International Telecommunication Union

DEFINITION

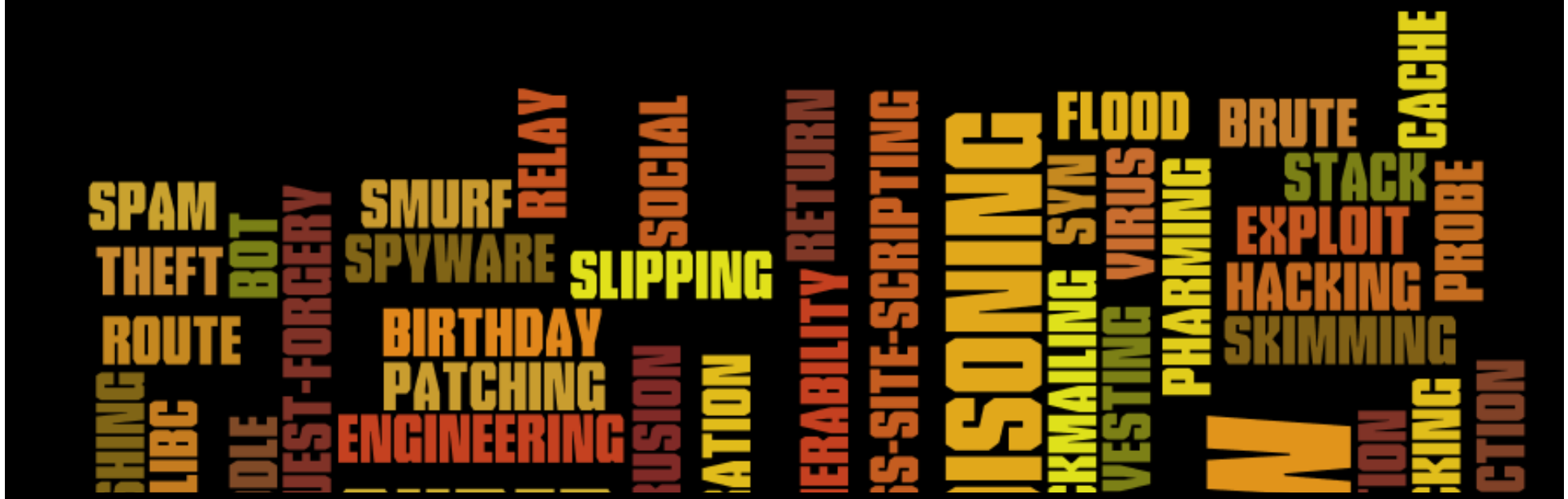
COMPUTER SECURITY INCIDENT

“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



There are no standard types for security Incidents!

INTRODUCTION

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

INTRODUCTION

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

INCIDENT RESPONSE

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.

INCIDENT RESPONSE

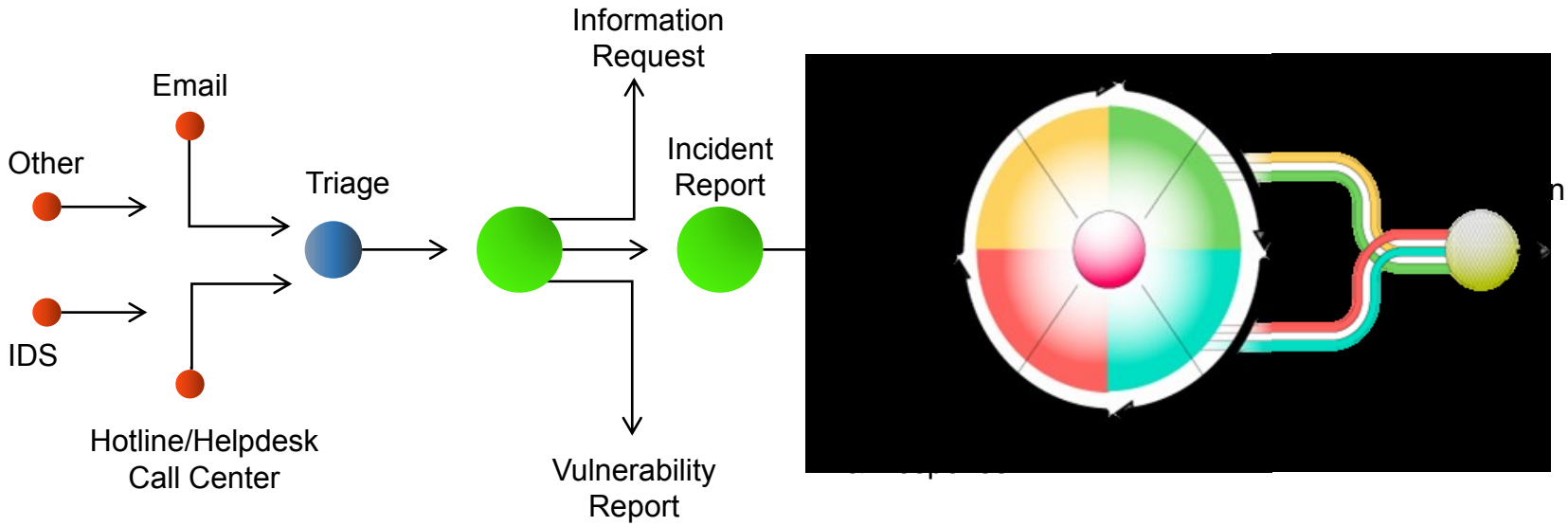
POLICIES & PROCEDURES

- Established procedures must be in place to:
  - ✓ Detect & identify the attack
  - ✓ Mitig
  - ✓ Recov
- 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.

INCIDENT RESPONSE

INCIDENT HANDLING LIFE CYCLE



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

INCIDENT RESPONSE

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

INCIDENT RESPONSE

ELEMENTS

Categorisation

No consensus has emerged in the security community as to which taxonomy is the best

