National Forensic Sciences University

An Institution of National Importance
Ministry of Home Affairs, Government of India

Incident Response Management & Threat Intelligence

Incident Handling

Presented By:
Mr. Ramya Shah
Assistant Professor,
SCSDF, NFSU

Goals of Incident Response

1. Verify that an incident occurred.
2. Maintain or Restore Business Continuity.
3. Reduce the incident impact.
4. Determine how the attack was done (i.e. the incident happened).
5. Prevent future attacks or incidents.
6. Improve security and incident response.
7. Prosecute illegal activity.
8. Keep management informed of the situation and response.

Incident Response Plan

- An Incident Response Plan (IRP) is needed because attacks frequently compromise data within organizations.
- Organizations should have a formal, focused, and coordinated approach to responding to incidents, including an incident response plan that provides the roadmap for implementing the incident response capability.
- Each organization needs a plan that meets its unique requirements, which relates to the organization's mission, size, structure, and functions.
- The plan should lay out the necessary resources and management support.

Elements of Incident Response Plan

- Mission
- Strategies and goals
- Senior management approval
- Organizational approach to incident response
- How the incident response team will communicate with the rest of the organization and with other organizations
- Metrics for measuring the incident response capability and its effectiveness
- Roadmap for maturing the incident response capability
- How the program fits into the overall organization.

Three Functions

- **Incident Reporting :**
  - Such functions enables a CERT to serve as a central point of contact for reporting problems
  - Allows all incidents reports and activity to be collected in one location
  - Here, Information can be reviewed and correlated across the organization
  - Information can then be used to determine patterns of intruders or activity
- **Incident Analysis**
- **Incident Response**

Three Functions

- **Incident Reporting**
- **Incident Analysis**
- **Incident Response:**
  - It can take many forms
  - A CERT may send out recommendations for recovery, containment and prevention of systems
  - Network administrators at sites then performs the response steps themselves
  - CERT may also perform these steps themselves but only, when network administrators are unable to mitigate the problem
  - Share information and lessons learned with other team members

SANS Institute Recommendations

- The SANS Institute is a private U.S. for-profit company founded in 1989.
- Specializes in information security, cybersecurity training and selling certificates.
- Topics available for training include cyber and network defenses, penetration testing, incident response, digital forensics, and audit.
- According to them, There are six steps to handle an incident most effectively

Steps to Handle an Incident ~ SANS

- Preparation
- Identification
- Containment
- Eradication
- Recovery
- Learning Lesson

Steps to Handle an Incident ~ SANS

Preparation: Preventing Incidents

- Risk Assessments
- Host Security
- Network Security
- Malware Prevention
- User Awareness and Training

Steps to Handle an Incident ~ SANS

Identification : ATTACK VECTORS

- External/Removable Media
- Web
- Email
- Impersonation
- Improper Usage
- Loss or Theft of Equipment
- Other

Steps to Handle an Incident ~ SANS

Identification : Sources of Precursors and Indicators

- Alerts
  - IDS & IPS
  - SIEMs
  - Antivirus
  - File integrity checking software
  - Third Party monitoring service

Steps to Handle an Incident ~ SANS

Identification : Sources of Precursors and Indicators

- Logs
  - OS logs
  - Service Logs
  - Application Logs
  - Network Logs

Steps to Handle an Incident ~ SANS

Identification : Sources of Precursors and Indicators

- Publicly Available Information:
  - Information on new Vulnerabilities
- People:
  - People from within the organization
  - People from other organizations

Steps to Handle an Incident ~ SANS

Incident analysis :

- Incident detection and analysis is generally easy if all precursor or indicator are guaranteed to be accurate; however, that may not be the case sometimes.
- User provided indicators such as a complain a server being unavailable can be incorrect.
- IDS may produce false positive
- Each indicators ideally should be evaluated to determine if it is a legitimate or not. But, depending on an organization, number of indicators may be thousands or millions a day.
- Such scenarios makes incident analysis a difficult task

