Incident Management

Definition

Computer Security Incident

“Any real or suspected adverse event in relation to the security of computer system or computer networks”

- (According to ‘CIRT FAQ’) in CERT/CC

A single or a series of unwanted or unexpected computer security events that have a significant probability of compromising business operations and threatening cybersecurity.

- ISO Definition

2


There are no standard types for security Incidents!
CYBER
ATTACK
SPAM
THEFT
BOT
ROUTE
SMURF
SPYWARE
RELAY
SOCIAL
SLIPPING
BIRTHDAY
PATCHING
ENGINEERING
RETURN
FLOOD
BRUTE
CACHE
STACK
EXPLOIT
HACKING
SKIMMING
PROBE
PHARMING
VIRUS
SYN
OVERFLOW
FRAUD
TROJAN
ZERO-DAY
SOCIAL-ENGINEERING
SCAN
SQL
WORM
DOS
SPOOFING
IDENTITY
HEAP
BUFFER
DDOS
BULLYING
MALWARE
INJECTION

3

Incident samples

Scan activity to firewall servers	Web defacement
Information leakage	Phishing sites
Compromised server	Espionage
Intrusion	DoS / DDoS attacks
Use of proxy server as open proxy	SMTP relay
Virus infection	SPAM
Laptop Theft	Malware distribution
Botnet and C&C	One-Click Fraud
Identity Theft	Unauthorized Access

4

Incident response

Process of addressing computer security incidents

- Observe system for unexpected behaviour or anything suspicious
- Investigate anything considered unusual
- If the investigation finds something that isn't explained by authorized activity, immediately initiate response procedures

5

Need for incident response

Even the most vigilant, secure organizations can come up against acts of fraud, theft, computer intrusions, and other computer security incidents.

Without up-front planning for Incident Response, it is much more difficult to recover from an incident.

6

Policies and procedures

Established procedures must be in place to:

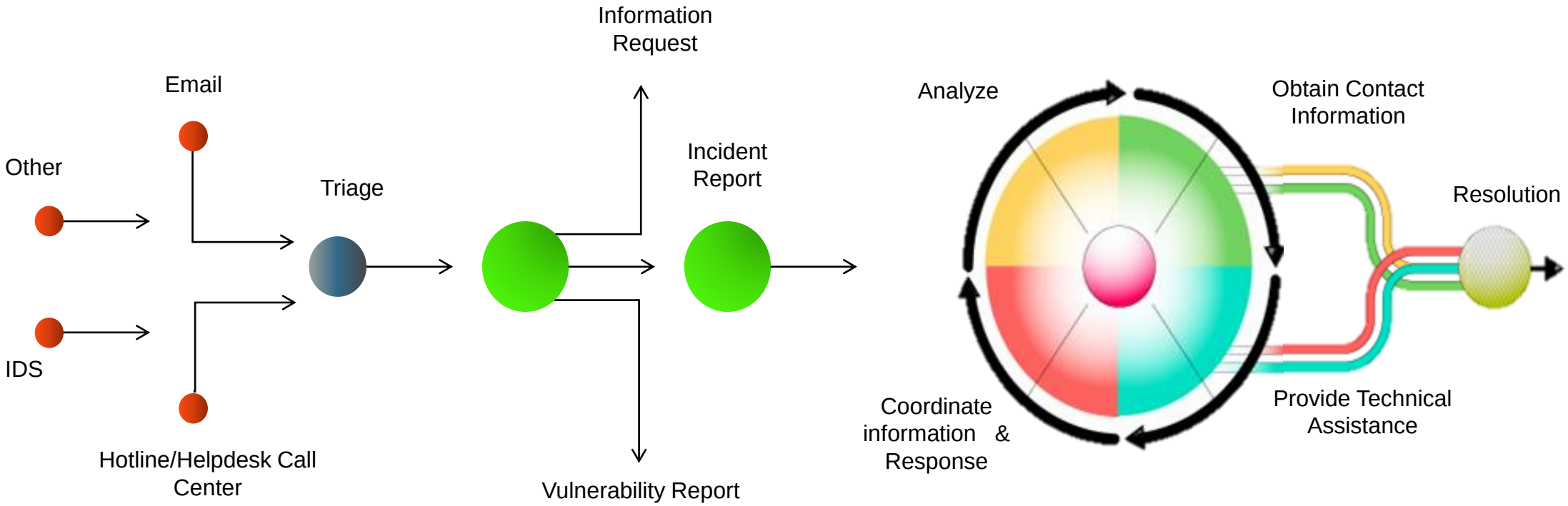
- ❑ Detect & identify the attack
- ❑ Mitigate the damage
- ❑ Recover from the attack

Without a formal process in place critical information may be lost

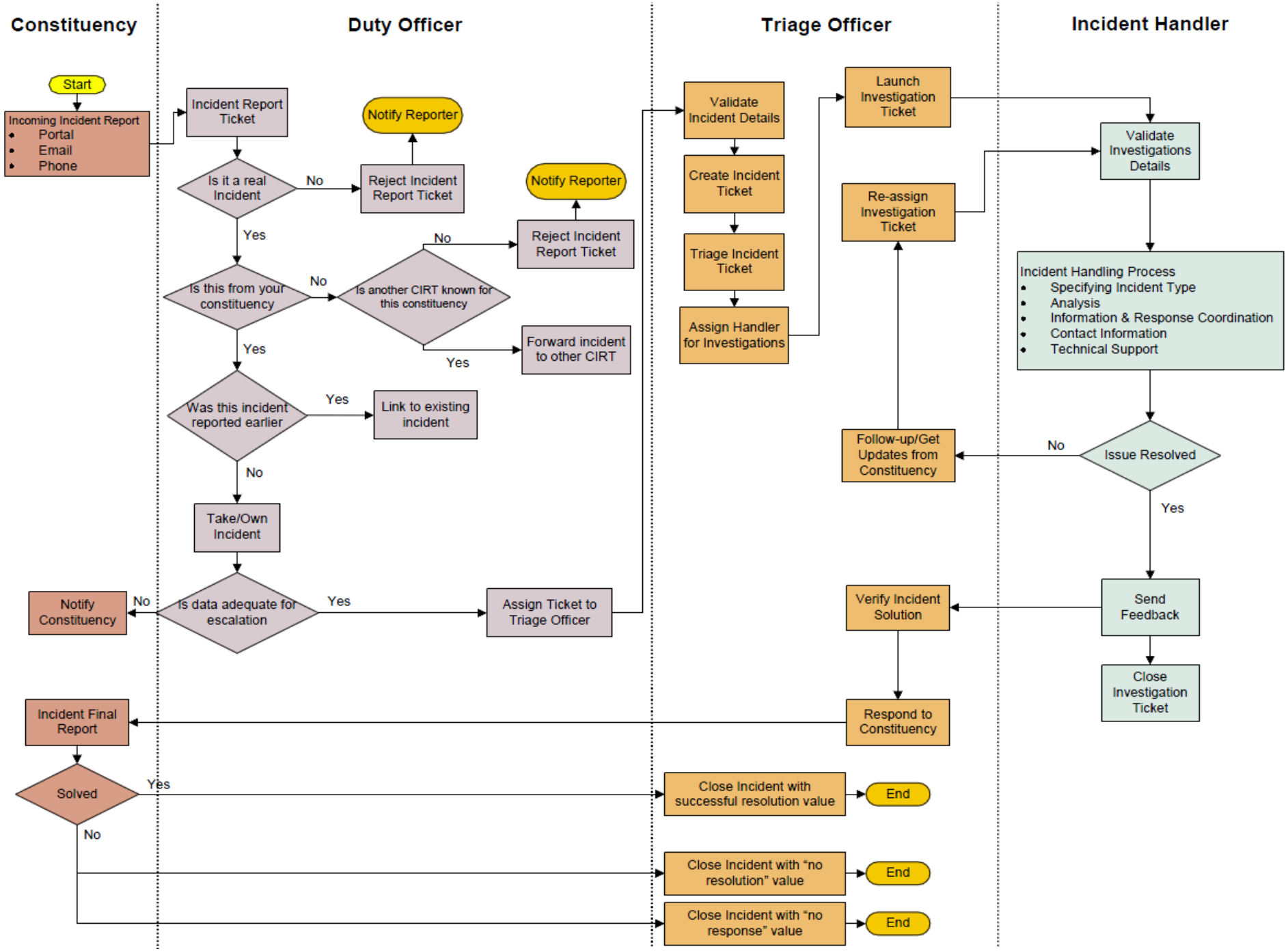
These procedures used in incident response can be thought of as the incident handling life cycle.