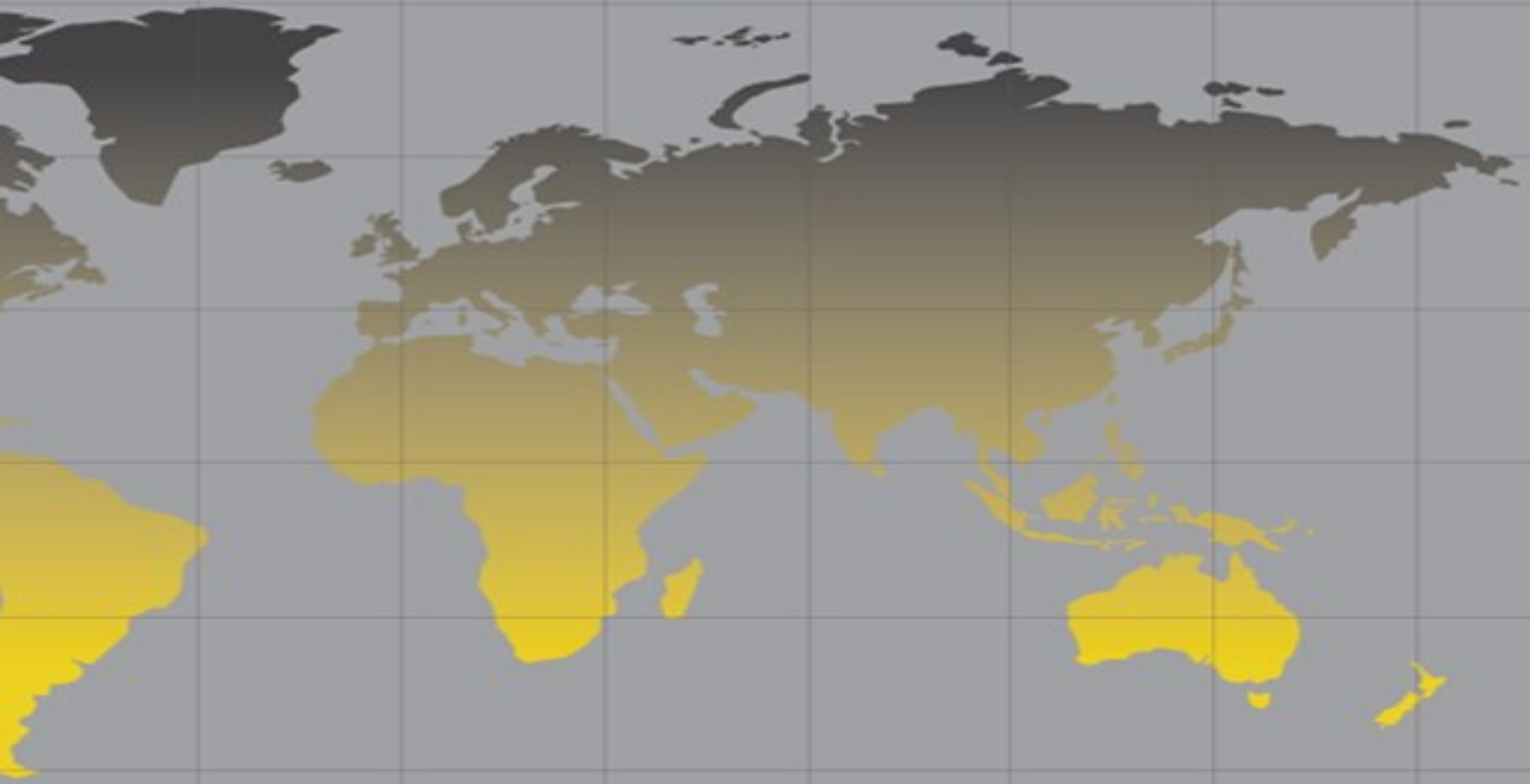
Prioritisation

Prioritisation of incidents is based on multiple factors.

Classification

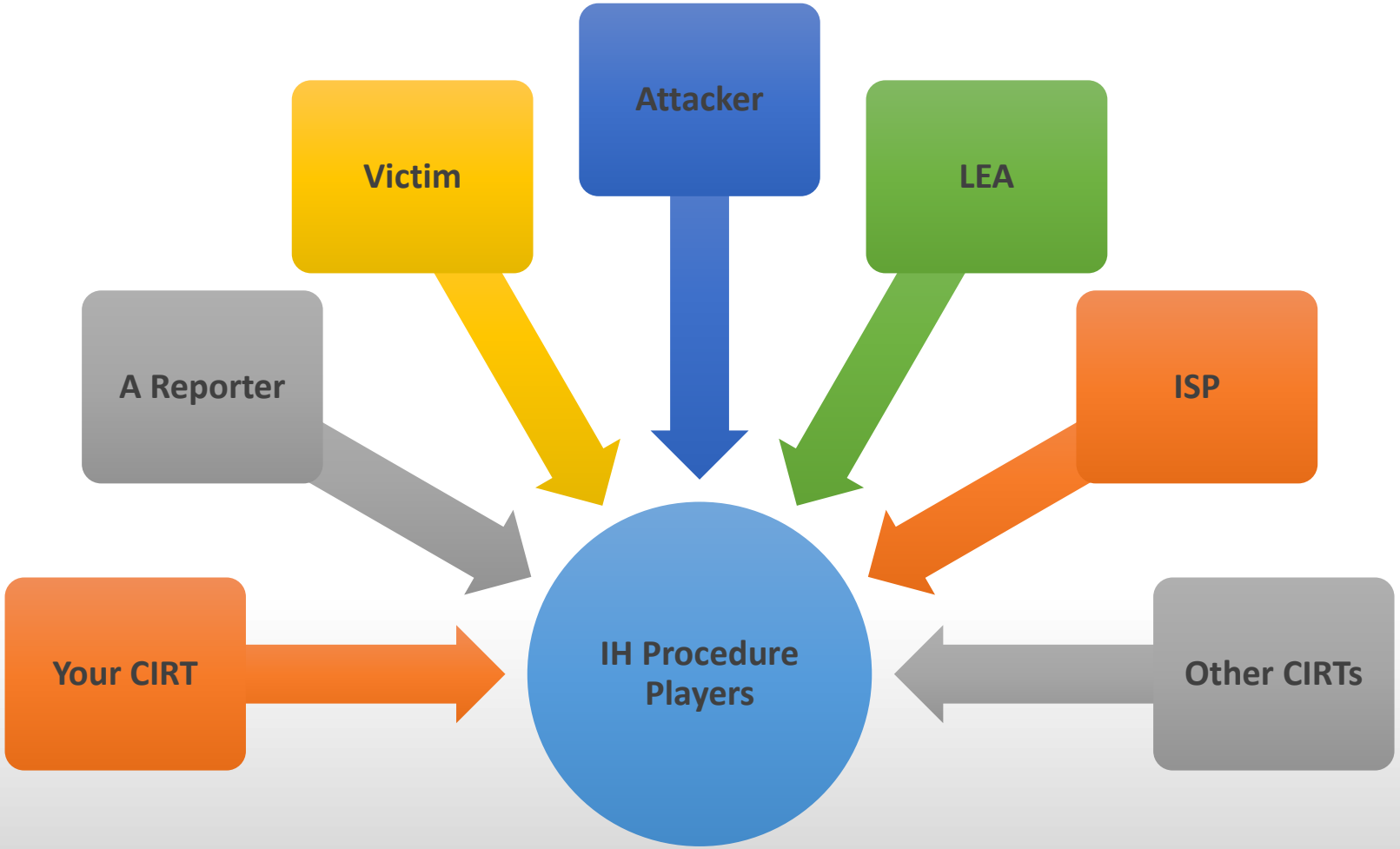
Classification of an incident is done based on the mission, operation field and other related elements.

INCIDENT HANDLING



INCIDENT HANDLING

PLAYERS INVOLVED



INCIDENT HANDLING

LIFECYCLE IN A CIRT PERSPECTIVE

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
- **Policy & Procedure**
  - 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

