y**	Yankee
M	Mike	**Z**	Zulu

Incident Reporting by Email -1

Email incidents come in at least two formats:

- user specified
- incident response team specified

Email messages with specific formats can be processed automatically.

Other email messages can be processed to extract what appears to be relevant data.

Incident Reporting by Email -2

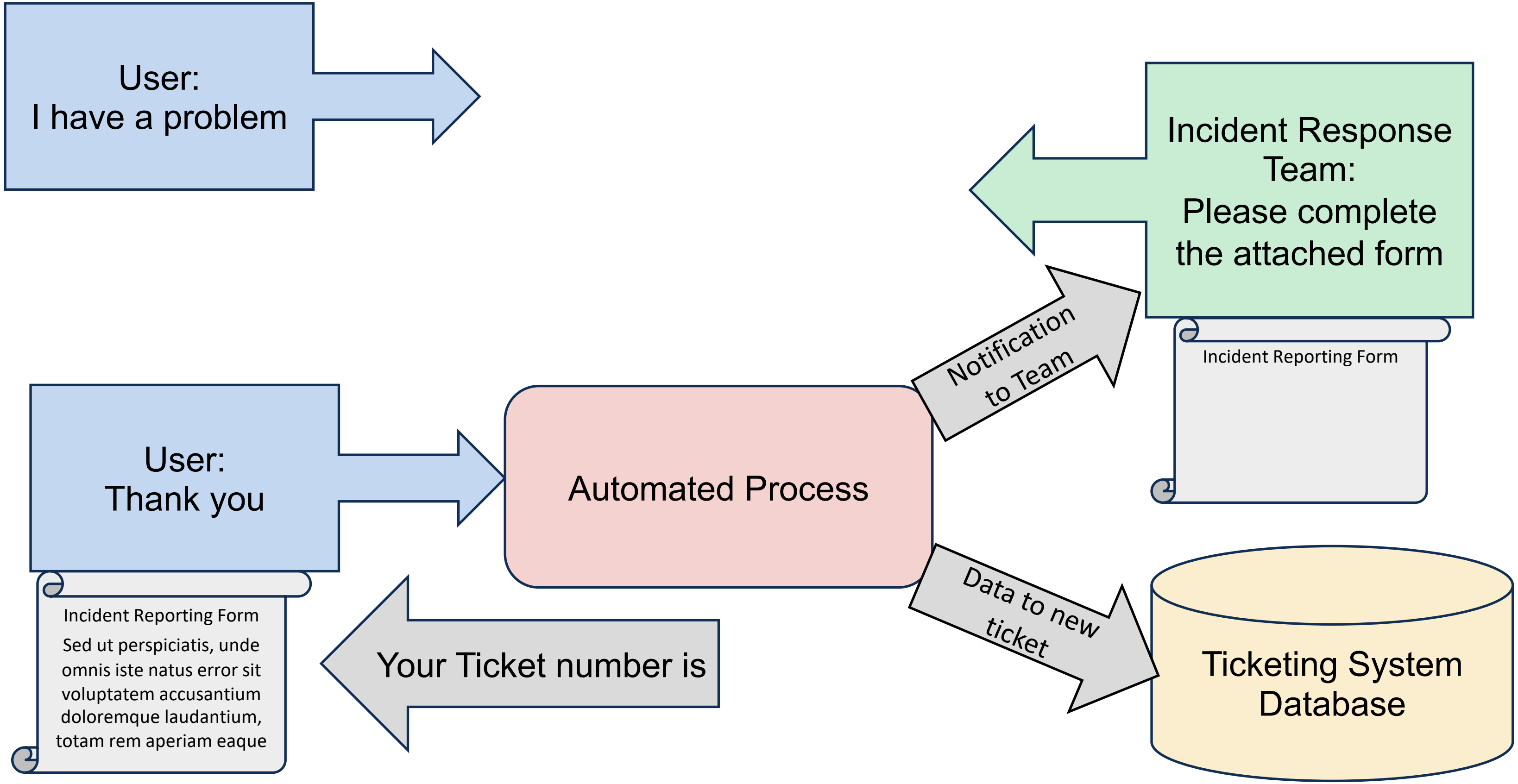
User specified

- Their format may not match yours.
  - They may not have a consistent format.
- They decide what information to include.
- Advantage (sort of): An incomplete report can be better than no report at all.

Incident response team specified

- Provide an email template with headings and spaces for the relevant data you need.
- You need to get it to the right person at the right time.
- Advantage: You have a better chance of getting the right information.

Incident Reporting by Email -3



User:
I have a problem

Incident Response Team:
Please complete the attached form

Incident Reporting Form

Notification to Team

User:
Thank you

Automated Process

Incident Reporting Form

Sed ut perspiciatis, unde omnis iste natus error sit voluptatem accusantium doloremque laudantium, totam rem aperiam eaque

Your Ticket number is

Data to new ticket

Ticketing System Database

Incident Reporting via the Web

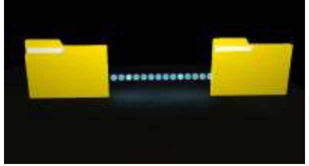
Web based forms will have the same data input requirements as other delivery mechanism.

