EUROPEAN UNION

EXPERTISE FRANCE

Projet financé par l'Union Européenne

Projet mis en œuvre par Expertise France

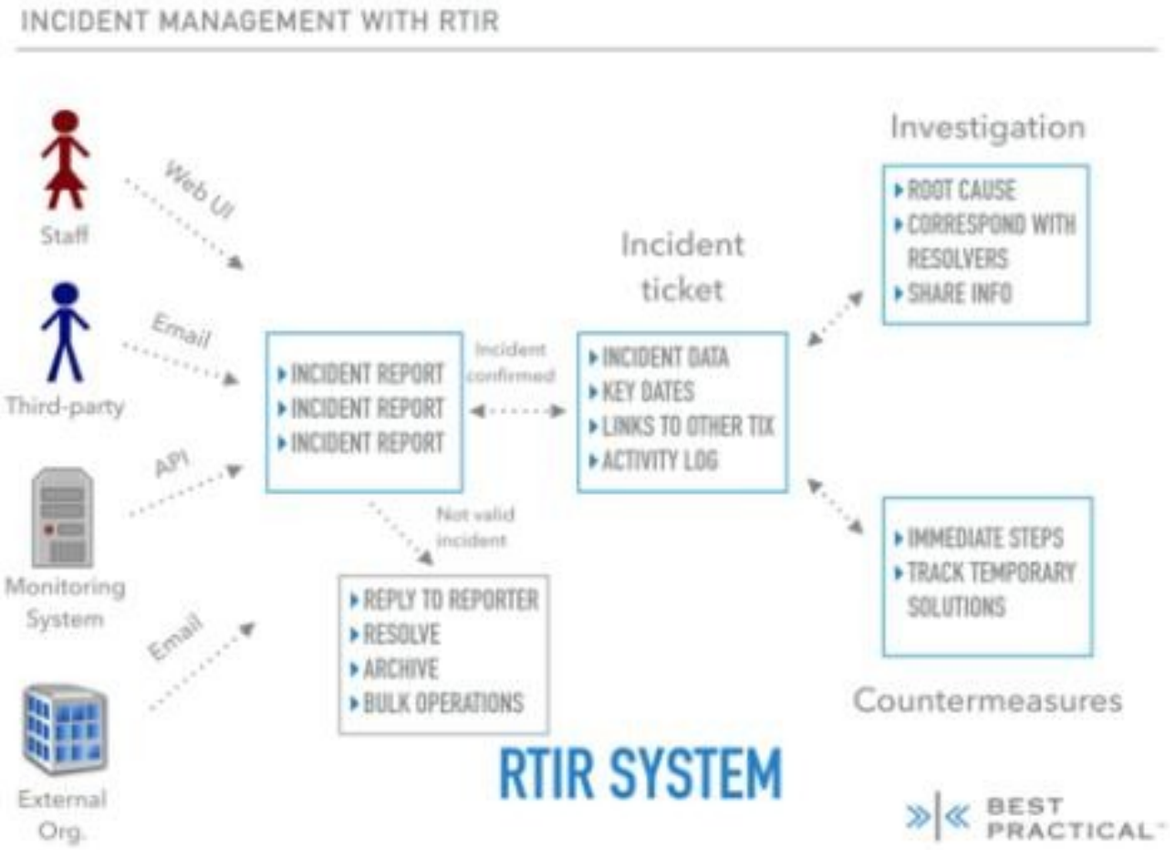
Basics of a CSIRT: Software Environment
RTIR: Installing RTIR

Accra, Ghana, ** August 2021

Index

Request Tracker Incident Response (RTIR)

- Builds on all the features of RT and provides pre-configured queues and workflows designed for incident response teams.
- Open Source solution built on Perl
- Has tools to correlate key data from incident reports, both from people and automated tools, to find patterns and link multiple incident reports with a common root cause incident.
- Manage communication to multiple interested parties including reporters, counterparts at other security teams collaborating on responses, and other internal teams coordinating countermeasures.
- Incident Management workflow-integrated, allowing for effective triage and the creation of tickets



Building the Application Vs Running Docker Images

RTIR can be installed and configured manually by using Perl either within a standalone environment on a server or through Docker

Building the application in a standalone environment requires the installation of MySQL and NGINX concurrently with the installation of RTIR

Building the application through Docker removes the requirement to manually install and configure MySQL and NGINX – assuming that the application has a Docker file which contains commands that will automatically create and configure MySQL and NGINX

Building the Application Vs Running Docker Images

A Docker image is a simple, easy and much faster method of installing, developing, testing, then running applications through Docker.

Images are created by the developer community and placed on Github or Dockerhub.

Only a few commands are required to pull the docker image from the repository and run it through Docker.

The image can then be configured within your Docker environment and saved to your own Docker repository.

Building the Application Vs Running Docker Images

What is best? … it depends on your overall requirements:

- **Request Tracker and Request Tracker Incident Response are very difficult to intall and configure within a standalone environment**
- **Configuration of security for the application, communication channels take a significantly long time**
- **Reducing that time slightly by pulling Docker images is one solution**

But... RTIR is not an out-of-the-box solution, it is open-source, not well-supported because of this, and requires users to have a good understanding of Perl

Build the Application

We will build the application through Docker, using a docker file.

First, we need to clone the repository:

```
$ sudo git clone https://github.com/dlee35/docker-rtir
```

Build the Application

Next, we need to change the directory to the cloned repository:

```
$ cd ~\Downloads
```

Build the Application

Now, we will build the application:

```
$ sudo docker build docker-rtir
```

While We Wait…

Add the GPG key for the official Docker repository to your system

```
$ curl -fsSL https://download.docker.com/linux/ubuntu/gpg |
sudo apt-key add -
```

Alerts, Warnings and Announcements

Step 1: Collecting Vulnerability Information

- Usually there exist two main types of information sources that contribute information as input for the services:
  - Vulnerability information about (your) IT systems
  - Incident reports
- Depending of the kind of business and IT infrastructure there are many public and closed sources for vulnerability information:
  - Public and closed mailing lists
  - Vendor vulnerability product information
  - Websites
  - Information on the Internet (Google, etc…)
  - Public and private partnerships that provide vulnerability information (FIRST, TFCSIRT, CERT-CC, US-CERT….)

