INCIDENT NOTIFICATION

- After an incident is analyzed and prioritized, the team needs to notify the appropriate individuals so that all who need to be involved will play their roles.
- Incident response policies should include provisions concerning incident reporting and what must be reported to whom and what times.
- During incident handling, the team may need to provide status updates to certain parties.
- The team should plan and prepare several communication methods

INCIDENT NOTIFICATION

CIO	Head of Information Security
Local Information Security Officer	Other IR Teams within the organization
External IRT	System Owner
HR (for case involving employees)	Public affairs (for incidents that may generate publicity)
Legal department (for incident with potential legal ramifications)	India-CERT
Law Enforcement (If appropriate)	

INCIDENT NOTIFICATION

- Possible Communication Methods Include
  - Email
  - Website (Internal, External, Portal)
  - Telephone calls
  - In person (e.g. Daily briefings)
  - Voice mailbox (Set up a separate voice mailbox for incident updates)
  - Paper (e.g., Post notices on bulletin boards and doors)

CONTAINMENT

- Important to decrease damage
- It provides time for developing a tailored remediation strategy
- Essential part of containment is decision-making
- Containment strategies very based on the type of incident

CONTAINMENT

- Criteria for determining the appropriate strategy include:
  - Potential damage to and theft of resources
  - Need for evidence preservation
  - Service availability
  - Time and resources needed to implement the strategy
  - Effectiveness of the strategy
  - Duration of the solution

CONTAINMENT

- Some organizations redirect the attacker to a sandbox so that they can monitor the attacker's activity, to gather additional evidence.
- If an organization knows that a system has been compromised and allows the compromise to continue, it may be liable if the attacker uses the compromised system to attack other devices
- The delayed containment is dangerous because an attacker could escalate unauthorized access or compromise other system.
- Some attacks may cause additional damage when they are contained

EVIDENCE GATHERING AND HANDLING

- The primary reason for gathering evidence is to resolve the incident and also to use it for legal proceedings.
- Important to clearly document how all evidence ,including compromised systems, has been preserved.
- Evidence should be collected according to procedures that meet all applicable laws and regulations that have been developed from previous discussions with legal staff and appropriate law enforcement agencies

EVIDENCE GATHERING AND HANDLING

- Detailed log should be kept for all evidence, including the following:
  - Identifying information (location, serial number, hostname, MAC address, IP Address)
  - Name, title and phone number of each individual who collected or handled the evidence during the investigation
  - Time and date of each occurrence of evidence handling
  - Locations where the evidence was stored.

EVIDENCE GATHERING AND HANDLING

- Collecting evidence from computing resources presents some challenges
- It is desirable to acquire evidence from a system of interest as soon as one suspects that an incident may have occurred.
- Many incidents cause a dynamic chain of events hence it is recommended to take initial system image as soon as you find the system of interest.
- From evidentiary standpoint, it is much better to get a snapshot of the system before incident handler starts investigation.

IDENTIFYING THE ATTACKING HOSTS

- During incident handling, system owners sometimes want to or need to identify the attacking host
- This may sound important but Incident handlers should stay focused on containment, eradication and recovery.
- Identifying an attacking host can be time consuming process that can prevent a team from achieving its primary goal

IDENTIFYING THE ATTACKING HOSTS

- Following items describe the most commonly performed activities for attacking host identification:
  - Validating the attacking host's IP Address
  - Researching the attacking host through search engines
  - Using Incident Databases
  - Monitoring Possible attacker communication channels