Steps to Handle an Incident ~ SANS

Incident analysis : First Hand / Initial Analysis

- Profile networks and systems
- Understand normal behaviors
- Create a log retention policy
- Perform event correlation
- Keep all host clocks synchronized

Steps to Handle an Incident ~ SANS

Incident analysis : Recommendations for performing initial analysis

- Maintain and Use a Knowledge base of information
- Use Internet search engines for research
- Run Packet sniffers to collect additional data
- Filter the data
- Seek assistance from others

Steps to Handle an Incident ~ SANS

Incident Documentation:

- An IR team that suspects that an incident has occurred should immediately start recording all facts regarding the incident
- A logbook is an effective and simple medium for this, but laptops, audio recorders and digital cameras can also serve this purpose.
- It leads to more efficient, more systematic and less error-prone handling of the problem.
- Every step taken from the time the incident was detected to its final resolution should be documented and timestamped and signed by the incident handlers.

Steps to Handle an Incident ~ SANS

Incident Documentation: The issue tracking system should contain information on the following:

- The current status of the incident
- A summary of the incident
- Indicators related to the incident
- Other incidents related to this incident
- Actions taken by all incident handlers on this incident
- Chain of custody, [if applicable]

Steps to Handle an Incident ~ SANS

Incident Prioritization:

- It can be considered as the most critical decision point in the incident handling process
- Incidents should NEVER be handled on first-come first-served basis
- Incident should always be prioritized on the relevant factors
- **The relevant factors are as follow:**
  - Functional Impact of the Incident
  - Information Impact of the Incident
  - Recoverability from the Incident

Steps to Handle an Incident ~ SANS

Incident Prioritization: Functional Impact

- Incidents targeting IT systems typically impact the business functionality that those system provide
- It can leave negative impact to the users of those systems
- Handlers should consider how the incident will impact the existing functionality of the affected systems.

Steps to Handle an Incident ~ SANS

Incident Prioritization: Functional Impact

Category	Definition
None	No effect to the organization's ability to provide all services to all users
Low	Minimal effect; the organization can still provide all critical services to all users but has lost efficiency
Medium	Organization has lost the ability to provide a critical service to a subset of system users
High	Organization is no longer able to provide some critical services to any users

Steps to Handle an Incident ~ SANS

Incident Prioritization: Information Impact

- Incidents may affect the confidentiality, integrity and availability of the organization's information.
- For example, A malicious agent may exfiltrate sensitive information.
- Incident handlers should consider how this information exfiltration will impact the organization's overall mission.

Steps to Handle an Incident ~ SANS

Incident Prioritization: Informational Impact

Category	Definition
None	No information was exfiltrated, changed, deleted, or otherwise compromised
Privacy Breach	Sensitive personally identifiable information (PII) of taxpayers, employees, beneficiaries, etc. was accessed or exfiltrated
Proprietary Breach	Unclassified proprietary information, such as protected critical infrastructure information (PCII), was accessed or exfiltrated
Integrity Loss	Sensitive or proprietary information was changed or deleted

Steps to Handle an Incident ~ SANS

Incident Prioritization: Recoverability from the Incident

- The size of the incident and the type of resources it affects will determine the amount of time and resources that must be spent on recovering from that incident.
- In fact, In some instances it is never possible to recover from an incident

Steps to Handle an Incident ~ SANS

Incident Prioritization: Recoverability from the Incident

Category	Definition
Regular	Time to recovery is predictable with existing resources
Supplemented	Time to recovery is predictable with additional resources
Extended	Time to recovery is unpredictable; additional resources and outside help are needed
Not Recoverable	Recovery from the incident is not possible (e.g., sensitive data exfiltrated and posted publicly); launch investigation

Steps to Handle an Incident ~ SANS

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

Steps to Handle an Incident ~ SANS

Incident Notification : Communication Possible Methods

- 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)

Steps to Handle an Incident ~ SANS

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

Steps to Handle an Incident ~ SANS

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

Steps to Handle an Incident ~ SANS

Evidence Gathering & 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.