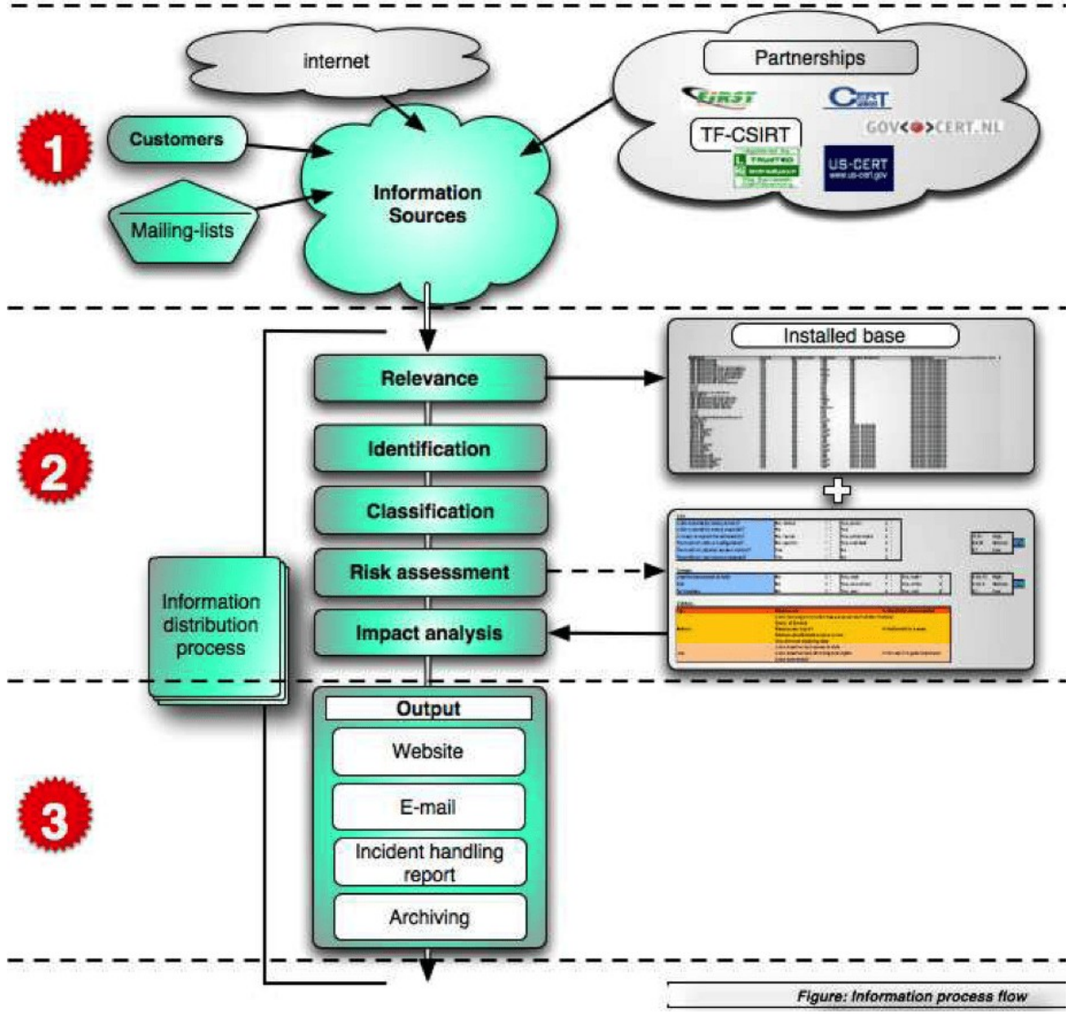


Figure: Information process flow

Alerts, Warnings and Announcements

Step 2: Evaluation of Information and Risk Assessment

- Identification:
  - Source trustworthiness
  - Reliability of Information
  - Prevents false alerts from being distributed
- Relevance:
  - Does the information indicate a threat to systems listed within the Constituency Installation Base?
- Classification:
  - Does the information require special handling conditions? If so, how do you communicate it?

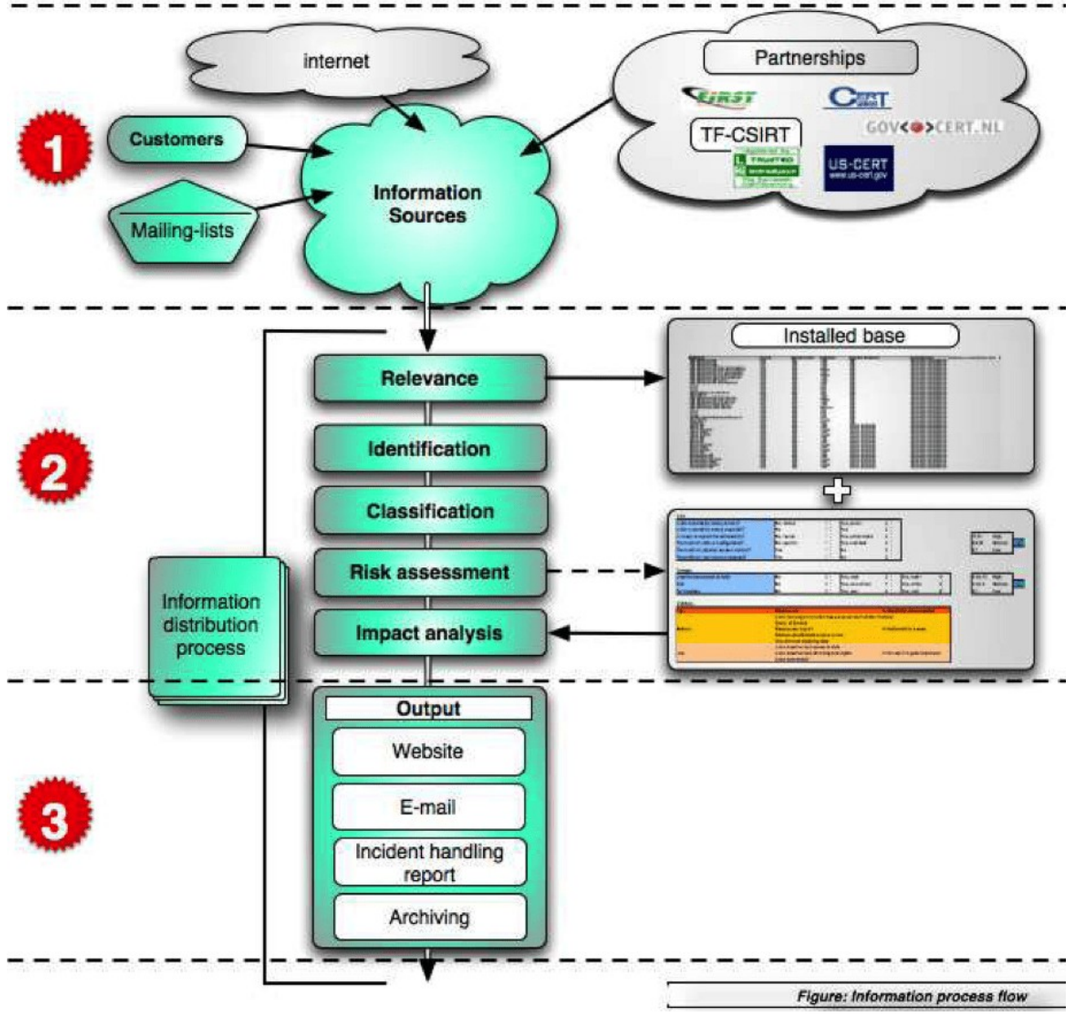


Figure: Information process flow

Alerts, Warnings and Announcements

Step 2: Evaluation of Information and Risk Assessment (Continued)

- Open-ended methods to analysing information in order to determine the risk and [potential] impact of a vulnerability

- Defining Risk:

  - Potential chance that a vulnerability can be exploited

    - Is the vulnerability well-known?
    - Is the vulnerability wide-spread?
    - Is it easy to exploit the vulnerability?
    - Is it a remotely exploitable vulnerability?