7

Incident handling life cycle



Source: CERT/CC Incident Handling Life Cycle in CERT/CC "Handbook for Computer Incident Response Teams (CIRTs)


Constituency
Duty Officer
Triage Officer
Incident Handler
Start
Incoming Incident Report
Portal
Email
Phone
Incident Report Ticket
Is it a real Incident
No
Reject Incident Report Ticket
Notify Reporter
Yes
Is this from your constituency
No
Is another CIRT known for this constituency
No
Reject Incident Report Ticket
Notify Reporter
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

9

Sample objectives

Provide support for recovering from and dealing with incidents

Provide technical support in response to computer security incidents

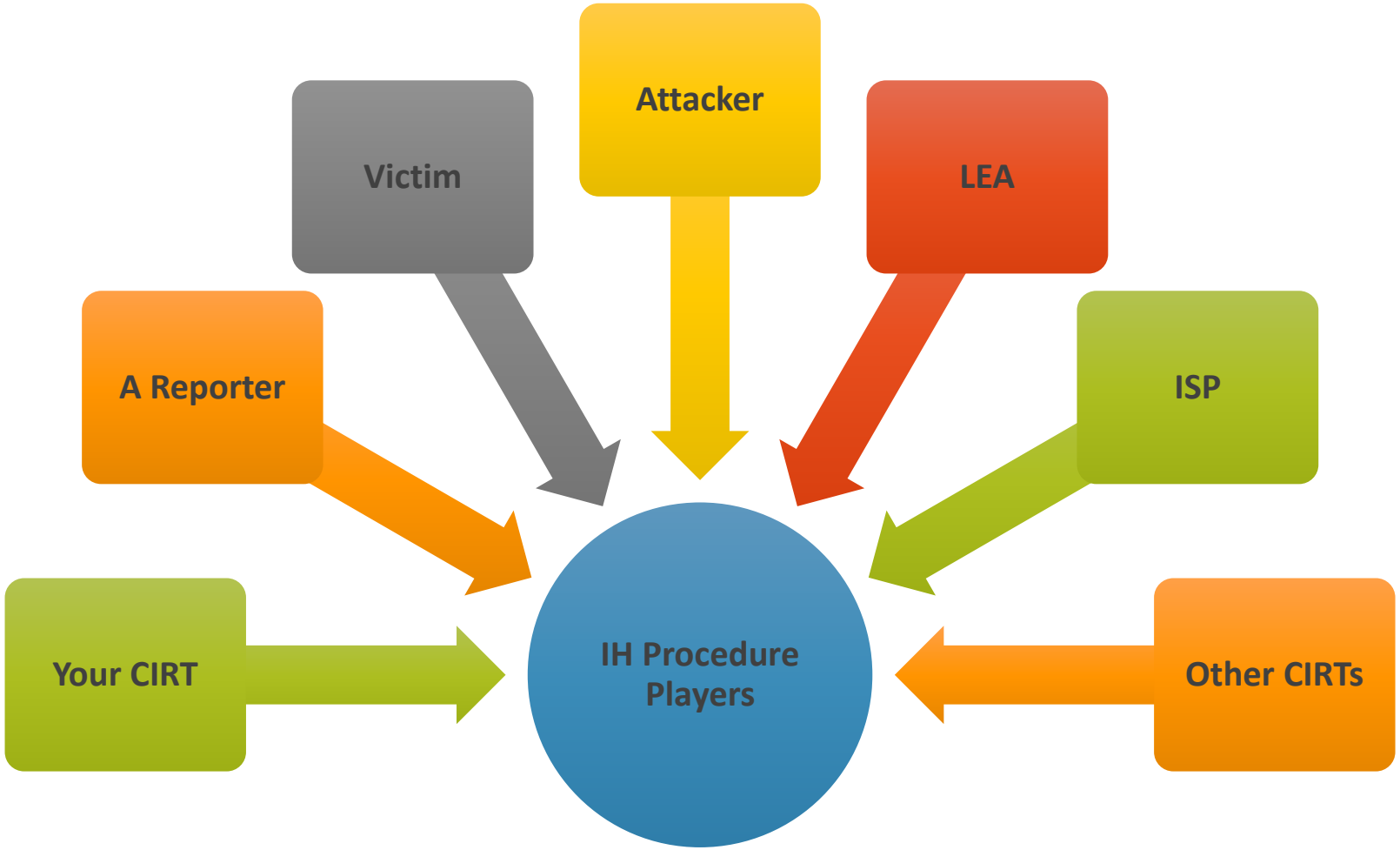
Help to stop attack

Contain the damage

The objective for the Incident Response will be derived from the CIRT mission statement

