Chapter 4

After Incident Detection

Ed Crowley

Spring 10

Topics

- Incident Response Process
- SANs Six Step IR Process
  1. Preparation
  2. Identification
  3. Containment
  4. Eradication
  5. Recovery
  6. Lessons learned
  7. Lessons learned feeds back into preparation
- Obtaining Preliminary Information
- Establishing an Incident Notification Procedure
- Recording Details after Initial Detection
- Incident Declaration
- Assembling the CSIRT
- Determining Escalation Procedures
- Implementing Notification Procedures
- Scoping an Incident
- Perform Traditional Investigative Steps
- Interviews
- Formulating a Response Strategy

Incident Response Process

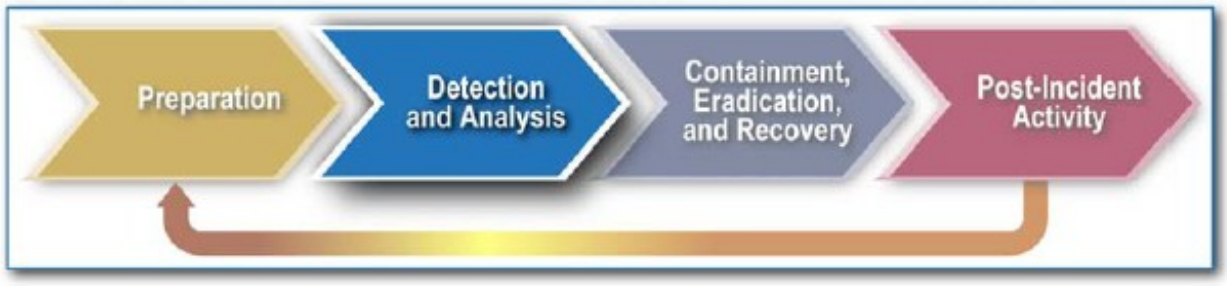

Figure 3-2. Incident Response Life Cycle (Detection and Analysis)

Focus on the initial response after detection i.e. detection and analysis. *(NIST 800-31).*