- Defining Threat

  - The possibility of a malicious attempt to damage or disrupt networks and / or systems

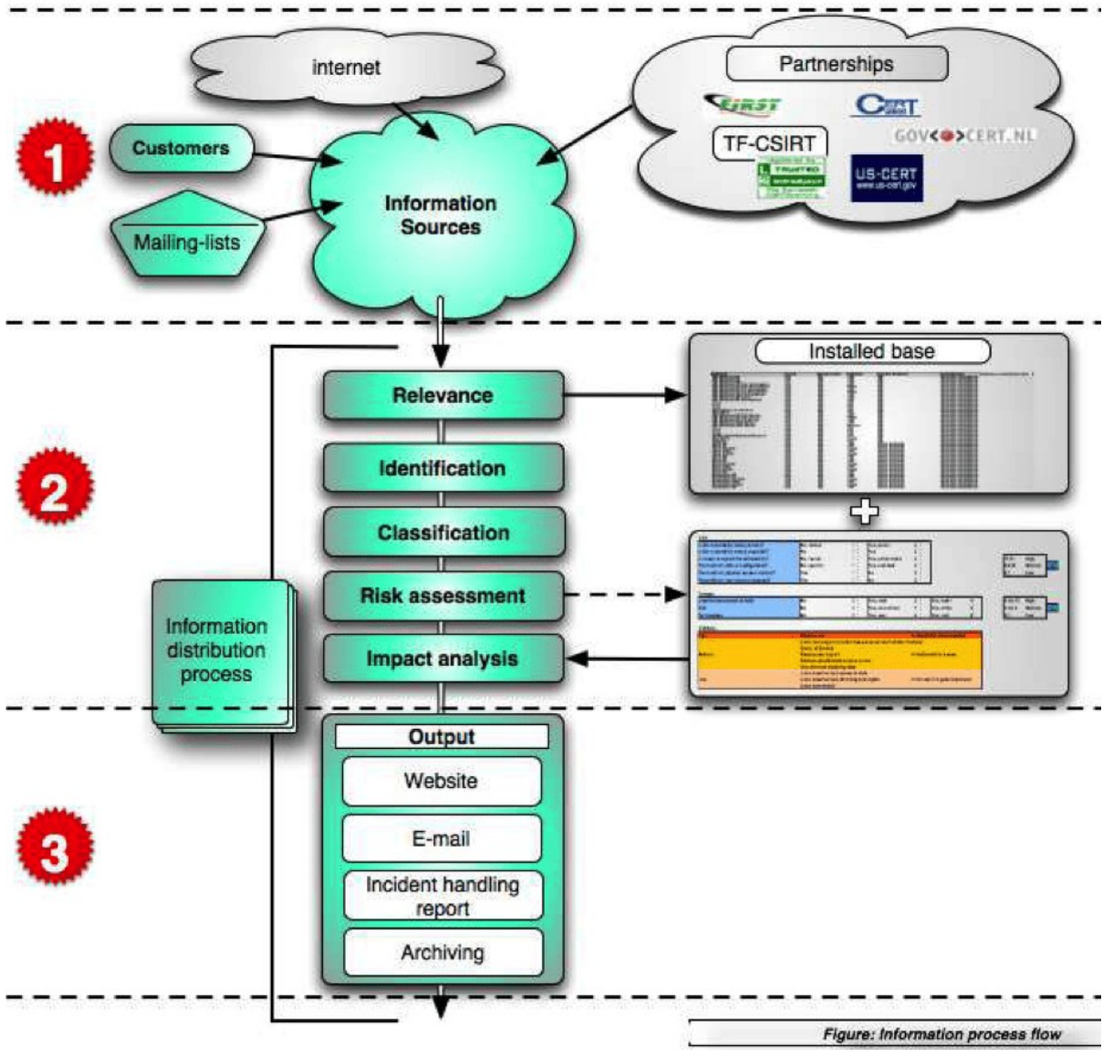


Figure: Information process flow

Alerts, Warnings and Announcements

Step 2: Evaluation of Information and Risk Assessment (Continued)

- Classifying Risks / Threats
  - Low
  - Medium
  - High
  - Severe

RISK

Is the vulnarability widely known?	No, limited	1	Yes, public	2
Is the vulnarability widely exploited?	No	1	Yes	2
Is it easy to exploit the vulnerability?	No, hacker	1	Yes, script kiddie	2
Precondition: default configuration?	No. specific	1	Yes, standard	2
Precondition: physical access required?	Yes	1	No	2
Precondition: user account required?	Yes	1	No	2

11,12	High	
8,9,10	Medium	0
6,7	Low	

Damage

Unauthorized access to data	No	0	Yes, read	2	Yes, read +	4
DoS	No	0	Yes, non-critical	1	Yes, critica	5
Permissions	No	0	Yes, user	4	Yes, root	6

6 t/m 15	High	
2 t/m 5	Medium	0
0,1	Low	

OVERALL

High	Remote root	>> Imediately action needed!
Medium	Local root exploit (attacker has a user account on the machine) Denial of Service Remote user exploit Remote unauthorized access to data Unauthorized obtaining data	>> Action within a week
Low	Local unauthorized access to data Local unauthorized obtaining user-rights Local user exploit	>> Include it in general process

Alerts, Warnings and Announcements

Procedure on how to identify the authenticity of a message and its source

General Checklist

1. Is the source known and registered as such?
2. Does the information come via a regular channel?
3. Is there “strange” information contained that “feels” wrong?
4. Follow your feeling, there’s doubt about an information don’t act but verify again!

E-Mail - Sources

1. Is the source address known to the organisation and known to the source list?
2. Is the PGP-signature correct?
3. When in doubt check the full headers of a message.
4. When in doubt use “nslookup” or ”dig” to verify the senders domain[20].