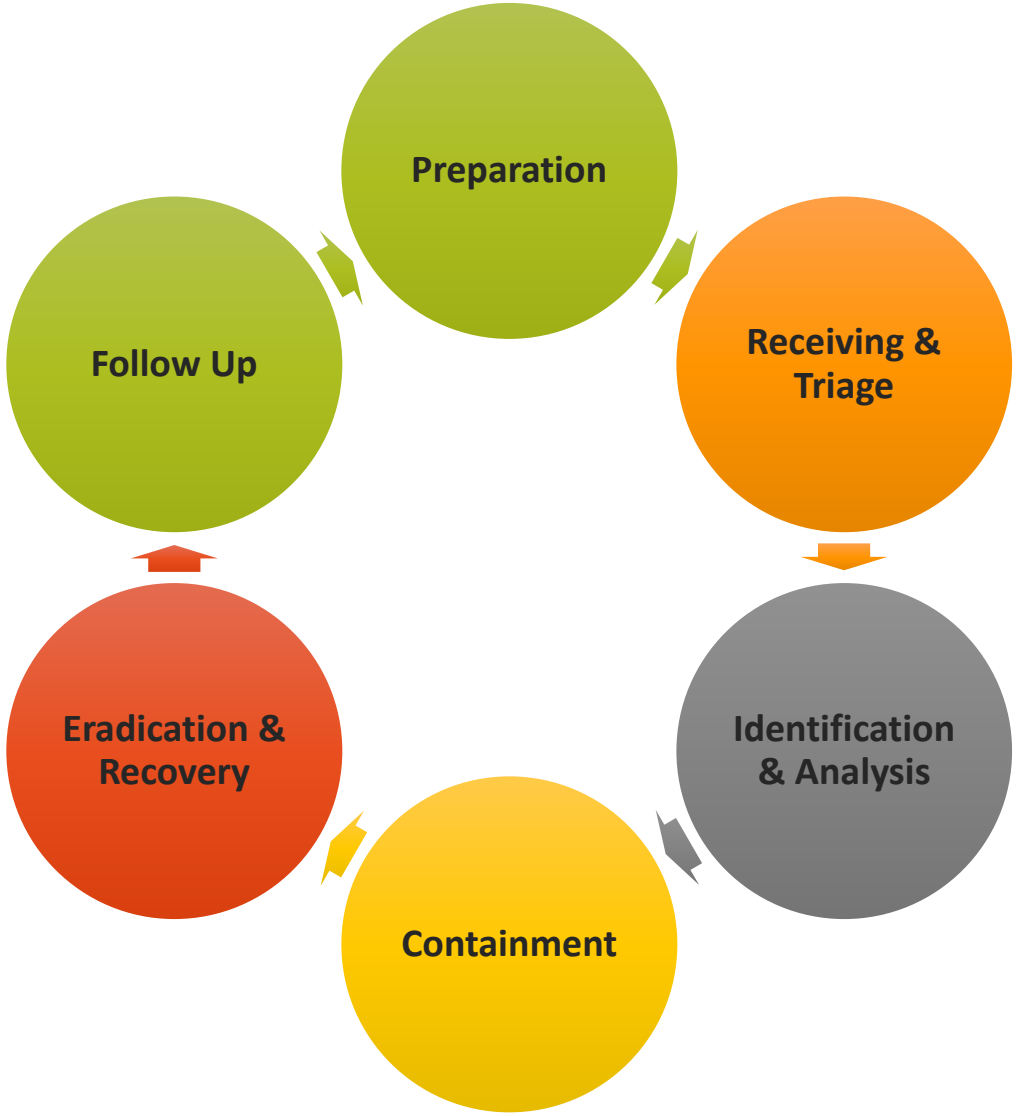
10

Incident handling Players involved



11

Incident handling Lifecycle in a CIRT perspective



12

Incident handling Lifecycle in a CIRT perspective

13

Incident handling Preparation

To respond to incident, the incident handling methodologies are very important.

Communication & Facilities

- Email
- Telephone
- Internal Communication
- POC (Point of Contact) List

Hardware & Software

- Incident Response Systems
- `Information Gathering Systems
- Mail / Web /dB Servers
- Monitoring system
- Remote Access
- Printer & FAX
- Shredder
- Whiteboard & Projector
- Notebook Computers

Policies & Procedures

- Security Policy
- Security Plan
- Incident Response Policy
- Incident Response Plan
- Resource Availability
- Capacity Building
- RFC 2350 "Expectations for Computer Security Incident Response”
- Types of Incidents and Level of Support
- Co-operation, Interaction and Disclosure of Information
- Communication and Authentication

14

Incident handling Preparation

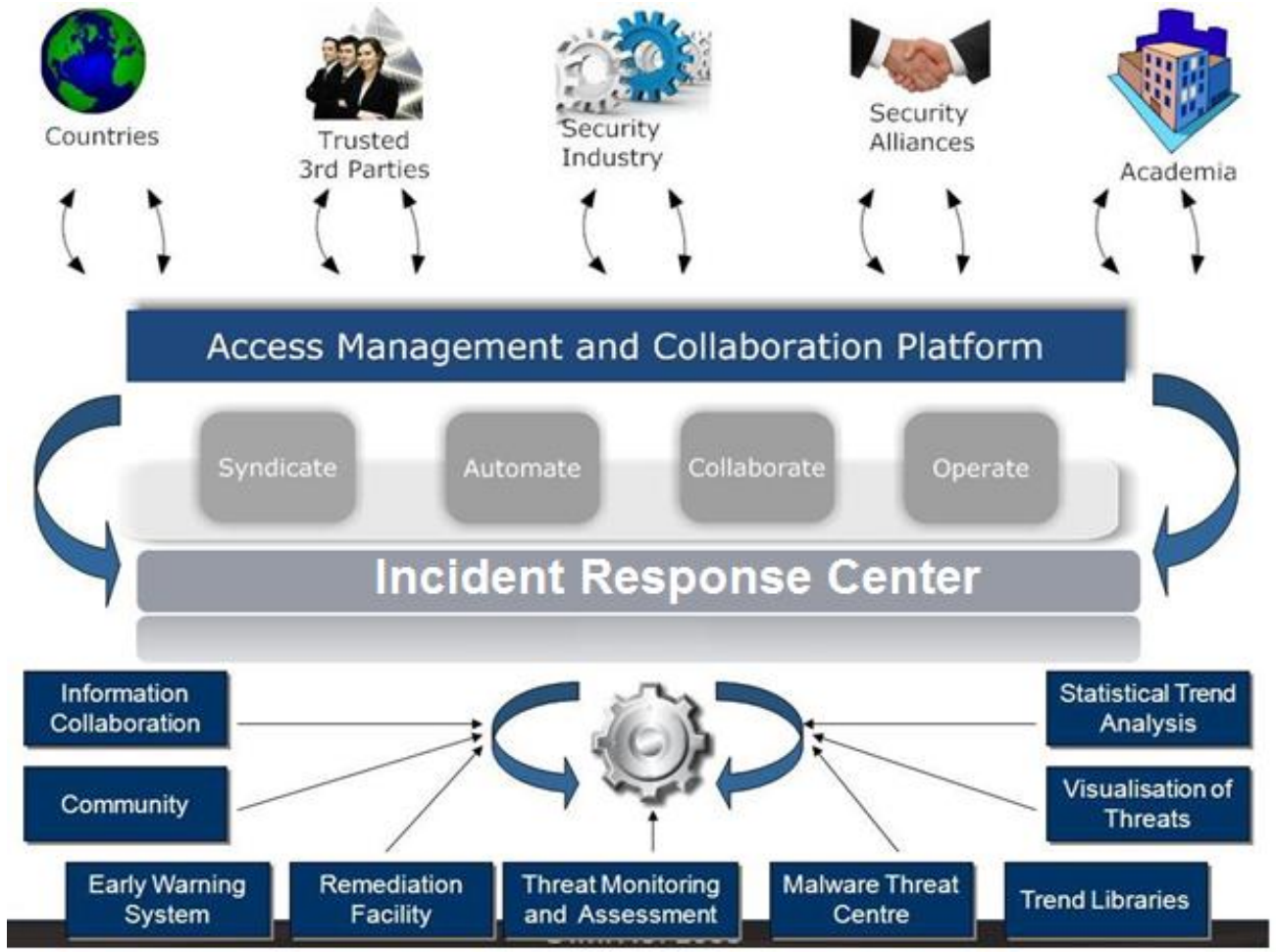
- Building Relationship with key players
  - Law Enforcement
  - Human Resource
  - System Administrators
  - Legal Counsel
  - Fellow Incident Handlers
- Response Kit
  - Quick Response Enablers
- Communication Plan
  - In-band Communication
  - Out-band Communication
  - Build a central point of contact

- Incidents checklist
  - are likChecklists are guidelines
  - Incident checklist e memory joggers
  - Don't use checklist as the 10 Commandments
- Perform threat modeling
  - How will we prepare for the incident?
  - How will we identify the incident?
  - How will we contain the incident?
  - How will we eradicate the incident?
  - How will we recover from the incident?
  - How will we capture the lessons learned from the incident?