INCIDENT HANDLING

PREPARATION

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

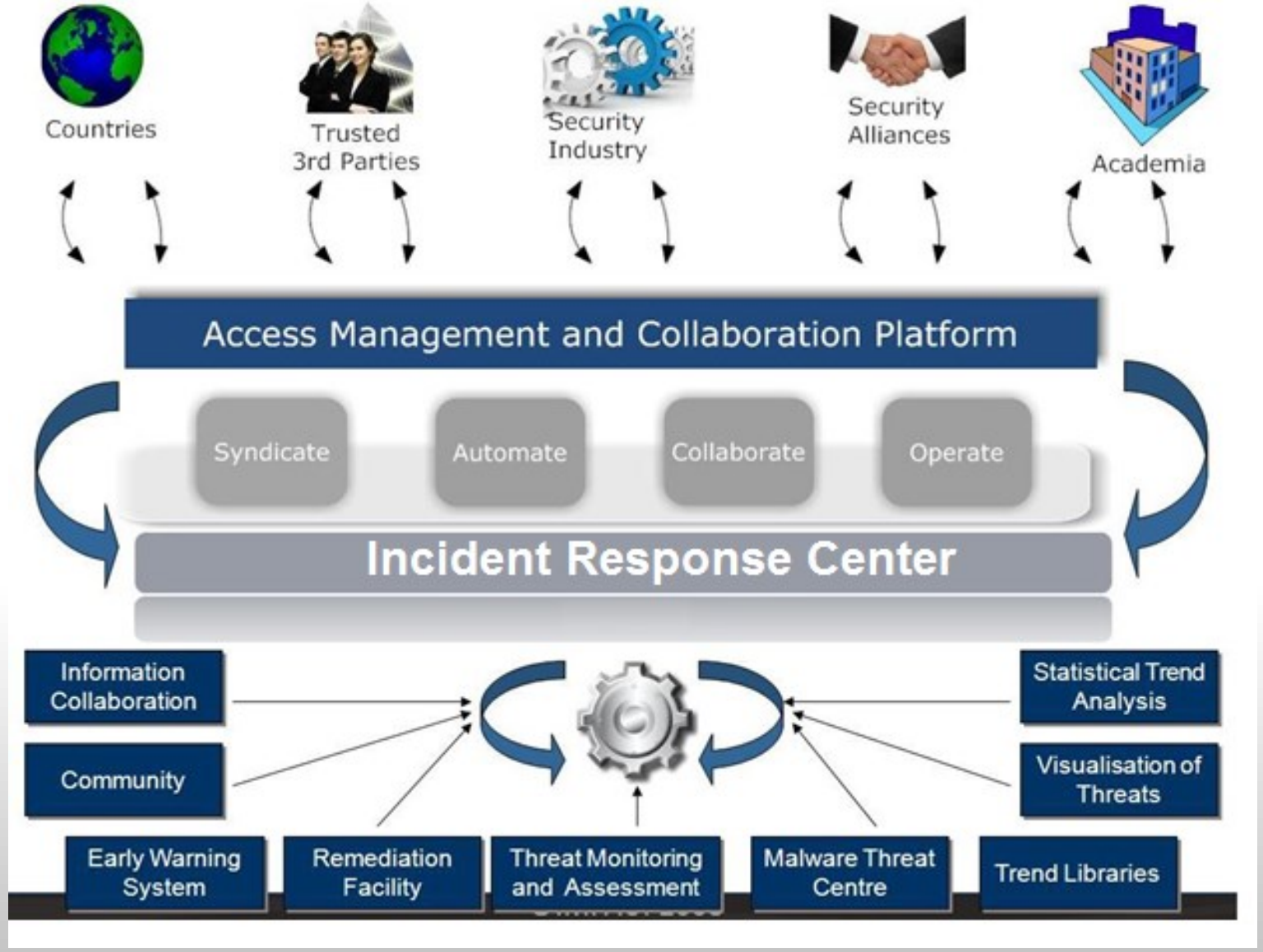
- **Building Relationship with key players**
  - Law Enforcement
  - Human Resource
  - System Administrators
- **Incidents checklist**
  - Checklists are guidelines
  - Incident checklist are like memory joggers

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.

- Build a central point of contact
- 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?