WWW - Sources

1. Check browser certificates when connecting to a secured website (https ://).
2. Check source on content and validity (technical).
3. When in doubt, don’t click any links or download any software.
4. When in doubt have a “lookup” and “dig” done on the domain and do a “traceroute”.

Telephone

1. Listen carefully to the name.
2. Do you recognise the voice?
3. When in doubt ask for a telephone number and request to call back the caller.

Alerts, Warnings and Announcements

Step 3: Distribution of Information

- Several methods dependent on constituent preferences:
  - Website
  - Email
  - Report
  - Archiving and research
- Advisories should always follow same structure and be presented in a clear and concise fashion

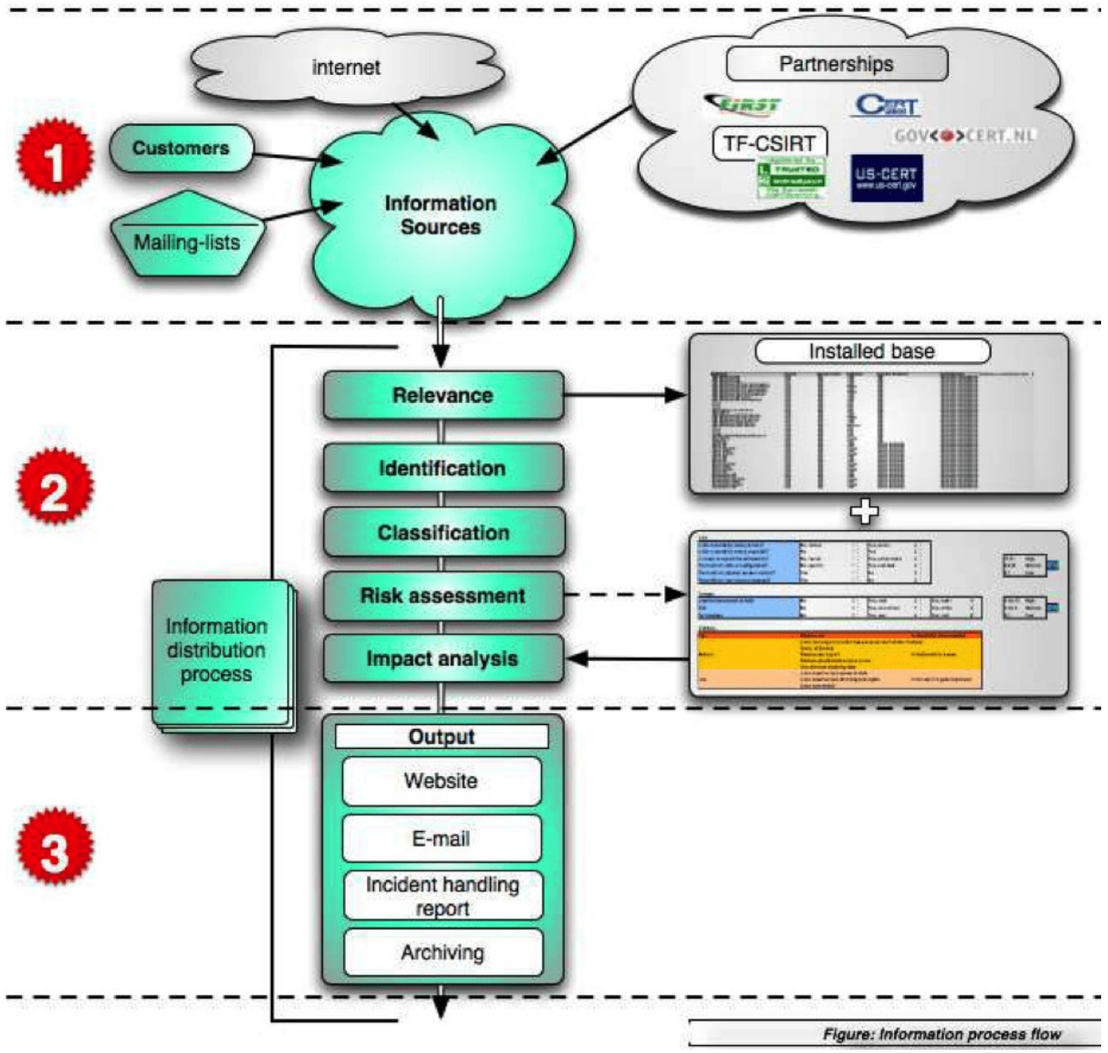


Figure: Information process flow

Alerts, Warnings and Announcements

Title of the advisory

.....

Reference number

.....

Systems affected

- .....
- .....

Related OS + version

.....

Risk (High-Medium-Low)

.....

Impact/potential damage (High-Medium-Low)

.....

External id's: (CVE, Vulnerability bulletin ID's)

.....

Overview of vulnerability

.....

Impact

.....

Solution

.....

Description (details)

.....

Appendix

.....

Alerts, Warnings and Announcements

Step 3: Distribution of Information (Continued)

- Incident handling
  - Same process used when generating and distributing alerts, warnings and announcements
  - Information-gathering phase is very different
    - Incident reports
    - Telephone call
    - Summary Email