Incident handlers need to practice working incidents to hone their skills.
One way to do this is to take part in cyber drill at security conferences.
Also work with other incident handlers in the area to set up practice sessions.

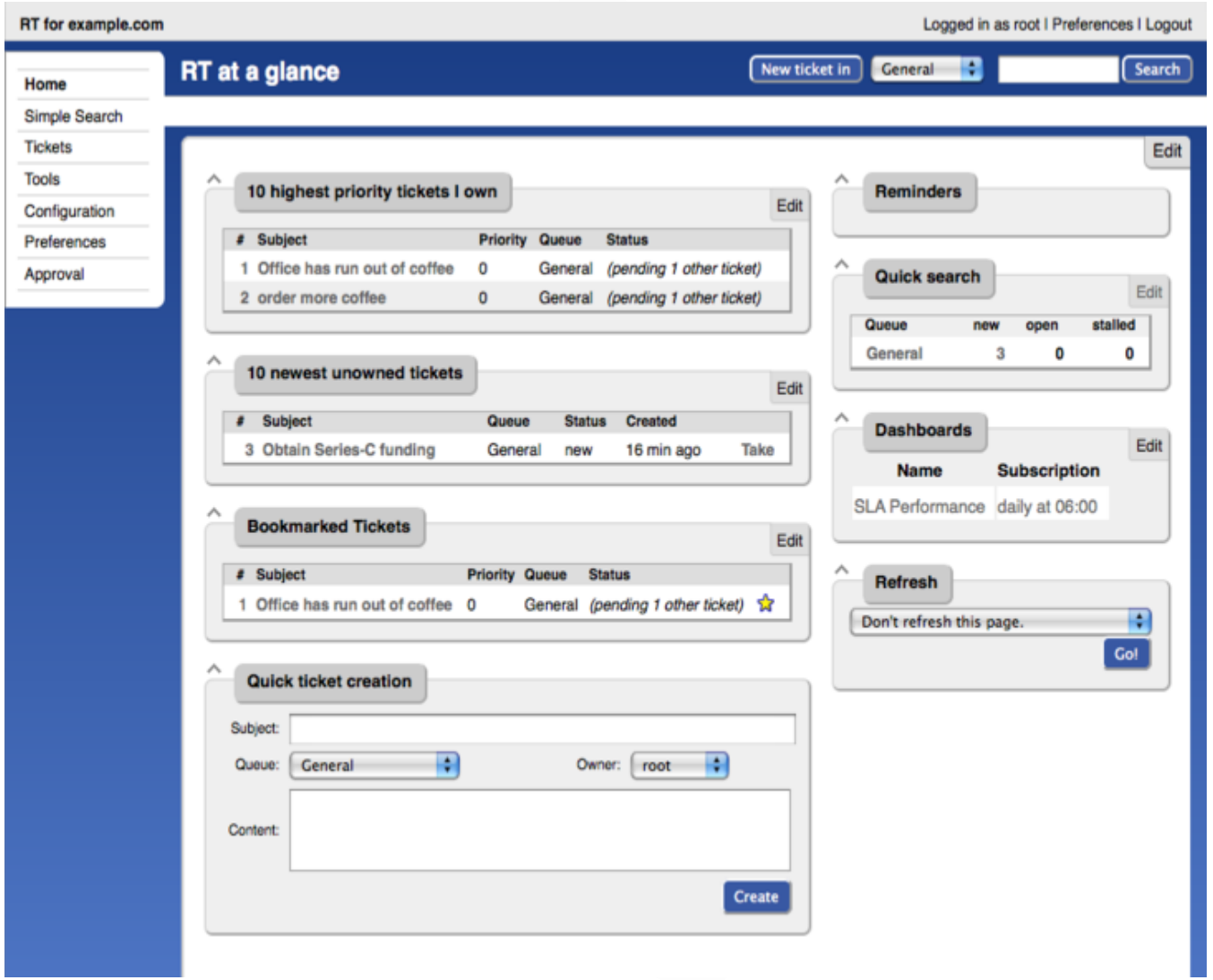
15

Incident handling Incident response structure: example



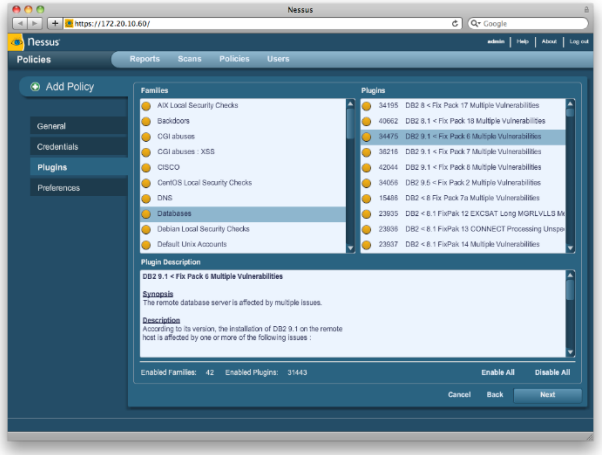
16

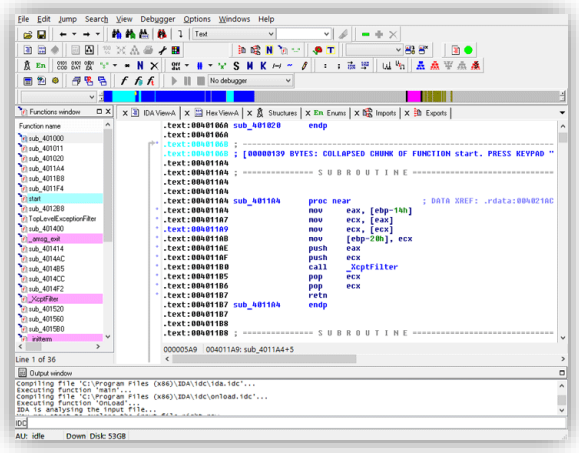
Incident handling Incident handlings systems : example