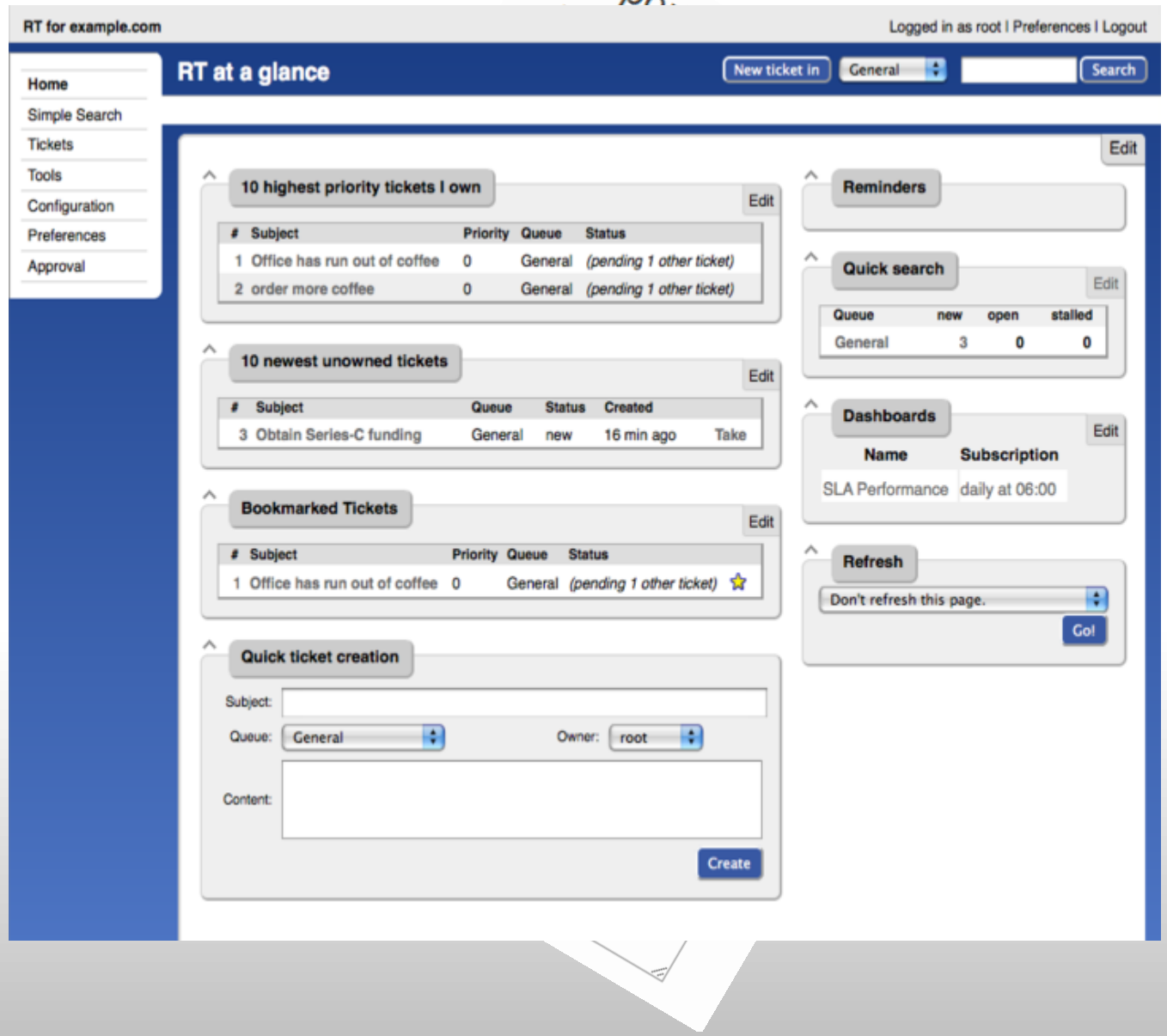
INCIDENT HANDLING

INCIDENT RESPONSE STRUCTURE: EXAMPLE



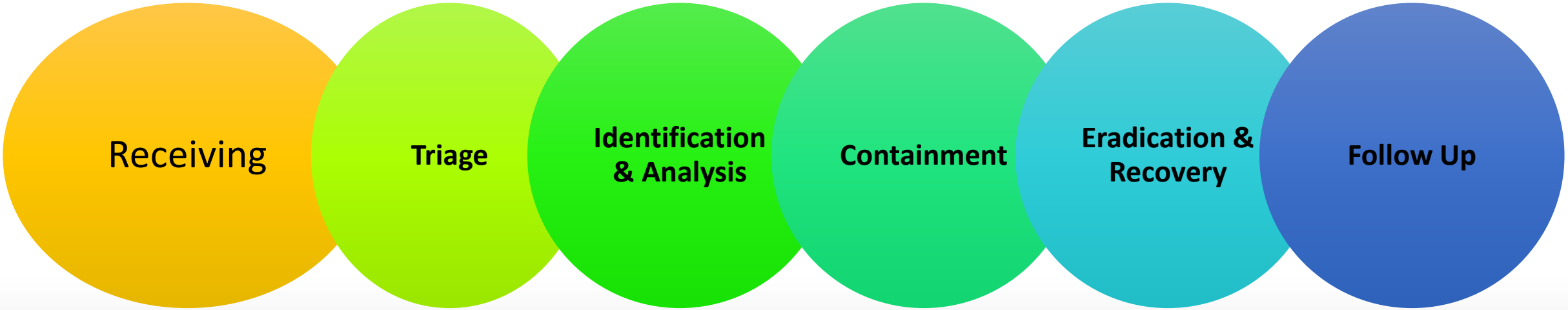
INCIDENT HANDLING

INCIDENT HANDLING SYSTEMS



INCIDENT HANDLING

BASICS



INCIDENT HANDLING

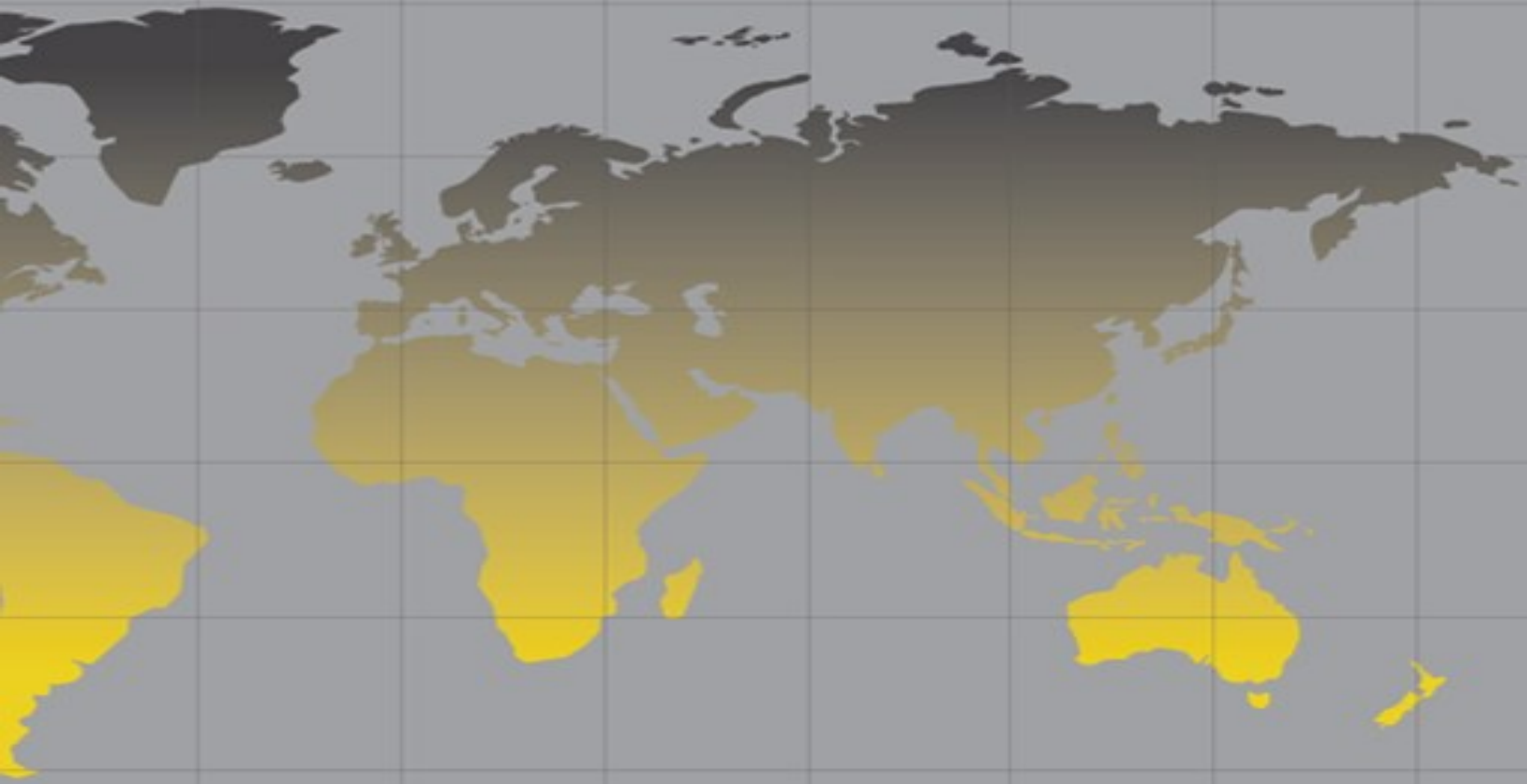
BASICS : PREPERATION

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

- Communication & Facilities
  - External
  - Internal
- Template
- Hardware & Software
- Policy & Procedure