  - Capture all information
  - Generate and issue incident number

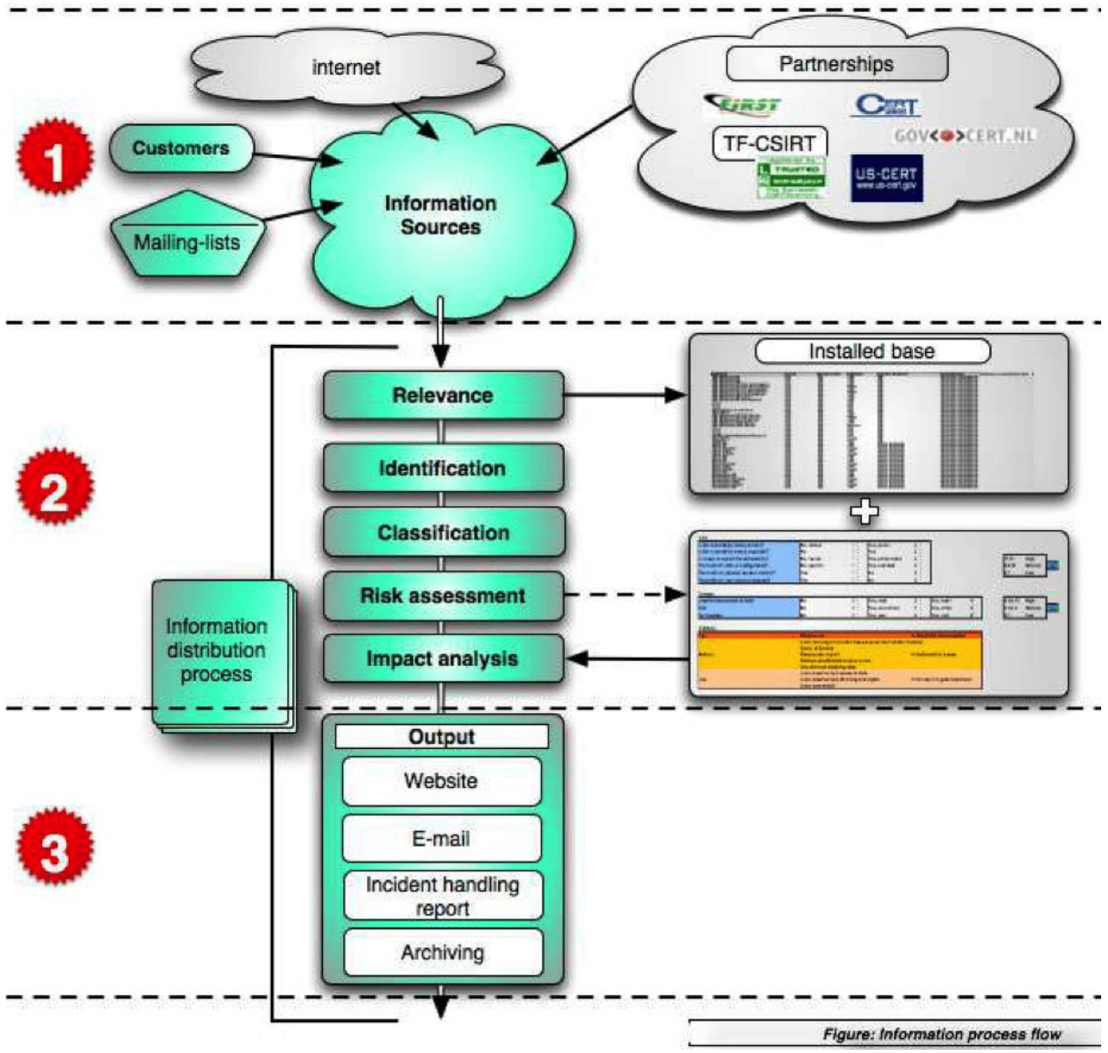


Figure: Information process flow

Incident Handling

- Same process used when generating and distributing alerts, warnings and announcements
- However, the information-gathering phase is very different. It consists of receiving information by the following means:
  - Incident reports
  - Telephone call
  - Summary Email
- The CSIRT must initially ensure the following is adhered to:
  - Capture all information
  - Generate and issue incident number