17

Incident handling Clearing house for IH tools





cuckoo

zmap

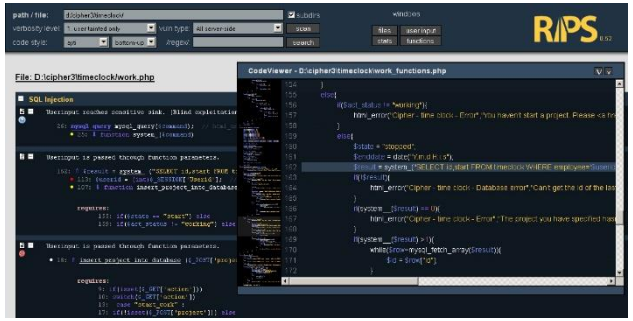
virustotal

Nessus®
vulnerability scanner

malwr

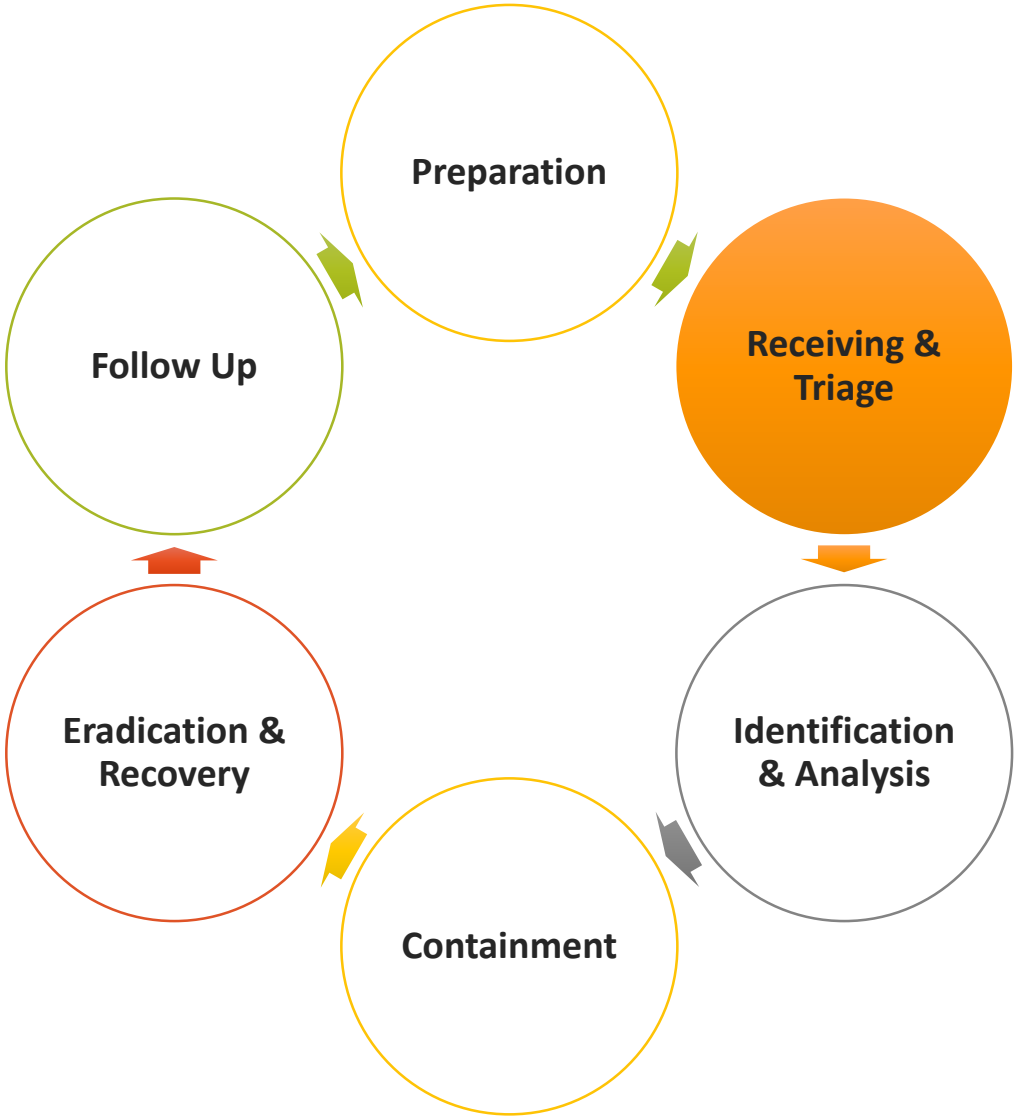
VEGA
BETA RELEASE
OPEN SOURCE WEB APPLICATION VULNERABILITY SCANNER, PROXY AND PLATFORM

TCPDUMP



18

Incident handling Lifecycle in a CIRT perspective



19

Incident handling Receiving

Elements that allow the CIRT to receive incidents.

CIRT can rely on humans/machines/autonomus systems to report incidents.

Some of the common systems that allows the CIRT to receive incidents are:

- Phone
- Email
- Portal
- Fax
- SMS

20

Incident handling Typical format and required information

Contact Info

- Name
- Organization Name
- Division
- E-mail address or FAX number

Purpose of Reporting

- Question
- Information providing
- Request to coordination
- Other

- Summary of the Incident
  - Source IP address or hostname
  - Description about the incident
  - System information of the system
  - IP address or hostname
  - Protocol / Port number
  - Hardware / OS
  - Timestamp
  - Time zone
- Log Information

21

Incident handling Triage

Real life example

In hospital, where patients who need to be attended immediately are separated from those who can wait for assistance.

Sorting, Categorizing, Prioritizing

Depending on resources available

Type

Incident, Vulnerability, Virus, Information

New report or related on-going report?

If on-going report, is it part of an existing Incident? Same IP address?

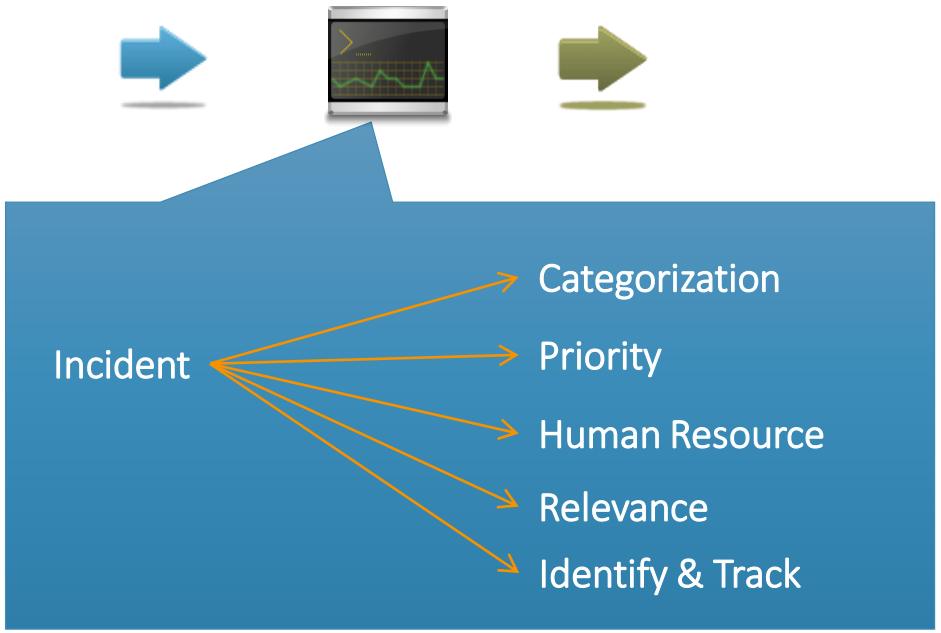
Linkage between separate reports

Tracking number?

22

Incident handling Triage

Triage helps the incident handlers optimize the time taken for incident handling as well as perform effective incident handling.



23

Incident handling Triage – prioritizing incidents

Due to limited resource and the growing number of incident reports, we may not be able to respond to every incidents reported to us.