RECEIVING

INCIDENT HANDLING



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

INCIDENT HANDLING

TYPICAL INCIDENT REPORTING FORMAT

Contact Info

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

Purpose of Reporting

- Question
- Information providing
- Request to coordination
- Other

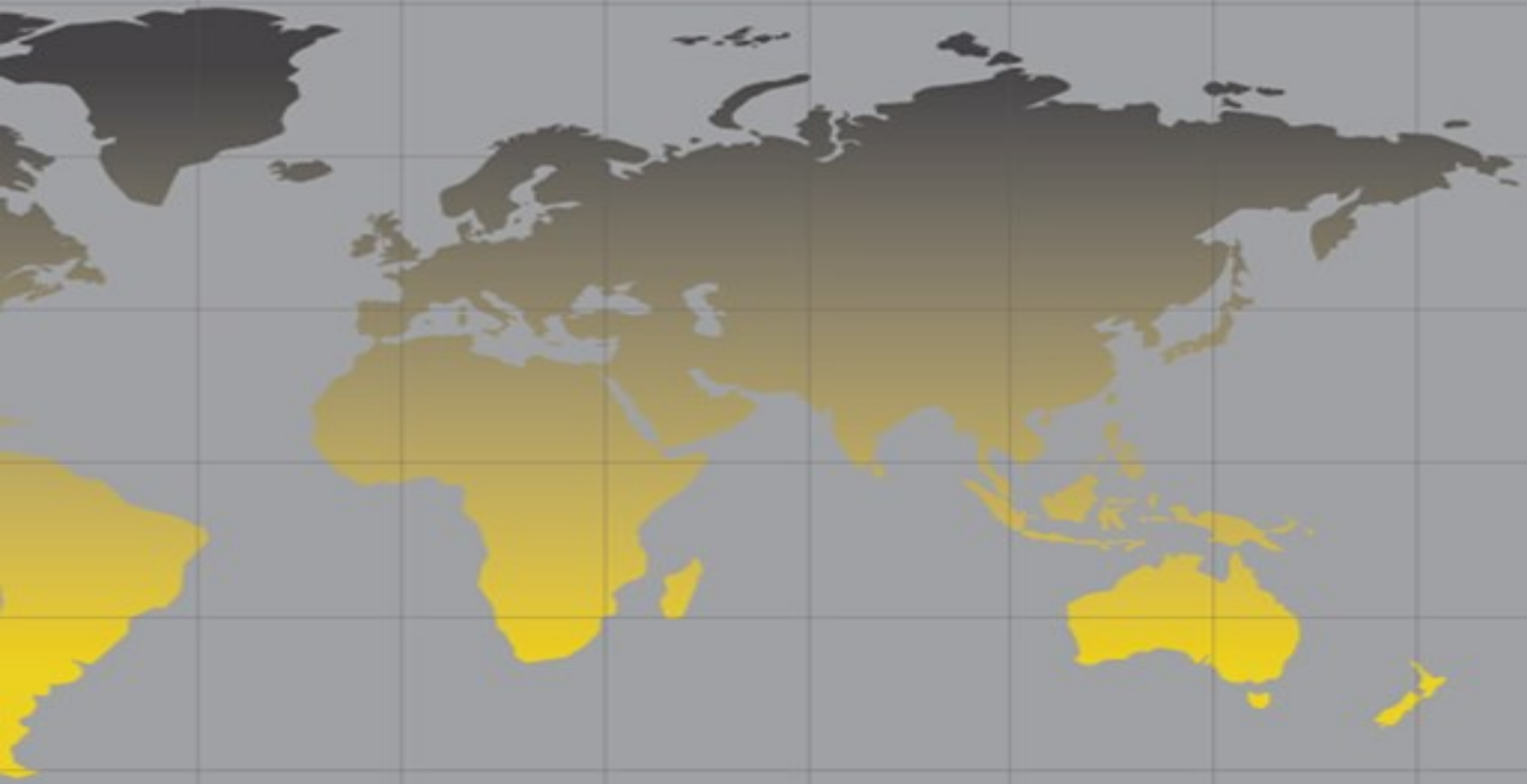
Summary of the Incident

- 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

TRIAGE

INCIDENT HANDLING



INCIDENT HANDLING

TRIAGE

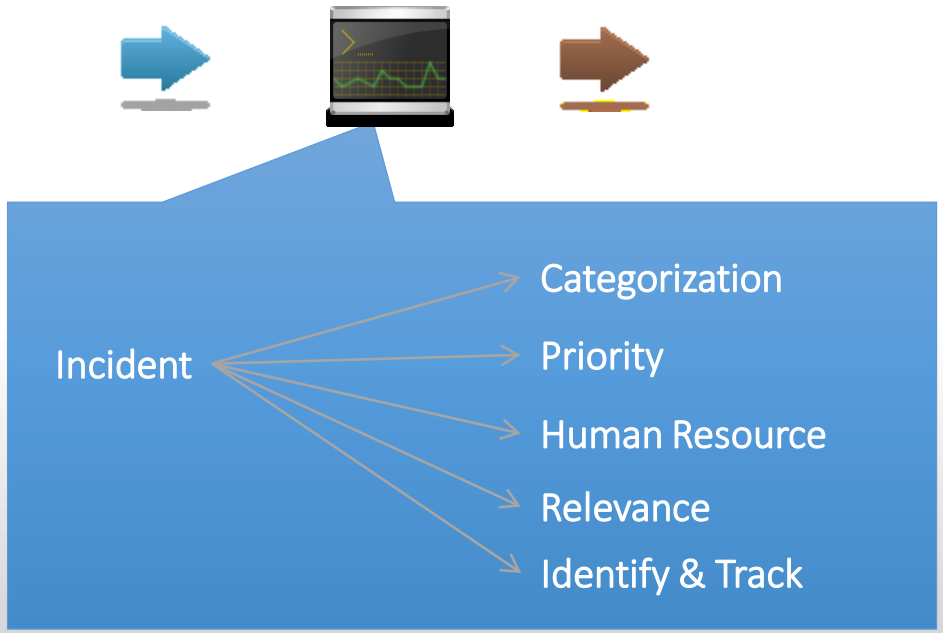
In hospital, where patients who need to be attended immediately are separated from those who can wait for assistance.

- 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?

INCIDENT HANDLING

TRIAGE

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



INCIDENT HANDLING

TRIAGE: PRIORITY

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

INCIDENT HANDLING

TRIAGE

Classification vs. Categorization

INCIDENT RESPONSE

ELEMENTS

Incident Class (mandatory input field)	Incident Type (optional but desired input field)	Description / Examples
Abusive Content	Spam	or "Unsolicited Bulk Email", this 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	Discreditation or discrimination of somebody (i.e. Cyberstalking)
	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	
Information Gathering	Scanning	Attacks that send requests to a system to discover weak points. This includes also some kind of testing processes to gather information about hosts, services and accounts. Examples: fingerd, DNS querying, ICMP, SMTP (EXPN, RCPT, ...).
	Sniffing	Observing and recording of network traffic (wiretapping).
	Social Engineering	Gathering information from a human being in a non-technical way (e.g. lies, tricks, bribes, or threats).

INCIDENT HANDLING

TRIAGE: PRIORITY

High

- Urgent report like phishing
- Incident still active
- Have to coordinate to other organization

Middle

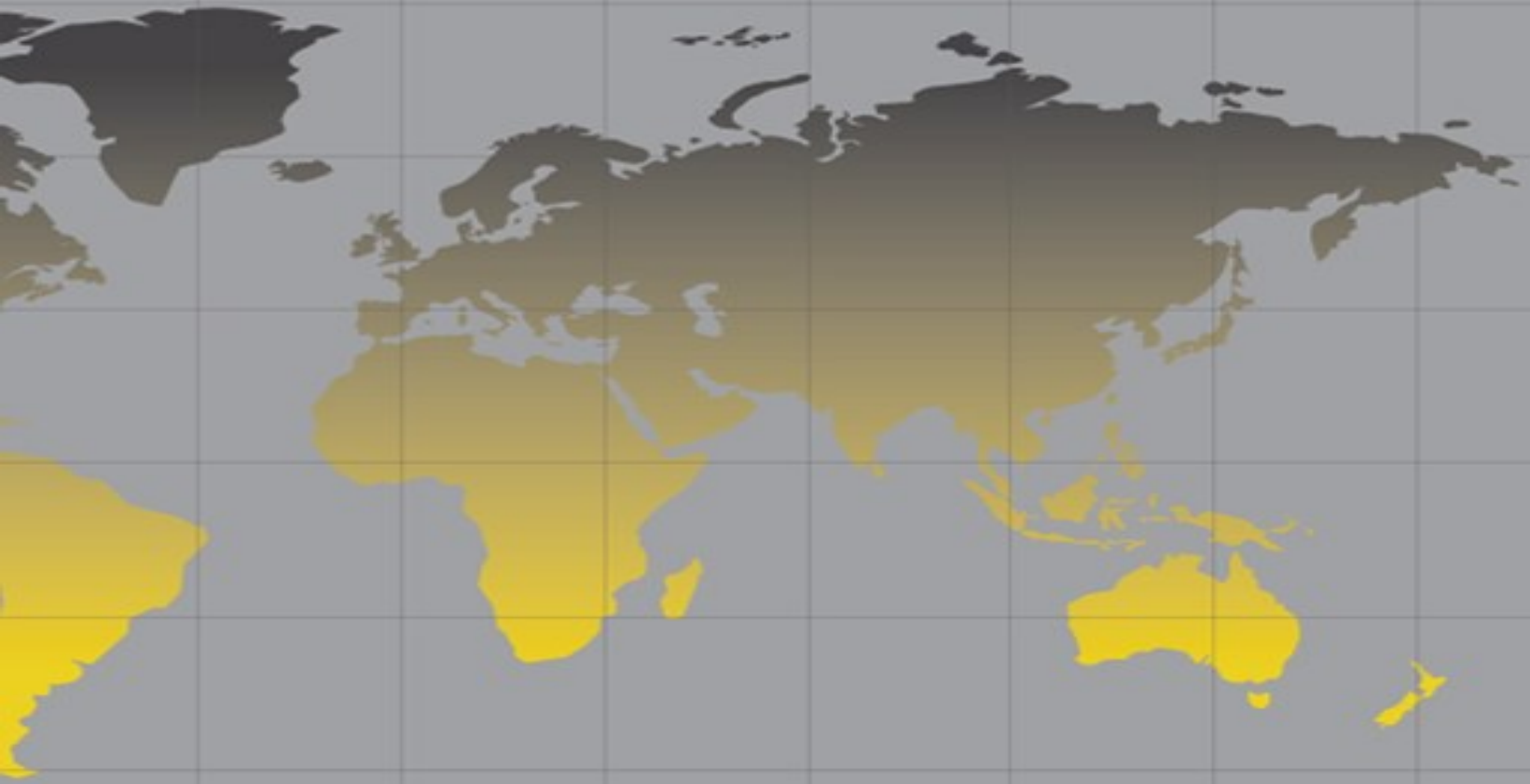
- Not urgent report
- Not active incident
- Will coordinate to other organization

Low

- Just a technical question to answer
- Just a FYI to us
- Others

LETS DO A QUICK EXERCISE

TRIAGE AND INCIDENT HANDLING



INCIDENT HANDLING

TRIAGE: 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	

INCIDENT HANDLING

TRIAGE: 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.