Alerts, Warnings and Announcements Vs Incident Handling

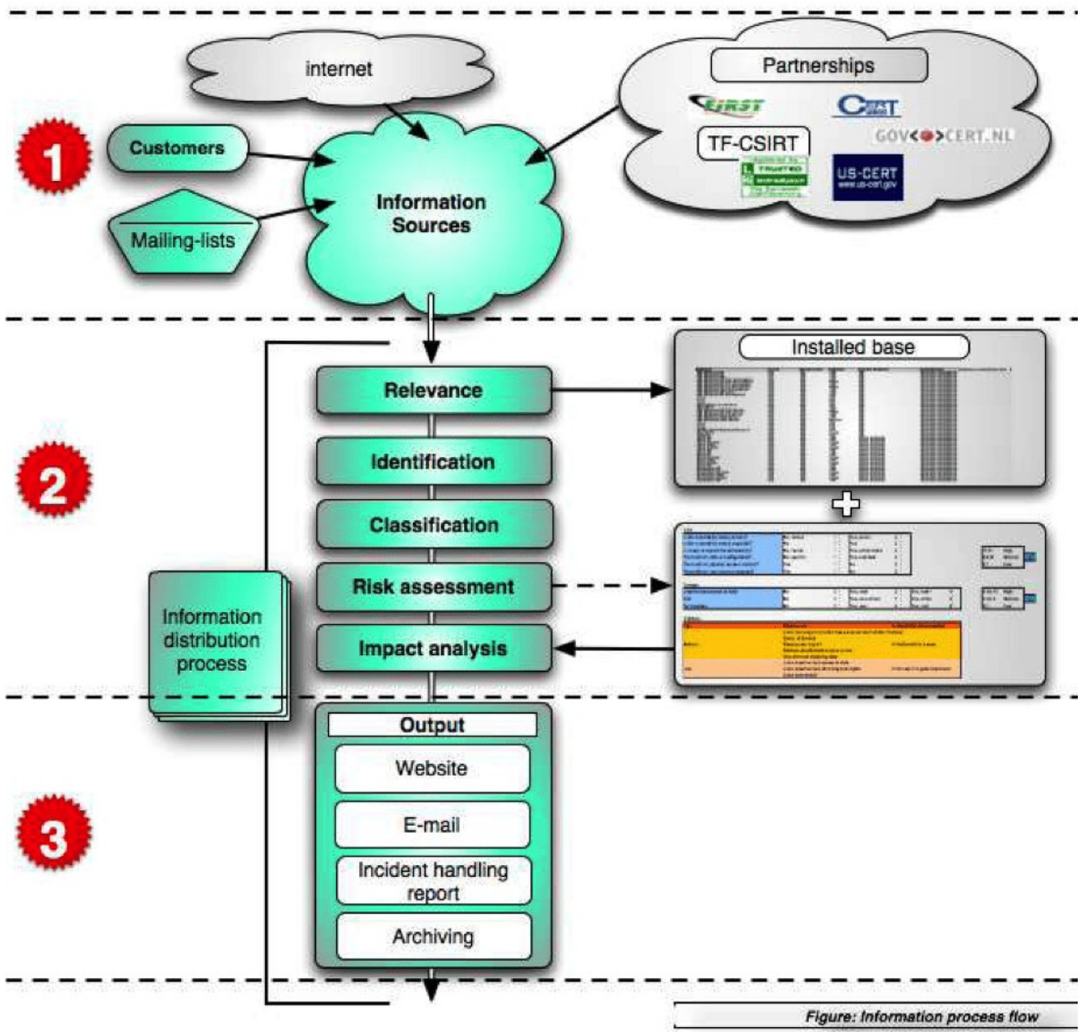


Figure: Information process flow

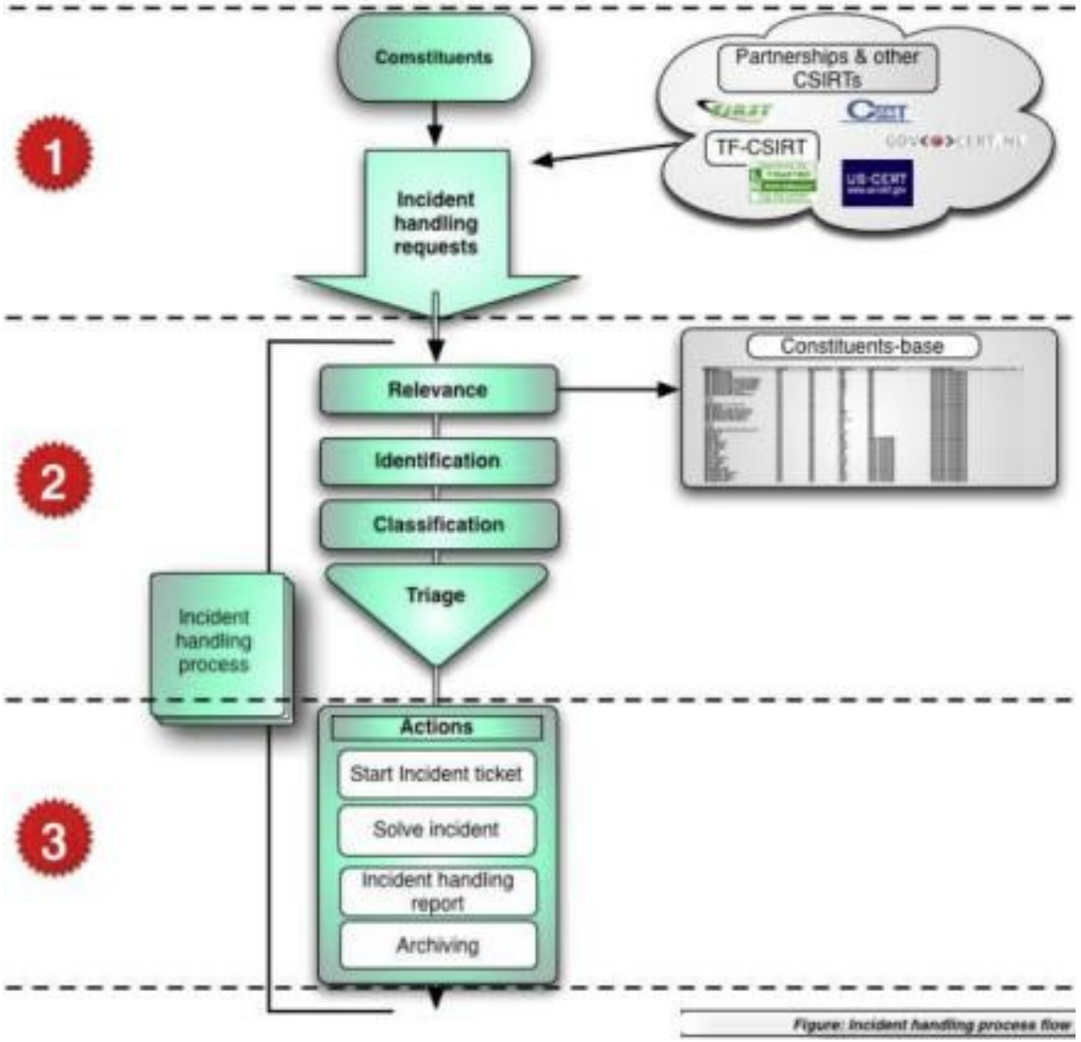


Figure: Incident handling process flow

Incident Handling

Step 1: Receiving Incident Reports

- A range of communication channels used to receive incident reports:
  - Email (Most preferred)
  - Telephone
  - Fax
- Immediate task is to obtain a thorough understanding of the incident within a set format – Incident Reporting Form containing the following headings:
  - Name and Organisation
  - Affected Host(s)
  - Incident