More can be done on the front and back ends than with other media.

Be careful with **required fields**: there may be one that is considered vital, but

- The person entering the data may not have or even understand what is expected.
- This may prevent a partial form from being submitted.

Direct Transfer



Direct transfers can be

- internal from a network security device
- external from another response team

Direct Transfer – Internal -1

Incident reports can be initiated by network security devices.

Example

- Snort IDS Alerts can be brought to the attention of an incident responder who decides between
  - Create a ticket.
  - Discard and ignore.
- Snort IDS Alerts can be processed to create tickets automatically.

Direct Transfer – Internal -2

From a network security device to your ticketing system with the approval of an incident responder

Advantages

- There is a human-in-the-loop to sanity check.
- Direct transfer such as this saves considerable data entry effort.

Disadvantages

- Different individuals may decide differently.
- It still takes time for the incident responder.
- The participating devices may produce a lot of alerts.

Direct Transfer – Internal -3

Directly from a network security device to your ticketing system

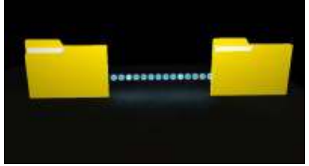
Advantages

- This is great when configured properly.
- Direct transfer such as this saves considerable data entry effort.

Disadvantages

- There is no human-in-the-loop to do a sanity check.
- There is a tendency to over-report.
- It needs to be maintained as the security device landscape changes.

Direct Transfer – External



Directly from their ticketing system to yours

Advantages

- This is great when configured properly.

Disadvantages

- A tendency is to configure it to send an incident report for **every** ticket entering their system.
- You don’t need to know that a user typed a password wrong or that their anti-virus just prevented a catastrophe.

Take the time to work with them to ensure that **relevant** data gets into your system **properly.**

How Information Gets into the Ticketing System

Manually

- if it comes in via phone or free form mail
- There probably isn’t much choice.

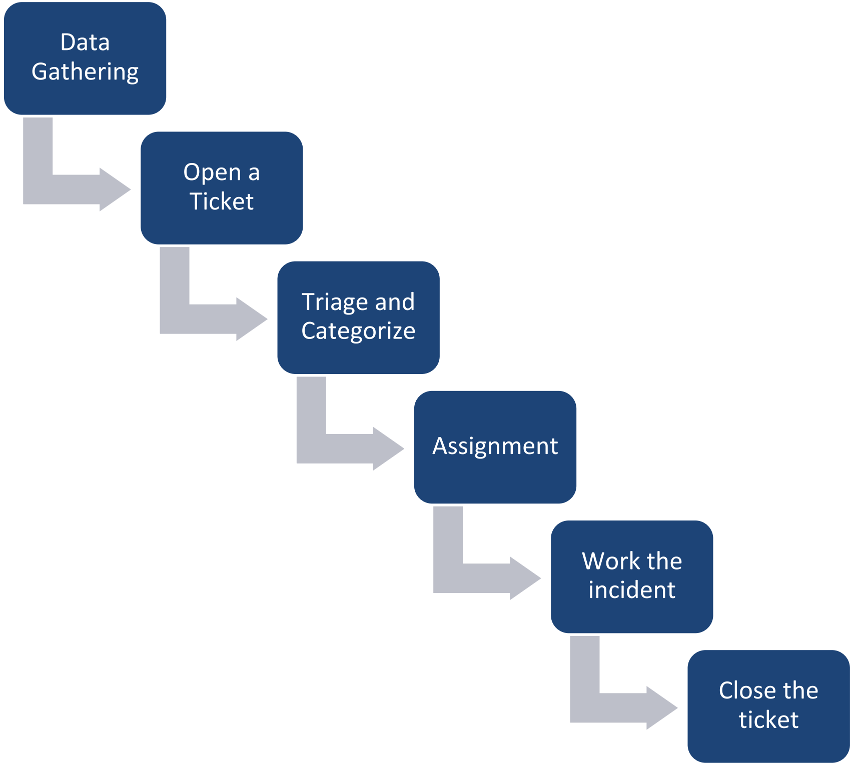
Semi-Automatically

- Automated email can do some or perhaps all.
- if the template is good

Automatically

- We’ve seen one example: direct transfer.
- web

The Lifecycle of a Ticket


Data Gathering

Open a Ticket

Triage and Categorize

Assignment

Work the incident

Close the ticket

Key Points

Triage is on the critical path for your other CSIRT services.

Triage can facilitate the prioritization and distribution of your CSIRT workload.

Use tools to support data collection, tracking, archiving, and retrieval.

Questions