INCIDENT HANDLING

TRIAGE: 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.

INCIDENT HANDLING

TRIAGE: RESPONSE LEVEL 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.

INCIDENT HANDLING

TRIAGE: RESPONSE LEVEL 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.

INCIDENT HANDLING

TRIAGE: RESPONSE LEVEL 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.

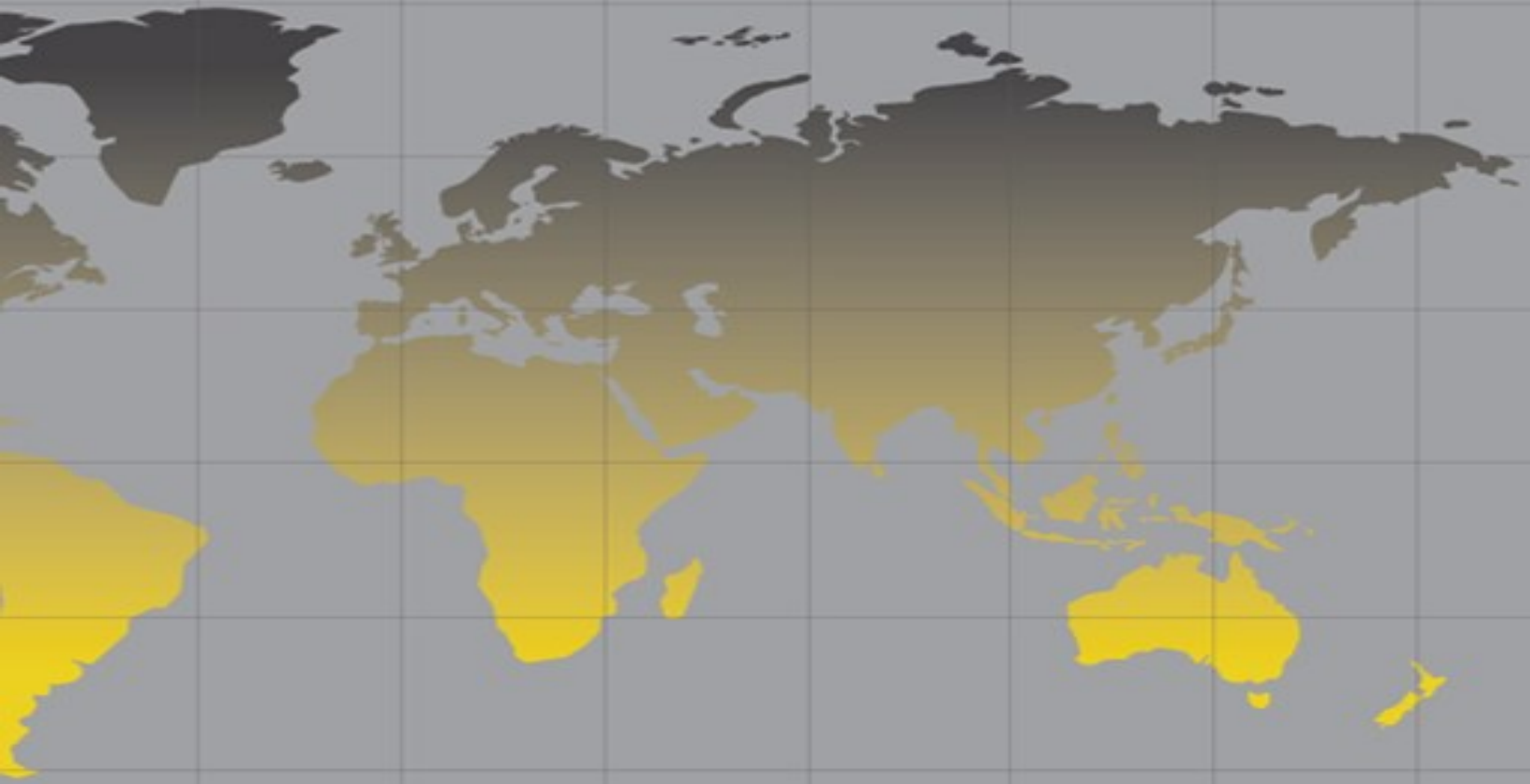
INCIDENT HANDLING

TRIAGE: SENSITIVITY 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

IDENTIFICATION & ANALYSIS

INCIDENT HANDLING



INCIDENT HANDLING

IDENTIFICATION & ANALYSIS

- Assign a handler in charge of responding / handling the incident
- Collect / Gather evidence
  - Audit trail, log files, contents of files…
- Survey situation on victim site
- Identify
  - What, Who, When, Why, How

INCIDENT HANDLING

IDENTIFICATION & ANALYSIS

Incident 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

INCIDENT HANDLING

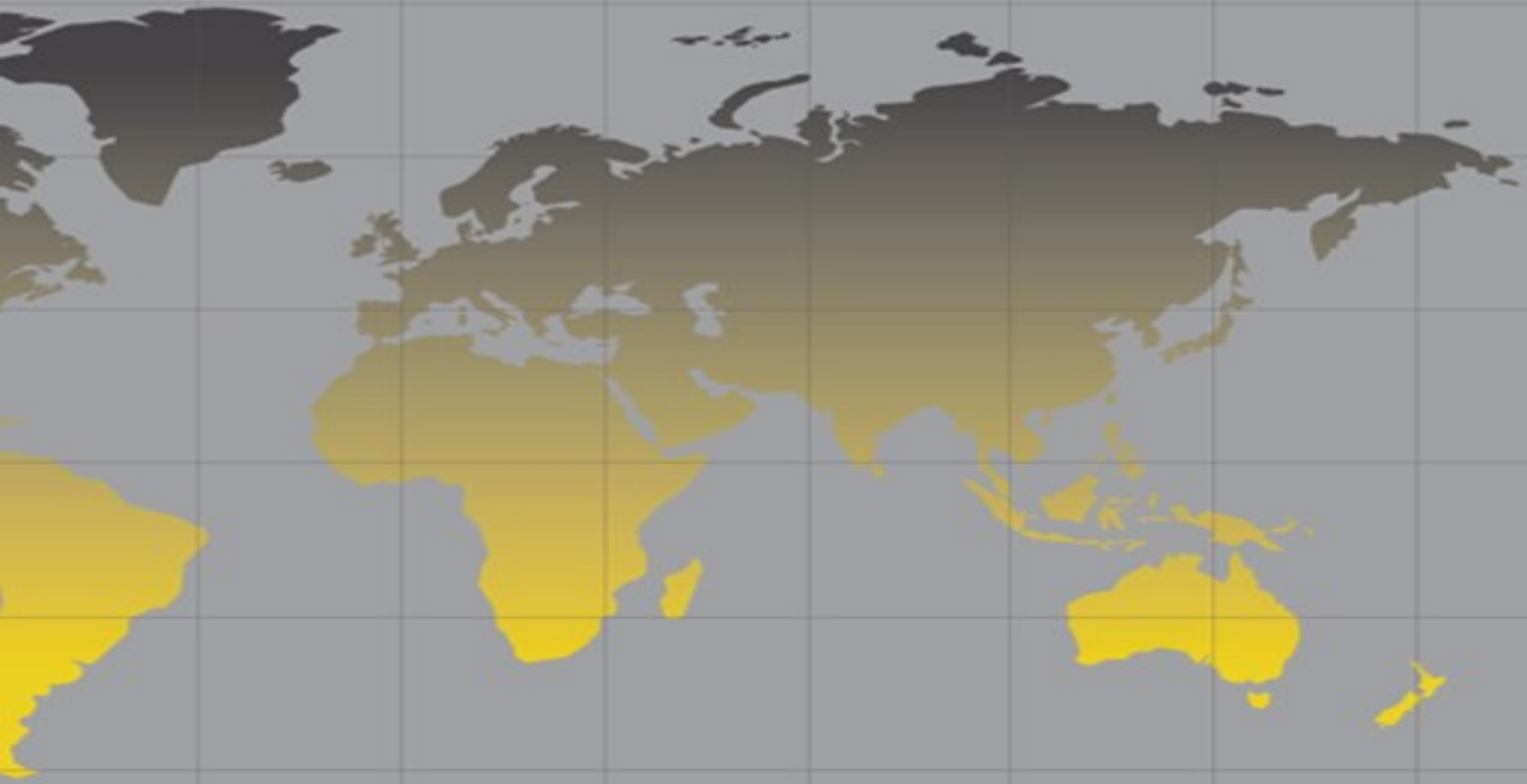
IDENTIFICATION & ANALYSIS

Evidence Collection and Archiving (RFC 3227)