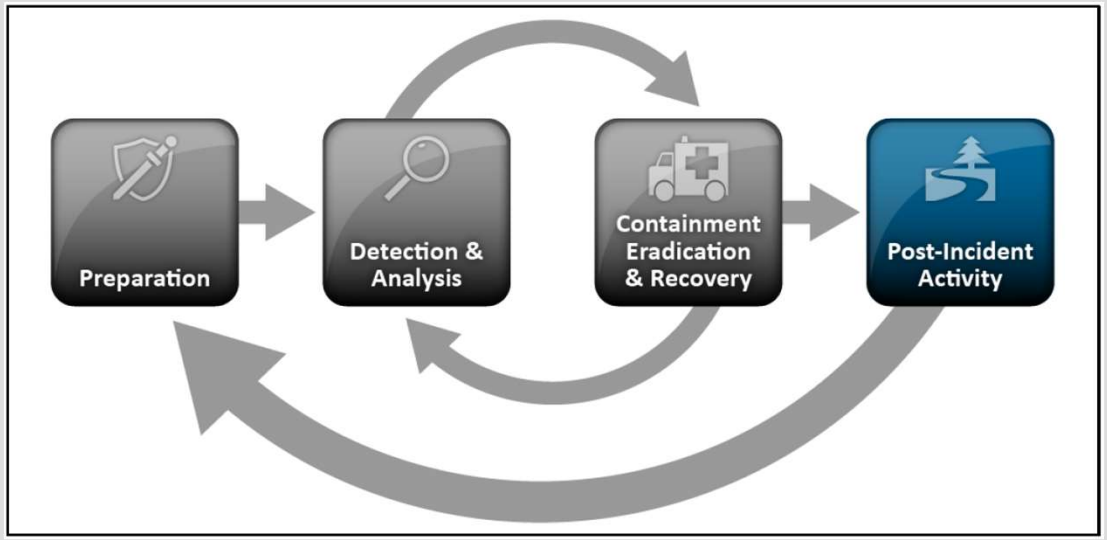
ERADICATION

- After an incident has been contained, Eradication may be necessary to eliminate components of the incident
- Removing malware, disabling breached user accounts as well as identifying and mitigating all vulnerabilities that were exploited.
- During eradication, it is important to identify all effected hosts within the organization so that they can be remediated.
- For some incidents, eradication is either not necessary or is performed during recovery.

RECOVERY

- Administrators would generally restore systems to normal operation
- Administrators also confirm that the systems are functioning normally
- It involve actions such as
  - Restoring systems from clean backups
  - Rebuilding systems from scratch
  - Replacing compromised files with clean versions
  - Installing patches
  - Changing passwords
  - Tightening network perimeter security

POST INCIDENT ACTIVITY



POST INCIDENT ACTIVITY

- It mainly includes
  - Lessons learned
  - Using Collected Incident Data
  - Evidence Retention

LESSONS LEARNED

- One of the most important parts of incident response is also the most often omitted: learning and improving
- Each incident response team should evolve to reflect new threats, improved technology and lessons learned
- Organizations generally call a "lessons learned" meeting with all involved parties after a major incident.
- It's extremely helpful in improving security measures and the incident handling process itself.

LESSONS LEARNED

- Questions to be answered in such meetings include:
  - Exactly what happened, and at what times?
  - How well did staff and management perform in dealing with the incident? Were the documented procedures followed? Were they adequate?
  - What information was needed sooner?
  - Were any steps or actions taken that might have inhibited the recovery?

LESSONS LEARNED

- Questions to be answered in such meetings include:
  - What would the staff and management do differently the next time a similar incident occurs?
  - How could information sharing with other organizations have been improved?
  - What corrective actions can prevent similar incidents in the future?
  - What precursors or indicators should be watched for in the future to detect similar incidents?
  - What additional tools or resources are needed to detect, analyze, and mitigate future incidents?

USING COLLECTED INCIDENT DATA

- Lessons learned activities should produce a set of objective and subjective data regarding each incident.
- Over the time, The collected incident data should be useful in several capacities.
- If incident data is collected and stored properly, it should provide several measures of the success of the incident response team.
- Incident data can also be collected to determine if a change to incident response capabilities causes a corresponding change in the team's performance

USING COLLECTED INCIDENT DATA

- Possible Metrics for incident-related data include:
  - Number of incidents handled
  - Time per incident
    - Total amount of labor spent working on the incident
    - Elapsed time from the beginning of the incident to each stage of of incident handling
    - How long it took the incident response team to respond to the initial report of the incident
    - How long it took to report the incident to management and if necessary, appropriate external entities like Ind-Cert