Resource needed to deal with it

Impact on constituency

Category of incident

Type or extent of damage

Target or source of an attack

24

Incident handling Triage – prioritizing incidents

- High
  - Urgent report like phishing
  - Incident still active
  - Have to coordinate to other organization
- Middle
  - Not urgent report
  - Not active incident
  - Will coordinate to other organization
- Low
  - Just a technical question to answer
  - Just a FYI to us
- Others

Priority Coding System		Impact		
		High	Medium	Low
Urgency	High	1	2	3
	Medium	2	3	4
	Low	3	4	5

Priority Code	Description	Target
1	Critical	1 hour
2	High	8 hours
3	Medium	24 hours
4	Low	48 hours
5	Planning	Planned

25

Incident handling Triage – Incident classification

Incident Class (mandatory input field)	Incident Type (optional but desired input field)	Description / Examples
Abusive Content	Spam	'Unsolicited bulk e-mail', which means that the recipient has not granted verifiable permission for the message to be sent and that the message is sent as part of a larger collection of messages, all having an identical content.
	Harassment	Discrediting, or discrimination against, somebody (ie, cyber stalking)
	Child/Sexual/Violence/...	Child pornography, glorification of violence, ...
Malicious Code	Virus	Software that is intentionally included or inserted in a system for a harmful purpose. A user interaction is normally necessary to activate the code.
	Worm	
	Trojan	
	Spyware	
	Dialer	

26

Incident handling Triage – Incident classification

Incident Class (mandatory input field)	Incident Type (optional but desired input field)	Description / Examples
Information Gathering	Scanning	Attacks that send requests to a system to discover weak points. This includes also some kinds of testing processes to gather information about hosts, services and accounts. Examples: fingerd, DNS querying, ICMP, SMTP (EXPN, RCPT)
	Sniffing	Observing and recording network traffic (wiretapping).
	Social Engineering	Gathering information from a human being in a non-technical way (eg, lies, tricks, bribes, or threats).
Intrusion Attempts	Exploiting Known Vulnerabilities	An attempt to compromise a system or to disrupt any service by exploiting vulnerabilities with a standardised identifier such as a CVE name (eg, buffer overflow, backdoors, cross side scripting, etc).
	Login Attempts	Multiple login attempts (Guessing or cracking passwords, brute force).
	New Attack Signature	An attempt using an unknown exploit.

27

Incident handling Triage – Incident classification

Incident Class (mandatory input field)	Incident Type (optional but desired input field)	Description / Examples
Information Security	Unauthorised Access to Information	Besides the local abuse of data and systems, information security can be endangered by a successful account or application compromise. Furthermore, attacks that intercept and access information during transmission (wiretapping, spoofing or hijacking) are possible.
	Unauthorised Modification of Information	
Fraud	Unauthorized Use of Resources	Using resources for unauthorised purposes, including profit-making ventures (eg, the use of e-mail to participate in illegal chain letters for profit or pyramid schemes).
	Copyright	Selling or installing copies of unlicensed commercial software or other copyright protected materials (Warez).
	Masquerade	Type of attacks in which one entity illegitimately assumes the identity of another in order to benefit from it.
Other	All incidents which do not fit in one of the given categories should be put into this class.	If the number of incidents in this category increases, it is an indication that the classification scheme needs to be revised.

28

Incident handling Triage – Incident classification

Criticality Level	Criticality Level Definition	Typical Incident Categories	Initial Response Time	Ongoing Response (Critical Phase)	Ongoing Response (Resolution Phase)	Ongoing Communication Requirement
1	Incident affecting critical systems or information with potential to be revenue or customer impacting.	▪ Denial of service ▪ Compromised Asset (critical) ▪ Internal Hacking (active) ▪ External Hacking (active) ▪ Virus / Worm (outbreak) ▪ Destruction of property (critical)	60 Minutes	CIRT Incident Manager assigned to work case on 24x7 basis.	CIRT Incident Manager assigned to work on case during normal business hours.	Case update sent to appropriate parties on a daily basis during critical phase. If CSIRT involvement is necessary to restore critical systems to service then case update will be sent a minimum of every 2 hours.

29

Incident handling Triage – Incident classification

Criticality Level	Criticality Level Definition	Typical Incident Categories	Initial Response Time	Ongoing Response (Critical Phase)	Ongoing Response (Resolution Phase)	Ongoing Communication Requirement
2	Incident affecting non-critical systems or information, not revenue or customer impacting. Employee investigations that are time sensitive should typically be classified at this level.	▪ Internal Hacking (not active) ▪ External Hacking (not active) ▪ Unauthorized access. ▪ Policy violations ▪ Unlawful activity. ▪ Compromised information. ▪ Compromised asset. (non-critical)	4 Hours	CIRT Incident Manager assigned to work case on 24x7 basis.	CIRT Incident Manager assigned to work on case during normal business hours.	Case update sent to appropriate parties on a daily basis during critical phase. Case update sent to appropriate parties on a weekly basis during resolution phase.

30

Incident handling Triage – Incident classification

Criticality Level	Criticality Level Definition	Typical Incident Categories	Initial Response Time	Ongoing Response (Critical Phase)	Ongoing Response (Resolution Phase)	Ongoing Communication Requirement
3	Possible incident, non-critical systems. Incident or employee investigations that are not time sensitive. Long-term investigations involving extensive research and/or detailed forensic work.	▪ Email ▪ Forensics Request ▪ Inappropriate use of property. ▪ Policy violations.	48 Hours	Case is worked as CIRT time/resources are available.	Case is worked as CIRT time/resources are available.	Case update sent to appropriate parties on a weekly basis.