Steps to Handle an Incident ~ SANS

Identifying the attacking hosts:

- Validating the attacking host's IP Address
- Researching the attacking host through search engines
- Using Incident Databases
- Monitoring Possible attacker communication channels

Steps to Handle an Incident ~ SANS

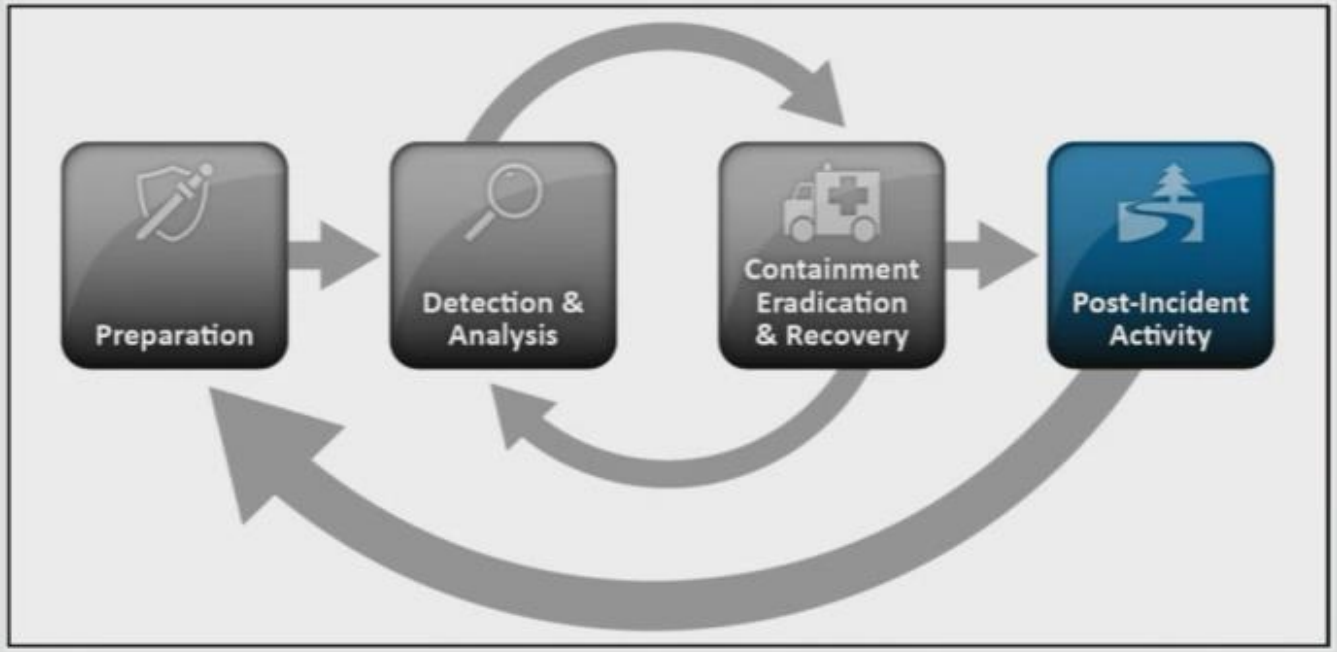
Eradication:

- 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.

Steps to Handle an Incident ~ SANS

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 : Lesson's Learned

- 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.

POST INCIDENT ACTIVITY : Lesson's Learned

Questions to be Asked & Answered :

- 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?

POST INCIDENT ACTIVITY : Lesson's Learned

Questions to be Asked & Answered :

- 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?

Points Discussed

- **Incident at an hospital**. Systems were down, cannot perform day to day services, how did the hospital face problems.
- Hospital was clueless about how, what, when the incident happened.
- How did the IR team initiated the process with what kinds of SOPs