Triage

Foundations of Incident Management (FIM)
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

<table>
<thead>
<tr>
<th>Category</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>CAT 0</td>
<td>Exercise/Network Defense Testing</td>
</tr>
<tr>
<td>CAT 1</td>
<td>Unauthorized Access</td>
</tr>
<tr>
<td>CAT 2</td>
<td>Denial of Service (DoS)</td>
</tr>
<tr>
<td>CAT 3</td>
<td>Malicious Code</td>
</tr>
<tr>
<td>CAT 4</td>
<td>Improper Usage</td>
</tr>
<tr>
<td>CAT 5</td>
<td>Scans/Probes/Attempted Access</td>
</tr>
<tr>
<td>CAT 6</td>
<td>Investigation</td>
</tr>
</tbody>
</table>

Prioritization

Possible criteria

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

Cyber Incident Severity Schema

The United States Federal Computer Incident Center, 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 them.

- The severity of a given incident;
- The urgency required for responding to a given incident;
- The security 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.

| Observed Component | \begin{tabular}{l|l}
\hline
Effect & Cause physical consequences \\
\hline
Prevention & Damage computer and network security \\
\hline
Engagement & Reduce or destroy data \\
\hline
Preparation & Improve availability of key systems or services \\
\hline
\end{tabular} |
|-------------------|--------------------------------------------------|

* 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
    o by you
    o 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 – Dashboards
### RT at a glance

#### 10 highest priority tickets I own

<table>
<thead>
<tr>
<th>#</th>
<th>Subject</th>
<th>Priority</th>
<th>Queue</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Office has run out of coffee!</td>
<td>0</td>
<td>Office</td>
<td>(pending 1 other ticket)</td>
</tr>
<tr>
<td>2</td>
<td>Order more coffee</td>
<td>0</td>
<td>Office</td>
<td>(pending 2 other tickets)</td>
</tr>
</tbody>
</table>

#### 10 newest unowned tickets

<table>
<thead>
<tr>
<th>#</th>
<th>Subject</th>
<th>Queue</th>
<th>Status</th>
<th>Created</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>Obtain Series-C funding</td>
<td>General</td>
<td>new</td>
<td>52 sec ago</td>
</tr>
</tbody>
</table>

#### Bookmark Tickets

<table>
<thead>
<tr>
<th>#</th>
<th>Subject</th>
<th>Priority</th>
<th>Queue</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>Evaluate responses to RFP for coffee roasts</td>
<td>0</td>
<td>Content</td>
<td>new</td>
</tr>
</tbody>
</table>

#### Quick ticket creation

- Subject: [Input Field]
- Queue: [Input Field] - [Select Option]
- Owner: [Input Field] - [Select Option]
- Requestors: [Input Field]
- Content: [Input Field]

#### My reminders

- [Empty]

#### Quick search

- Queue: [Input Field]
- Status: [Input Field]
- Created: [Input Field]

#### Dashboards

- RT System's dashboards: [Subscription]
- SLA Performance: [Daily at 6:00 AM]

#### Refresh

- Don't refresh this page: [Input Field] - [Refresh]
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

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)

<table>
<thead>
<tr>
<th>Indicator</th>
<th>Trend</th>
<th>W1 2015</th>
<th>W2 2015</th>
<th>W3 2015</th>
<th>W4 2015</th>
<th>W5 2015</th>
<th>Score</th>
<th>Target</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of open incidents</td>
<td></td>
<td>951</td>
<td>954</td>
<td>1,026</td>
<td>713</td>
<td>587</td>
<td>555</td>
<td>600</td>
</tr>
<tr>
<td>% of incidents resolved by first assigned group</td>
<td></td>
<td>95.60%</td>
<td>95.99%</td>
<td>97.41%</td>
<td>98.02%</td>
<td>98.35%</td>
<td>98.57%</td>
<td>95.00%</td>
</tr>
<tr>
<td>% of open incidents not updated in last 5 days</td>
<td></td>
<td>25.04%</td>
<td>26.75%</td>
<td>26.77%</td>
<td>23.48%</td>
<td>36.10%</td>
<td>52.61%</td>
<td>35.00%</td>
</tr>
<tr>
<td>% of open incidents not updated in last 30 days</td>
<td></td>
<td>11.19%</td>
<td>11.49%</td>
<td>11.81%</td>
<td>13.27%</td>
<td>19.26%</td>
<td>31.23%</td>
<td>12.50%</td>
</tr>
</tbody>
</table>
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
    o local online form
    o directly into the ticketing system
    o pre-printed list of questions and space for answers
    o (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

<table>
<thead>
<tr>
<th>Phonetic Alphabet</th>
<th>Phonetic Alphabet</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>Alpha</td>
</tr>
<tr>
<td>B</td>
<td>Bravo</td>
</tr>
<tr>
<td>C</td>
<td>Charlie</td>
</tr>
<tr>
<td>D</td>
<td>Delta</td>
</tr>
<tr>
<td>E</td>
<td>Echo</td>
</tr>
<tr>
<td>F</td>
<td>Foxtrot</td>
</tr>
<tr>
<td>G</td>
<td>Golf</td>
</tr>
<tr>
<td>H</td>
<td>Hotel</td>
</tr>
<tr>
<td>I</td>
<td>India</td>
</tr>
<tr>
<td>J</td>
<td>Juliet</td>
</tr>
<tr>
<td>K</td>
<td>Kilo</td>
</tr>
<tr>
<td>L</td>
<td>Lima</td>
</tr>
<tr>
<td>M</td>
<td>Mike</td>
</tr>
<tr>
<td>N</td>
<td>November</td>
</tr>
<tr>
<td>O</td>
<td>Oscar</td>
</tr>
<tr>
<td>P</td>
<td>Papa</td>
</tr>
<tr>
<td>Q</td>
<td>Quebec</td>
</tr>
<tr>
<td>R</td>
<td>Romeo</td>
</tr>
<tr>
<td>S</td>
<td>Sierra</td>
</tr>
<tr>
<td>T</td>
<td>Tango</td>
</tr>
<tr>
<td>U</td>
<td>Uniform</td>
</tr>
<tr>
<td>V</td>
<td>Victor</td>
</tr>
<tr>
<td>W</td>
<td>Whiskey</td>
</tr>
<tr>
<td>X</td>
<td>X-ray</td>
</tr>
<tr>
<td>Y</td>
<td>Yankee</td>
</tr>
<tr>
<td>Z</td>
<td>Zulu</td>
</tr>
</tbody>
</table>
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 Reporting Form
Sed ut perspiciatis, unde omnis iste natus error sit voluptatem accusantium doloremque laudantium, totam rem aperiam eaque

Incident Response Team: Please complete the attached form

Notification to Team

Automated Process

Your Ticket number is

Ticketing System Database

Data to new ticket

User: Thank you
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
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

1. Data Gathering
2. Open a Ticket
3. Triage and Categorize
4. Assignment
5. Work the incident
6. 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