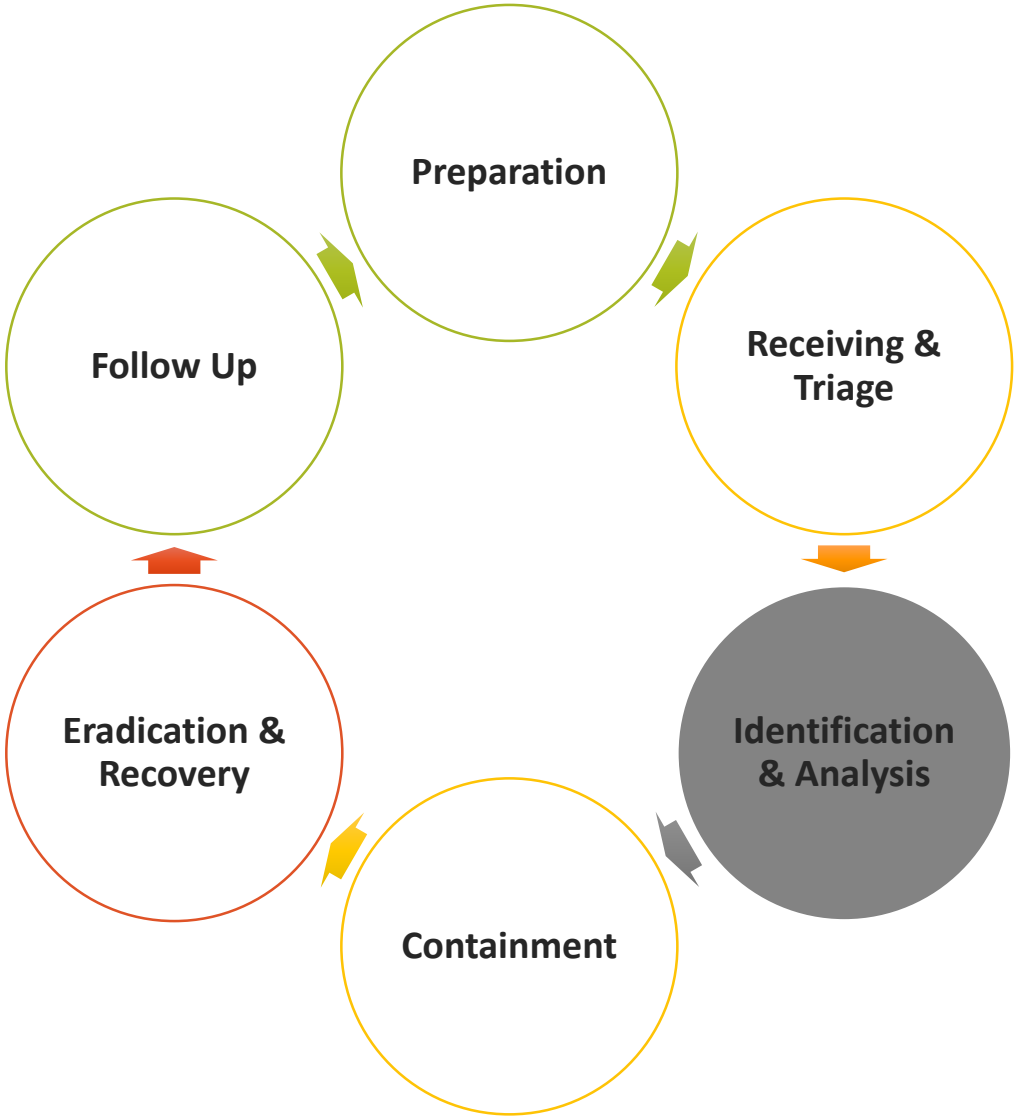
31

Incident handling Triage – Incident classification

Sensitivity Level	Sensitivity Level Definition	Typical Incident Categories	Required On Case Communication	Optional On Case Communication	ITS Access
1	Extremely Sensitive.	▪ Global Investigations Initiated. ▪ Forensics Request ▪ Destruction of property. ▪ Compromised asset. ▪ Compromised information. ▪ Unlawful activity. ▪ Inappropriate use of property. ▪ Policy violations	CIRT, CPOC	CIRTM	CIRT, CIRTM
2	Sensitive.	▪ External Hacking ▪ Internal Hacking ▪ Unauthorized Access	CIRT, CPOC	Security Operations, OWNERS	Security Operations
3	Not Sensitive.	▪ Denial of service. ▪ Virus / Worm ▪ Email	CIRT, CPOC	ANY	ALL Agents in ITS

32

Incident handling Lifecycle in a CIRT perspective



33

Incident handling Identification and analysis

Define objectives and investigate situation

- **Who** has attacked us?
- **What** is the scope and extent of the attack?
- **When** did the attack occur?
- **What** did the attackers take from us?
- **Why** did they do it?

- Determine what investigation actions are to be taken
- Determine CSIRT resources are required to conduct the investigation, request/secure hardware, software, personnel resources
- Communicate with parties that need to be aware of the investigation

34

Incident handling Identification and analysis

Profile Network and Systems

Understand Normal Behaviours

Use Centralized logging and Create a Log Retention Policy

Perform Event Correlation

Keep All Host Clocks Synchronized

Maintain and Use a Knowledgebase of Information

Use Internet Search Engines for Research

Run Packet Sniffers to Collect Additional Data

Consider Filtering the Data

Consider Experience as Being Irreplaceable

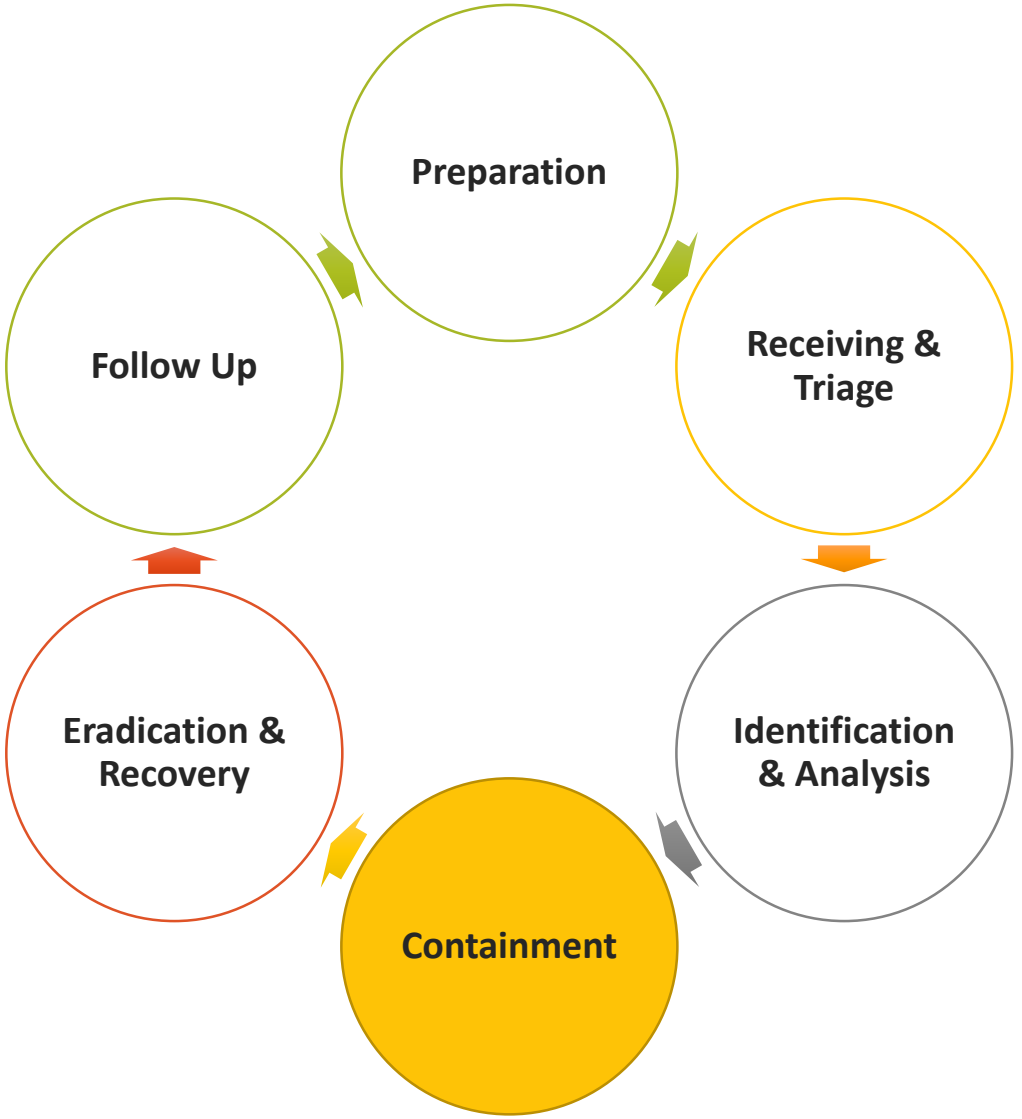
Create a Diagnosis Matrix for Less Experienced Staff

Seek Assistance From Others

- Order of Volatility
  - Registers
  - Routing table
  - Temporary file systems
  - Disk
  - Others
- Things to avoid
  - It's all too easy to destroy evidence (fragile).
- Privacy Considerations
  - Respect the privacy rules
  - Do not intrude on people's privacy without strong justification
  - Make user backing of procedure that company's established.
- Legal Considerations
  - Computer evidence needs to be Admissible, Authentic, Complete, Reliable and Believable.

