3.1 Introduction.

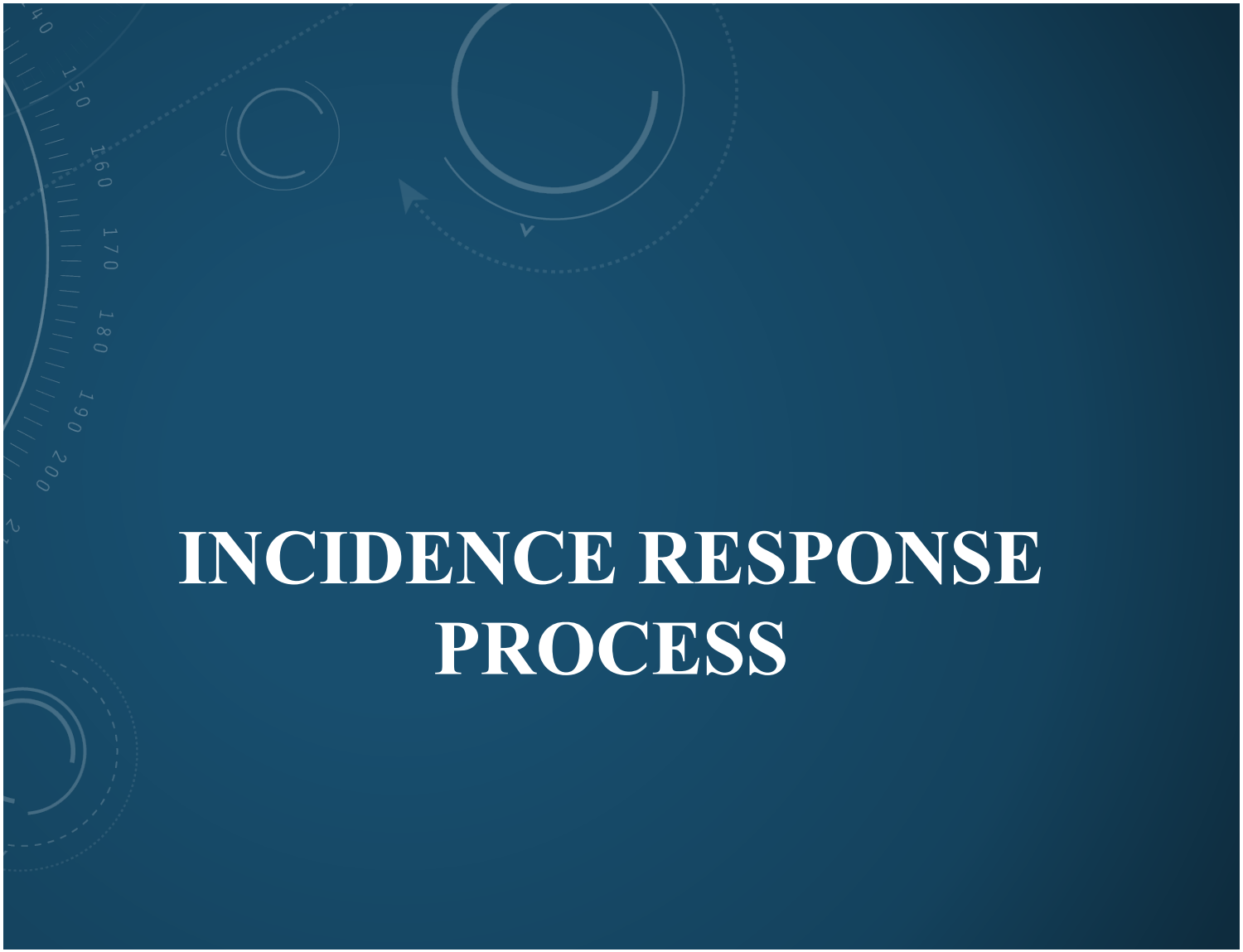
3.2 People Involved in Incident Response Process.