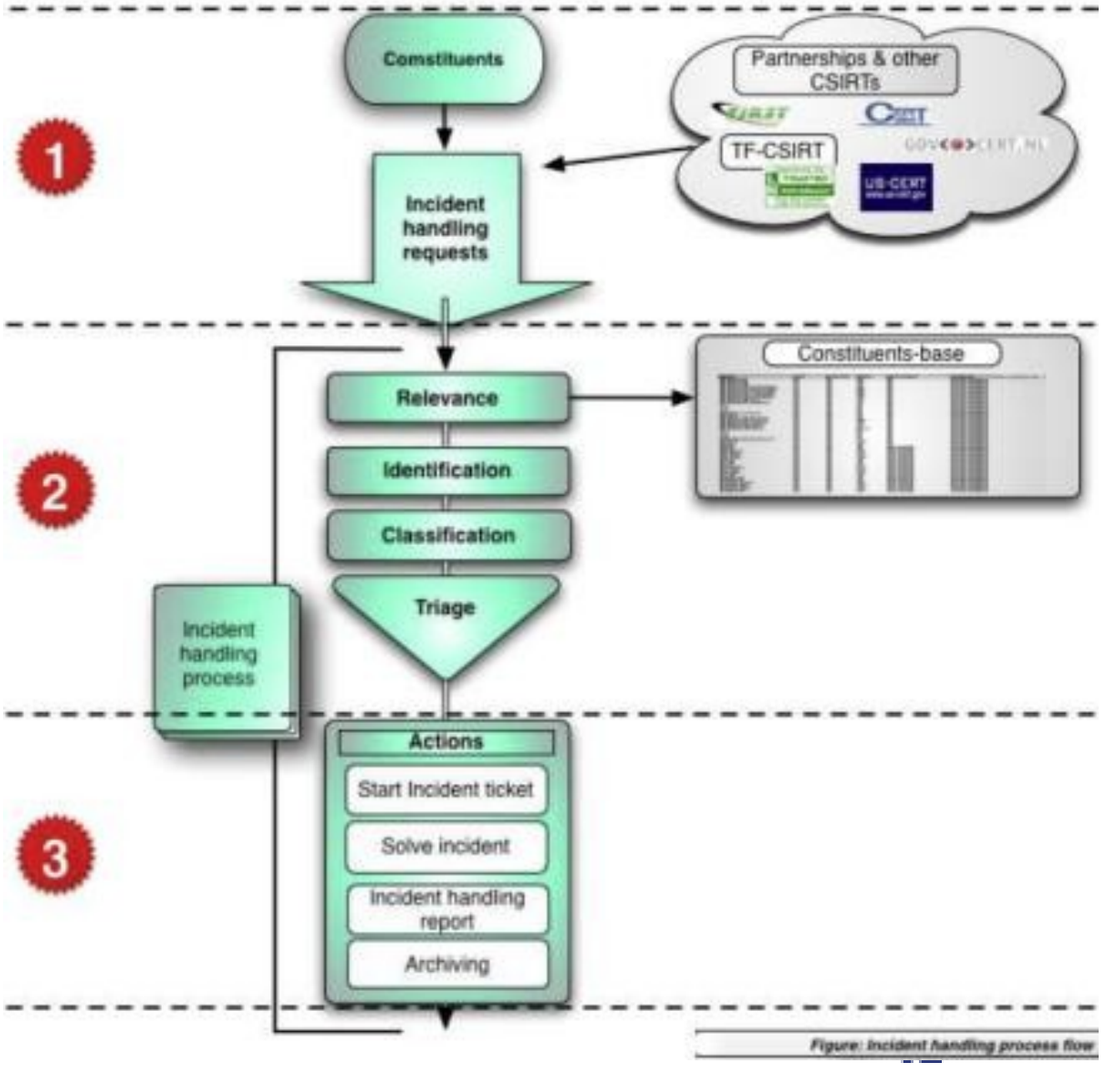


Figure: Incident handling process flow

Incident Handling

INCIDENT REPORTING FORM

Please fill out this form and Fax or email it to: ……..
*Lines marked with * are required.*

Name and Organisation
1. Name*:
2. Name of Organisation*:
3. Sector type:
4. Country*:
5. City:
6. E-Mail address*:
7. Telephone number*:
8. Other:

Affected Host(s)
9. Number of Hosts:
10. Hostname & IP*:
11. Function of the Host*:
12. Time-Zone:
13. Hardware:
14. Operating System:
15. Affected Software:
16. Affected Files:
17. Security:
18. Hostname & IP:
19. Protocol/port:

Incident
20. Reference number ref #:
21. Type of Incident:
22. Incident Started:
23. This is an ongoing incident: YES NO
24. Time and Method of Discovery:
25. Known Vulnerabilities:
26. Suspicious Files:
27. Countermeasures:
28. Detailed description*:

Incident Handling

Step 2: Incident Evaluation

- Identify the originator of the Incident Report:
  - Verify the trustworthiness of the originator
  - Verify whether the originator is a constituent or an associate
- Determine the relevance of the incident:
  - Identify whether the incident involves the originator or a system associated to the constituency
  - If not, the report is re-routed to the SOC
- Classification of the incident:
  - Assess the severity of the incident by applying a triage system.