35

Incident handling Lifecycle in a CIRT perspective



36

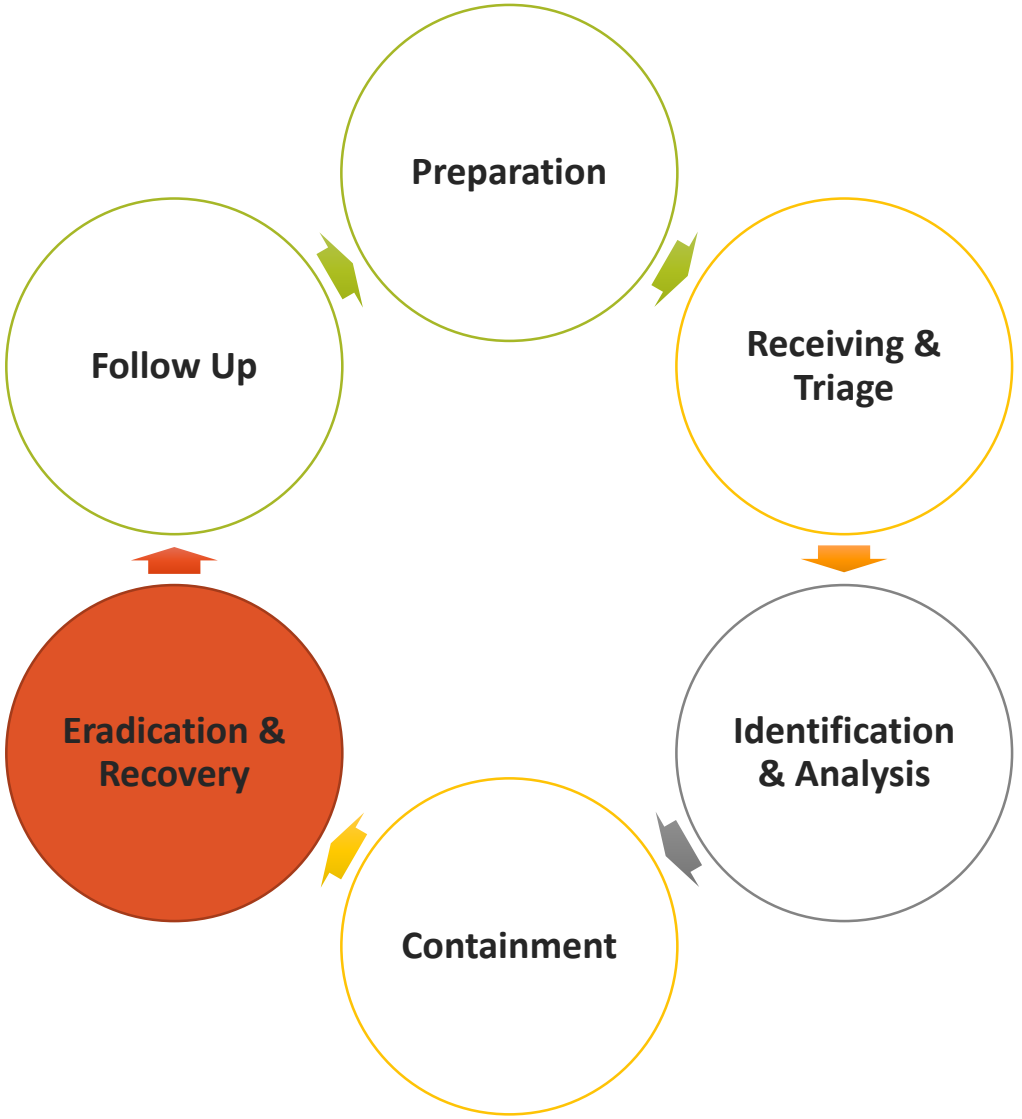
Incident handling Containment

- Take appropriate action to contain the incident
  - Blocking (and logging) of unauthorised access
  - Blocking malware sources (e.g. email addresses and websites)
  - Blocking botnet connections to external site
  - Closing particular ports and services
  - Changing system administrator passwords where compromise is suspected
  - Firewall filtering
  - Relocating website home pages
  - Isolating systems

- Delayed containment is usually NOT good.
- Need additional evidence to do containment?
- Need to get approval from legal section?
- If so (above), attacker could escalate unauthorized access / compromise other system in short time…
- Other potential issues
- Some attacks may cause additional damage when contained (e.g. disconnected).

37

Incident handling Lifecycle in a CIRT perspective



38

Incident handling Eradication and recovery

Further investigation should be performed to uncover the cause of the incident by analyzing system logs of various devices(router, firewall and host logs)

Eliminate intruder's means of access and any related vulnerabilities

- Recover systems, data and connectivity
  - To **restore** systems to normal operation;
  - To confirm that the systems are functioning normally; and
  - To **remediate vulnerabilities** to prevent similar incidents occurring
- Performs system hardening
  - Install security patches
  - Strong authentication
  - Strengthen logging
  - Tighten perimeter security

39

Incident handling Eradication and recovery

Example of eradication

- Delete malicious code
- Disable breached user account

Example of recovery

- Restore the system
- Rebuild systems from scratch
- Replace compromised files with clean versions
- Install patches
- Change passwords
- Tighten network perimeter security - Configuration of firewall & router
- Higher levels of system logging or network monitoring

40

Incident handling Lifecycle in a CIRT perspective

41

Incident handling Documentation

Carry out a post incident review

- Important information about the cyber security incident should be discussed during a post incident review
- All key discussions and decisions conducted during the eradication event should be well documented
- A report should be produced from the post incident review and presented to all relevant stakeholders

- Incident history
  - Chronicle of all email and other correspondence
- Status
  - Current status of the incident
- Actions
  - List of past, current, and future actions to be taken
- Incident coordinator
  - A team may choose to assign a staff member to coordinate the response to this incident
- Quality assurance parameters
  - Information that might help to measure the quality of the service

42

Incident handling Communication

Report the incident to relevant stakeholders

- A **full description** of the **nature** of the incident, it's history, and what actions were taken to recover
- A realistic **estimate** of the financial **cost** of the incident, as well as other impacts on the business
- **Recommendations** regarding enhanced or additional **controls** required to prevent, detect, remediate or recover from cyber security incidents more effectively

Communicate and build on lessons learned

To document, communicate and build on lessons learned

On-going process through which you can collaborate and learn from previous mistakes, incidents and experiences

Develop an action plan to leverage on lessons learned to become more resilient in the face of future cyber security attacks

43

Incident handling Self learning

Update key information, controls & documents

- Review security incident management methodologies or processes
- Review management controls (e.g. training and awareness)
- Review Technical controls (e.g. patching, configuring system logs, and use of intrusion prevention/detection tools)
- Review Internal IT auditing procedures

- Post-mortem after the incident is resolved.
- The meeting is helpful in improving security measures and the incident handling process itself.
- Assess time and resources used and damage incurred.
- Update policy and procedures as necessary.
- Update knowledgebase.

44