- Order of Volatility
  - Registers
  - Routing table
  - Temporary file systems
  - Disk
  - Remote logging
  - Physical configuration
  - Archival media
- 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.

CONTAINMENT

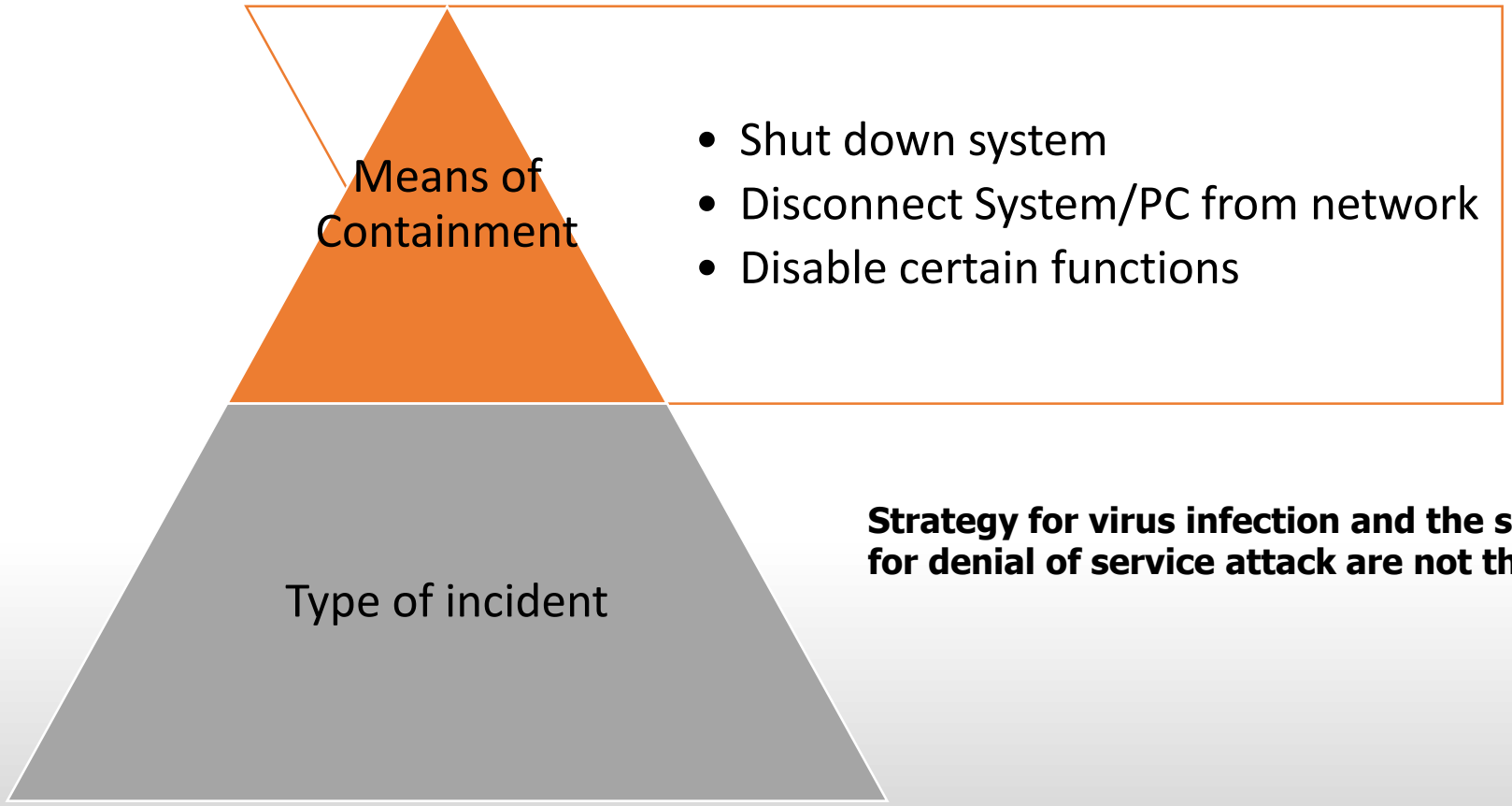
INCIDENT HANDLING



INCIDENT HANDLING

CONTAINMENT

Creating a containment strategy



- Shut down system
- Disconnect System/PC from network
- Disable certain functions

Strategy for virus infection and the strategy for denial of service attack are not the same.

INCIDENT HANDLING

CONTAINMENT

Criteria for determining the strategy include:

- Potential damage to resource
- Theft of resources
- Need for evidence preservation
- Service availability
  - (e.g.) Network connectivity, service provided to others
- Time and recourses needed to implement the strategy
- Effectiveness of the strategy
  - (e.g.) Partial or full containment
- Duration of the solution
  - (e.g.) To be removed in several week

INCIDENT HANDLING

CONTAINMENT

Delayed containment is usually NOT good.