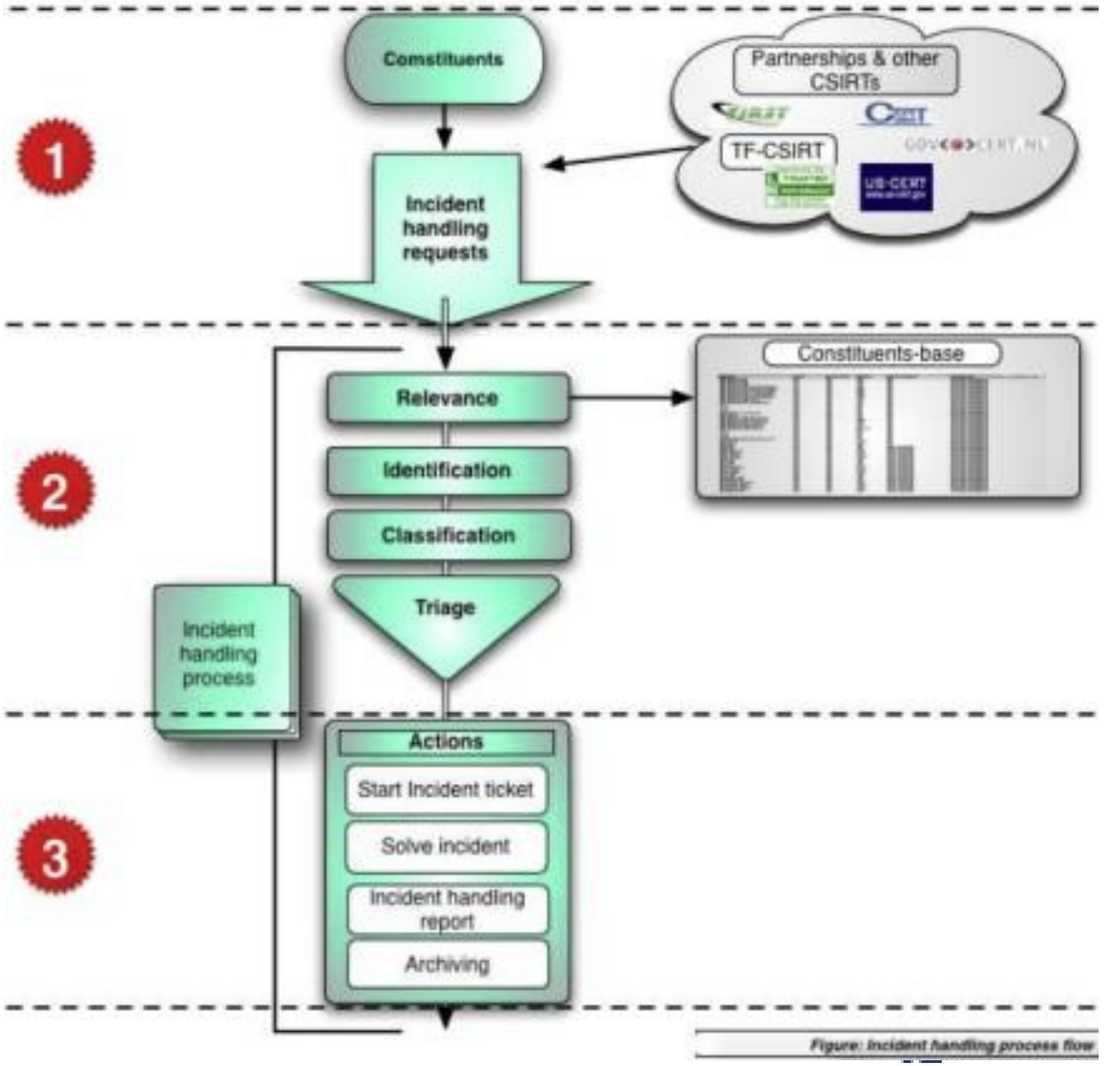


Figure: Incident handling process flow

Incident Handling

Incident Category	Sensitivity*	Description
Denial of service	S3	• DOS or DDOS attack.
Forensics	S1	• Any forensic work to be done by CSIRT.
Compromised Information	S1	• Attempted or successful destruction, corruption, or disclosure of sensitive corporate information or Intellectual Property.
Compromised Asset	S1, S2	• Compromised host (root account, Trojan, rootkit), network device, application, user account. This includes malware-infected hosts where an attacker is actively controlling the host.
Unlawful activity	S1	• Theft / Fraud / Human Safety / Child Porn. Computer-related incidents of a criminal nature, likely involving law enforcement, Global Investigations, or Loss Prevention.
Internal Hacking	S1, S2, S3	• Reconnaissance or Suspicious activity originating from inside the Company corporate network, excluding malware.
External Hacking	S1, S2, S3	• Reconnaissance or Suspicious Activity originating from outside the Company corporate network (partner network, Internet), excluding malware.
Malware	S3	• A virus or worm typically affecting multiple corporate devices. This does not include compromised hosts that are being actively controlled by an attacker via a backdoor or Trojan. (See Compromised Asset)
Email	S3	• Spoofed email, SPAM, and other email security-related events.
Consulting	S1, S2, S3	• Security consulting unrelated to any confirmed incident.
Policy Violations	S1, S2, S3	• Sharing offensive material, sharing/possession of copyright material. • Deliberate violation of Infosec policy. • Inappropriate use of corporate asset such as computer, network, or application. • Unauthorized escalation of privileges or deliberate attempt to subvert access controls.
* - Sensitivity will vary depending on circumstances. Guidelines are provided.		

Incident Handling

Step 3: Actions

- Triaged incidents will be processed through a queue within an incident handling tool. The CSIRT will follow this process:
  - Start Incident Ticket
  - Incident Lifecycle Process:
    - Analysis
    - Obtain contact information
    - Provide technical assistance
    - Coordination
  - Produce and distribute Incident Handling Report:
  - Archiving

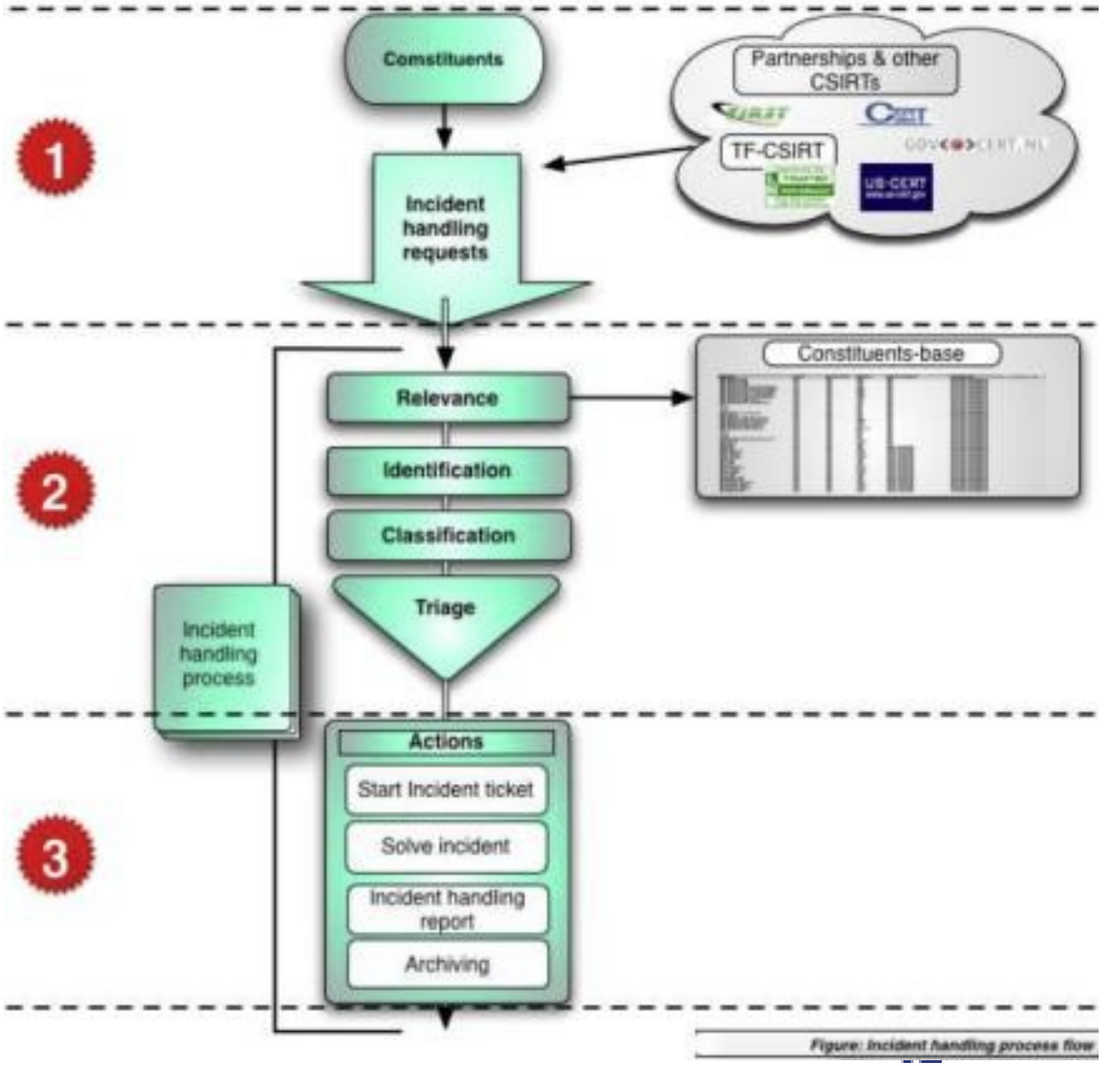


Figure: Incident handling process flow

Running the Docker Image

With RTIR built via Docker on our server, it can now be run.

However, another way that we can pull and run Docker images is by invoking the following command in our terminal:

```
$ sudo docker pull dlee35/docker-rtir
```

Running the Docker Image

RTIR has now been pulled from Dockerhub and is now ready to be run by invoking the following command:

```
$ sudo docker run -d -p 443:443 --name rtir dlee35/docker-rtir
```

Options

```
-d = Detached mode, runs the container in the background
-p = Opens and publishes the indicated ports ‘443:443’ for the container
--name = Assigns a name to the container ‘rtir’
```

Running the Docker Image

RTIR is now running on your allocated subdomain on port 443

```
[yoursubdomain].cyberresponse.africa:443
```

Native admin user credentials:

Username: user
Password: root

Thank you

Contact:

Joseph Jones,

Founder, Strategy Nord and OS2INT

Senior Advisor, Paliscope

https://www.linkedin.com/in/josephstrategynord/

OCWAR-C

12 Charles de Gaulle Street Asokoro,

Abuja - NIGERIA

contact@ocwarc.eu