1. Preparation
2. Detection and Analysis
3. Containment, Eradication, and Recovery
4. Post-Incident Activity

SANs Compatible

Six Step Incident Handling Process Loop

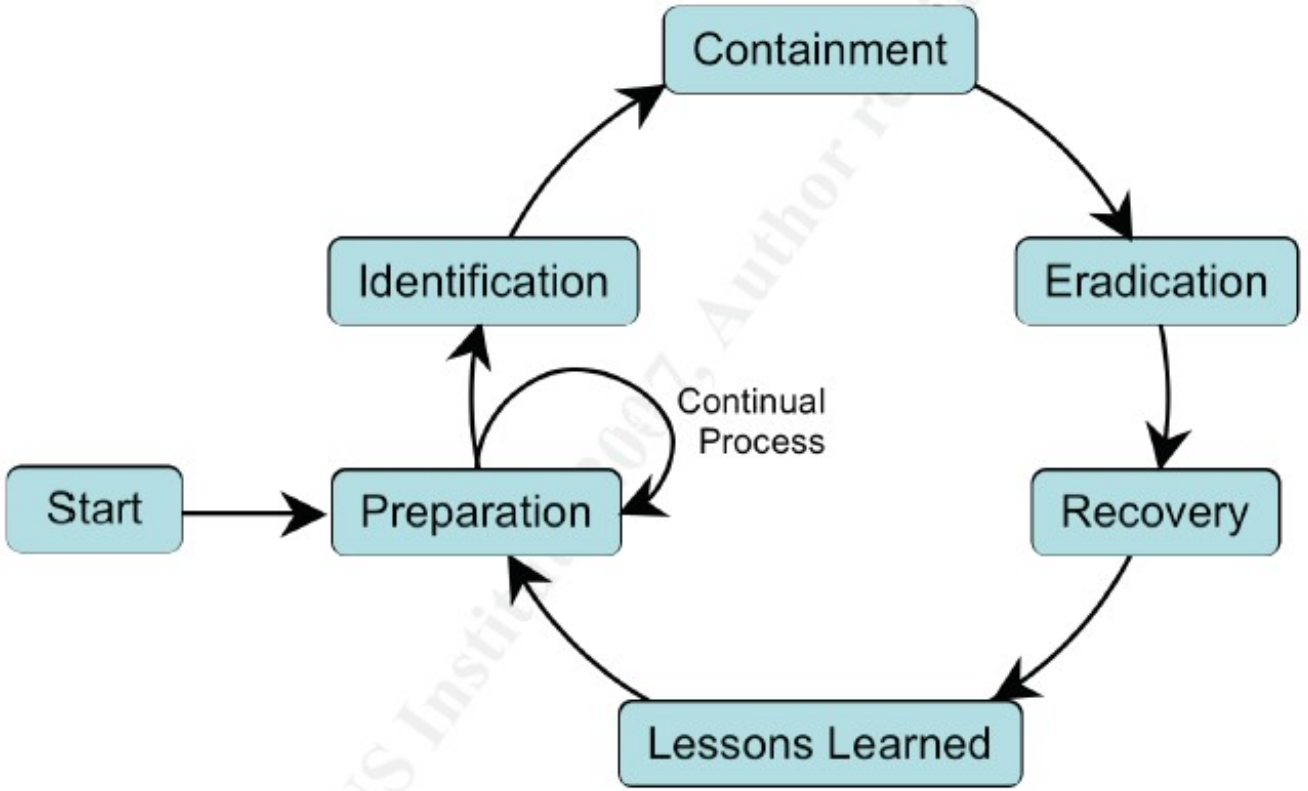

Figure 1: Six-Step Incident Handling Process Loop

Illustration from SANs.

Overview of Initial Response Phase

IR Process attributes

- Rapid and effective decision making
- Rapid accumulation of forensically sound information
- Appropriate incident escalation
- Rapid notification of the participants required to assemble CSIRT

Obtaining Preliminary Information

Goal

Obtain enough information to determine appropriate response.

May include:

- Initial incident notification
- Recording details
- CSIRT assembly
- Traditional investigative steps
- Conducting interviews
- Determining whether the incident is to be escalated

Establishing an Incident Notification Procedure

- Requires all employees to participate
- Establish procedure for users to report potential computer security incident(s)
- Make an initial response checklist for help desk employees who are not security professionals.

Initial Response Checklist

- Incident date
- Reporter's contact info
- Incident:
  - Type
  - Location
  - Date incident first noticed
- Location's physical security description
- How incident was detected
- Since incident , who accessed or touched relevant systems?
- Who has had physical access to system?
- Who knows about incident?

Initial Response Checklist, Second Section

System Details

- Make and model
- Operating system
- Primary system users
- Sys admin
- IP & MAC addresses
- System network name
- Resident critical info

- Incident contained or ongoing?
- Network monitoring needed?
- System still connected?
- Backup tapes?
- Employee need to know?
- Remedial steps?
- Information storage

Case Names and Notes

- Case notes are any documentation that records steps taken during incident response process

Incident Declaration

- In a few cases, it may be difficult to determine if an incident occurred.
  - That is, difficult based on details recorded in the initial response checklist.

Check

- Scheduled maintenance
- Unscheduled downtime
- Recent system upgrades, patches, etc?
- Testing?
- Employee suspicions

Assembling the CSIRT

- Many organizations utilize dynamic CSIRTs in response to a particular situation or incident.
  - In contrast to an established, centralized team dedicated to incident response.
- One of incident response's biggest challenges is knowing who, and when, to contact

Determining Escalation Procedures

- For each incident, a determination must be made as to whether the incident will be handled at the local or at the corporate level.

Implementing Notification Procedures

- Organizations need a central contact point.
  - And a notification checklist
- Points of contact that need to be maintained:
  - HR
  - General counsel
  - Network operations
  - Corporate investigations
  - Physical security
  - Outside LE
  - Other business units

Internal Investigations

- Often require a different notification process than external security incidents.

Notification should only include people that:

- Need to know and can help
- Will not be confused, panicked, otherwise hinder the investigation
- Are not close friends of the suspects

- Should employ the “need to know” principle

Scoping an Incident

IR requires

- Rapid decisions
- A capable principal investigator

Size of team depends upon number of involved:

- Hosts
- O/Ss
- Systems

- Investigation Timeframe
- Potential exposure or case profile
- Litigation likelihood
- Subjects awareness of investigation

Assigning a Team Leader

All computer related investigations require professionals who understand the incident's:

- Technical aspects
- Computer security incident investigative process

Team Leader's Tasks

- Manage
  - CSIRT
  - Interview process
- Provide status
- Ensure utilization of best practices
- Provide overall incident analysis
- Protect evidence
  - Verify evidence's chain of custody
- If necessary, perform forensic duplication and analysis
- Compile, manage, and present the investigative report
  - Offer management recommendations
- Understand
  - Legal issues
  - Corporate policies
- Provide an unbiased investigation

Technical Staff

- Often part time or temporary

Need to have

- Complete O/S knowledge
- Ability to review logs, audit trails, other trace evidence
- Understand evidence handling process
- Perform proper damage assessments
- Assist in determining incident scope
- Determine incident nature
  - Identify specific technical details
- Maintain perspective
- Document everything
- Support team leader
- When needed, perform interviews

Perform Traditional Investigative Steps

- Host based evidence
- Network based evidence
- Other evidence

Sample Interview Questions

- What happened?
- When did it happen?
- What systems are relevant /compromised/involved?
- Who did it?
- Who uses affected/relevant systems?
- What actions have already been taken?
- What is the relevant corporate policy?

Interviewees

- System Administrators
- Managers
- End Users

Formulating a Response Strategy

- Likely, response strategy development will be an iterative process.
  - Many options examined before final response strategy is implemented.
- Policy Verification

Questions?