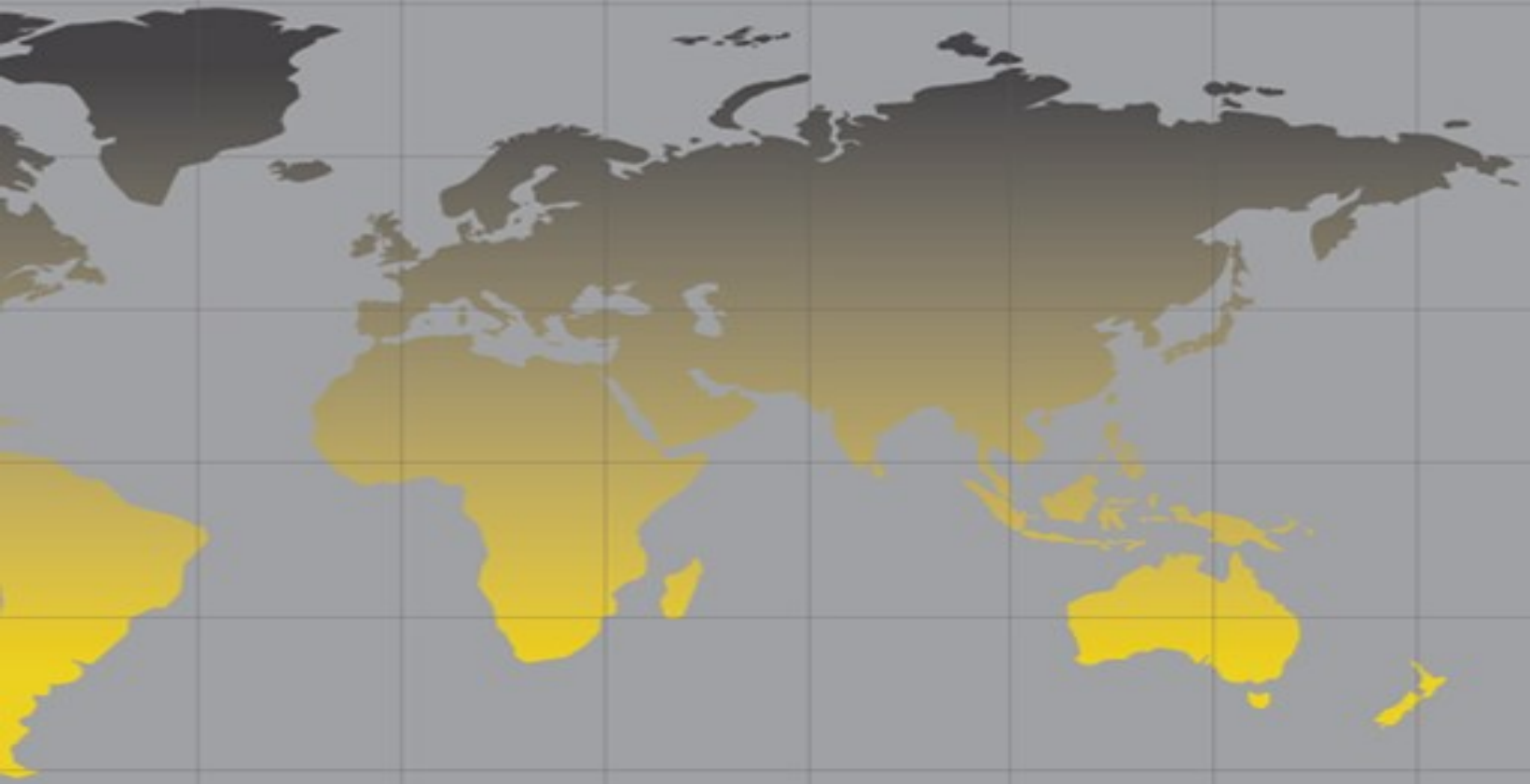
- Need additional evidence to do containment?
- Need to get approval from legal section?
- If so (above), attacker could escalate unauthorized access / compromise other system in short time…

Other potential issues

- Some attacks may cause additional damage when contained (e.g. disconnected).

ERADICATION & RECOVERY

INCIDENT HANDLING



INCIDENT HANDLING

ERADICATION & RECOVERY

Determine case & origin of incident by Evidence

Especially, the detailed log should be kept for all evidences, including:

- Identifying information
  - Location

REFERENCE
RFC 2337 “Evidence Collection and Archiving

  - phone number
  - Time and date
    - Including time zone
- Location where evidence was stored

INCIDENT HANDLING

ERADICATION & RECOVERY

Example of eradication

- Delete malicious code
- Disable breached user account

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

INCIDENT HANDLING

ERADICATION & RECOVERY

Which method would you recommend?

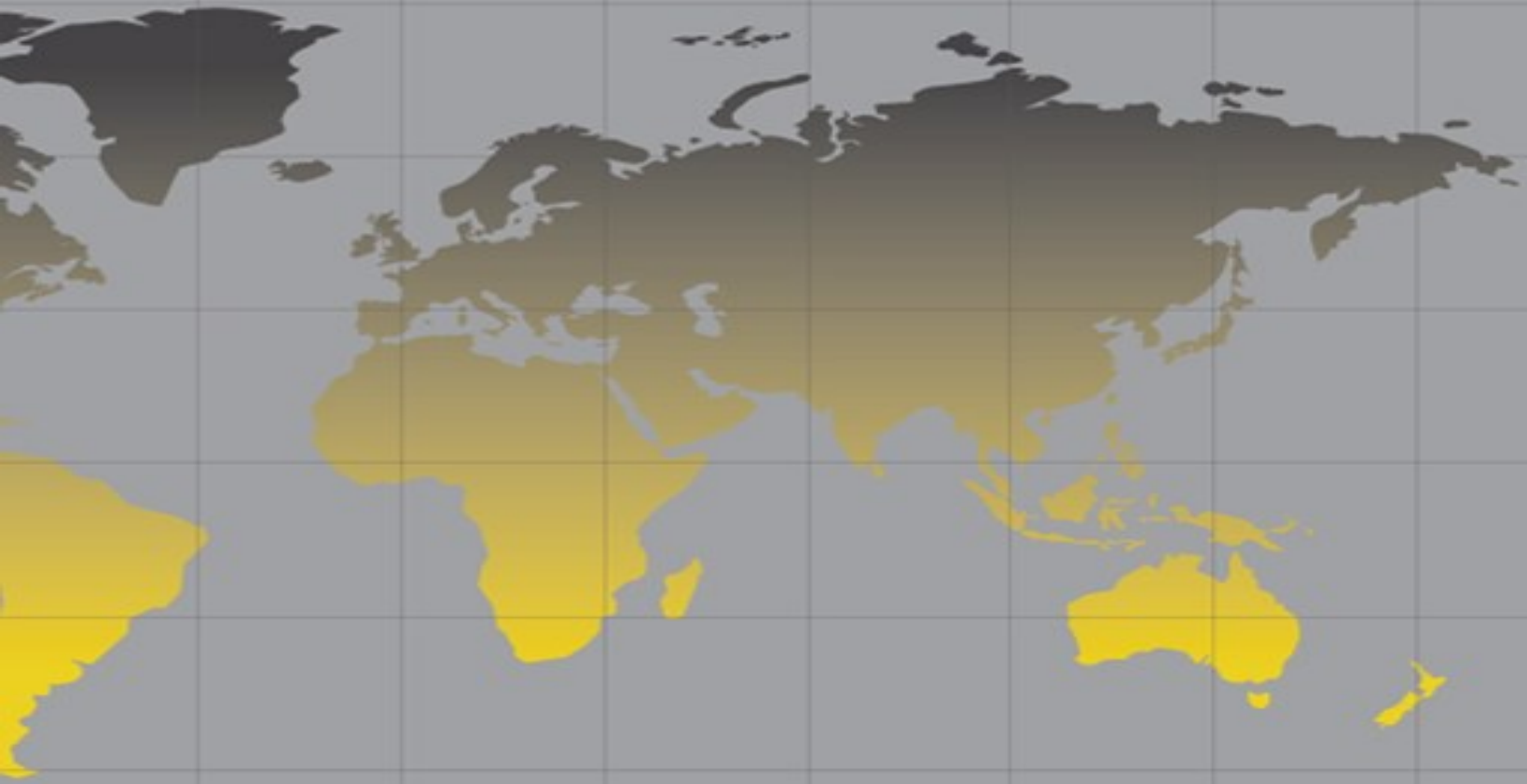
1)There is a rootkit inside a particular computer.

2)Your nations tourism department website has been defaced.

3)The email address of all the users in the prime ministers office has been leaked out.

FOLLOW UP

INCIDENT HANDLING



INCIDENT HANDLING

FOLLOW UP: DOCUMENTATION

Document what occurred in detail, including:

- Unique incident tracking number
  - To track all information and actions relating to the incident
- Keywords or categorization
  - Information to characterize the incident
  - Establish relationships between difference incidents
- Contact information
  - Name, Phone number, Email address, Other Contact information for all parties
- Policies
  - Legal parameters or policies that the way incident might be handled

INCIDENT HANDLING

FOLLOW UP: DOCUMENTATION

- 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

INCIDENT HANDLING

FOLLOW UP: COMMUNICATION

Ensure that the restored system is no longer vulnerable to the same attack type.

- Monitor the restored system.
- Provide the updated information, including:
  - Relevant incident
  - Vulnerability patch
  - Security patch
  - Different solution

INCIDENT HANDLING

FOLLOW UP: SELF LEARNING

Lesson Learned

- 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.

Be prepared for media inquiries