3.3 Incident Response Process.

3.4 Incident Response Methodology.

3.5 Activities in Initial Response.

3.6 Phases after Detection of an Incident.



3.1 Introduction.

3.2 People Involved in Incident Response Process.

3.3 Incident Response Process.

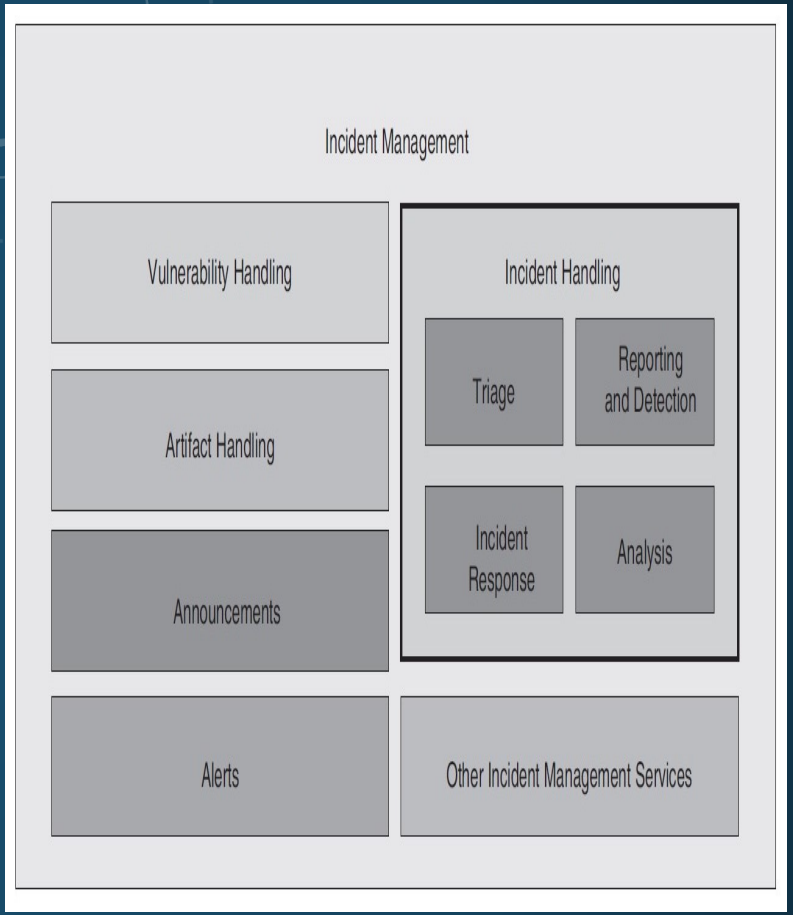
3.4 Incident Response Methodology.

3.5 Activities in Initial Response.

3.6 Phases after Detection of an Incident.

Introduction :

According to incidence response (IR) investigator team, they have responded to a gamut of incidents: criminal incidents, incidents that involved civil litigation, and incidents that disrupted business but were not actionable (cases where criminal or civil action was improbable). They also have developed incident response plans for numerous organizations, ranging from financial services institutions to companies that produce mainstream products.



3.1 Introduction.

3.2 People Involved in Incident Response Process.

3.3 Incident Response Process.

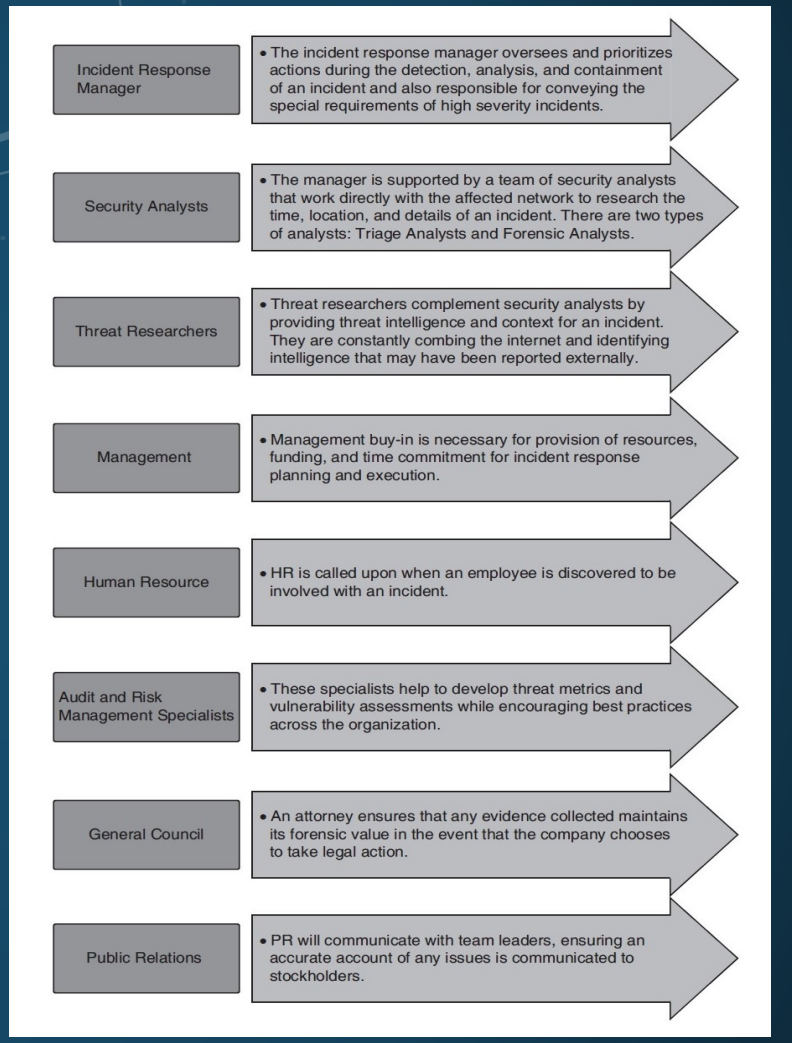
3.4 Incident Response Methodology.