USING COLLECTED INCIDENT DATA

- Possible Metrics for incident-related data include:
  - Objective Assessment of Each incident
    - Reviewing logs, forms, reports and other incident related documentation
    - Identifying which precursors and indicators of the incident were recorded to determine how effectively the incident was logged
    - Determining if the incident caused damage before it was detected
    - Determining if the actual cause of the incident was identified

USING COLLECTED INCIDENT DATA

- Possible Metrics for incident-related data include:
  - Objective Assessment of Each incident
    - Determining if the incident is recurrence of a previous incident
    - Calculating the estimated monetary damage
    - Measuring the difference between the initial impact assessment and final impact assessment
    - Identifying which measures, if any, could have prevented the incident

USING COLLECTED INCIDENT DATA

- Possible Metrics for incident-related data include:
  - Subjective Assessment of Each Incident
    - Team members assessing their own performance as well as that of other team members and of the entire team
    - Input from the owner of the resource that was attacked
    - To determine if the owner thinks the incident was handled efficiently and if the outcome was satisfactory

EVIDENCE RETENTION

- Organization should establish policy for how long evidence from an incident should be retained
- Most organizations choose to retain all evidence for months and years after the incident ends
- Following factors should be considered during the policy creation:
  - Prosecution
  - Data Retention
  - Cost

INCIDENT RESPONSE TEAM MEMBERS ROLES

- For incident management to be successful, it is essential to carefully consider the roles within a CERT(Computer Emergency Response Team) and to tailor these to your specific mission, constituency and environment.
- A CERT can be a virtual team with no formal members and with tasks distributed between different employees in various company departments such as the network operations centre, internal IT security team, legal department, PR department, help desk, etc.
- It can also be a department in a company's organizational structure, with several core members but also with some members from different departments, who work part-time or only on a specific task. it can also be an organisation or department with only full-time members.

INCIDENT RESPONSE TEAM MEMBER ROLES

- The mandatory Roles are:
  - Duty Officer
  - Triage Officer
  - Incident handler
  - Incident Manager

DUTY OFFICER

- A duty officer has to take care of all in-coming requests as well as carry out periodic or ad hoc activities dedicated to this role.

TRIAGE OFFICER

- The triage officer has to deal with all incidents that are reported to or by the team.
- He needs to decide whether it is an incident that is to be handled by the team, when to handle it and who is going to be the incident handler according to the triage process

INCIDENT HANDLER

- The incident handler is a crucial role in the incident handling team.
- He deals with the incidents analyzing data, creating workarounds, resolving the incident and communicating clearly about the progress he has made to his incident manager and to and with the appropriate constituent(s).

INCIDENT MANAGER

- The incident manager is responsible for the coordination of all incident handling activities.
- He represents the incident handling team outside his team

INCIDENT RESPONSE TEAM STRUCTURE

- Possible structures for an incident response team include the following:
  - Central Incident Response Team
  - Distributed Incident Response Team
  - Coordinating Team
  - Employees
  - Partially Outsourced
  - Fully Outsourced

CENTRAL INCIDENT RESPONSE TEAM

- A single incident response team handles incidents throughout the organization.
- This model is effective for small organizations and for organizations with minimal geographic diversity in terms of computing resources.

DISTRIBUTED INCIDENT RESPONSE TEAM

- The organization has multiple incident response teams, each responsible for a particular logical or physical segment of the organization.
- This model is effective for large organizations (e.g., one team per division) and for organizations with major computing resources at distant locations (e.g., one team per geographic region, one team per major facility).

COORDINATING TEAM

- An incident response team provides advice to other teams without having authority over those teams—for example, a department wide team may assist individual agencies' teams.

EMPLOYEES

- The organization performs all of its incident response work, with limited technical and administrative support from contractors.

PARTIALLY OUTSOURCED

- The organization outsources portions of its incident response work.

FULLY OUTSOURCED

- The organization completely outsources its incident response work, typically to an onsite contractor.
- This model is most likely to be used when the organization needs a full-time, onsite incident response team but does not have enough available, qualified employees.