3.5 Activities in Initial Response.

3.6 Phases after Detection of an Incident.

People Involved in Incident Response Process :

The main quality of incident response is that they have a multisided discipline. Hence, the people involved in incident response process should belong to various multidiscipline field. To properly prepare for and address incidents across the organization, a centralized incident response team should be formed. This team is responsible for analyzing security breaches and taking any necessary responsive measures. The incident response team should not be exclusively responsible for addressing security threats.



3.1 Introduction.

3.2 People Involved in Incident Response Process.

3.3 Incident Response Process.

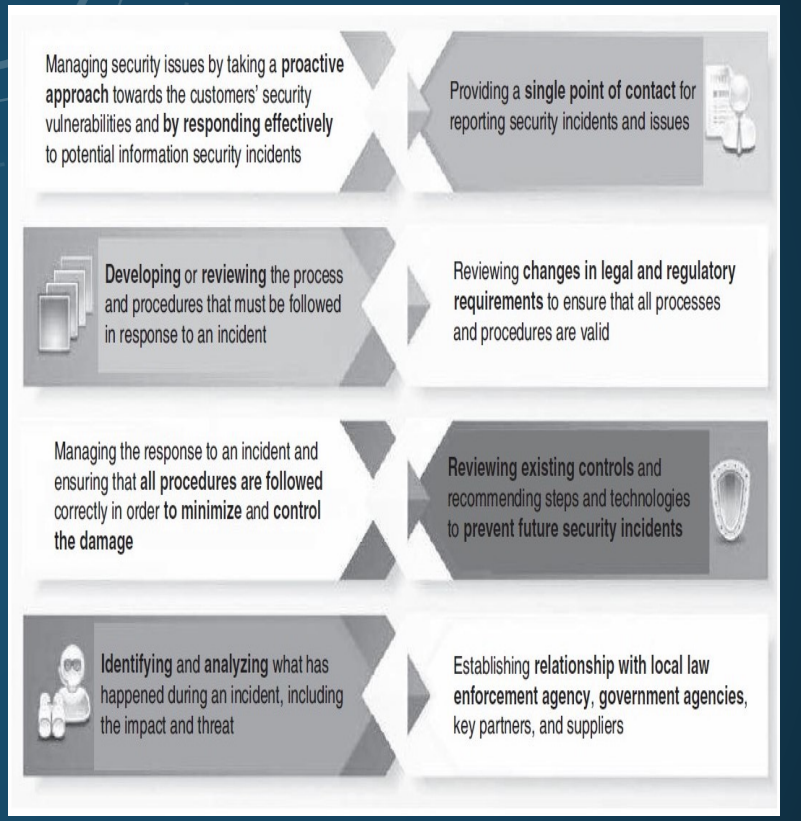
3.4 Incident Response Methodology.

3.5 Activities in Initial Response.

3.6 Phases after Detection of an Incident.

Role of Computer Security in Incident Response Team :

There is always a division between human resources who investigate laptop security incidents and people
who investigate normal crimes. Separate functions for company security human resources and laptop security
human resources area units are characterized by several companies. Network attacks (e.g., laptop intrusions and
Denial of Service attacks) are solely responded to by Computer Security Incident Response Team. The security
officers or corporate investigators perform the investigation once an additional crime is committed.



3.1 Introduction.

3.2 People Involved in Incident Response Process.

3.3 Incident Response Process.

3.4 Incident Response Methodology.

3.5 Activities in Initial Response.

3.6 Phases after Detection of an Incident.

Incident Response Process :

1. Initial Response : Initial response includes those activities that respond to an incident: policies, tools, procedures, effective governance and communication plans.
2. Investigation : Investigation is the phase where team personnel determine the priority, scope, and root cause of the incident.
3. Remediation : Remediation is the post-incident repair of affected systems, communication and instruction to affected parties, and analysis that confirms the threat has been contained.
4. Tracking of Significant Investigative Information :

1. **List of evidence collected**
2. **List of affected systems**
3. **List of any files of interest**
4. **List of accessed and stolen data**
5. **List of significant attacker activity**
6. **List of network-based IOCs**
7. **List of host-based IOCs**
8. **List of compromised accounts**
9. **List of ongoing and requested tasks for your teams**

5. Reporting : All incident response activities will be documented to include artifacts obtained using methods consistent with chain of custody and confidentiality requirements.

3.1 Introduction.

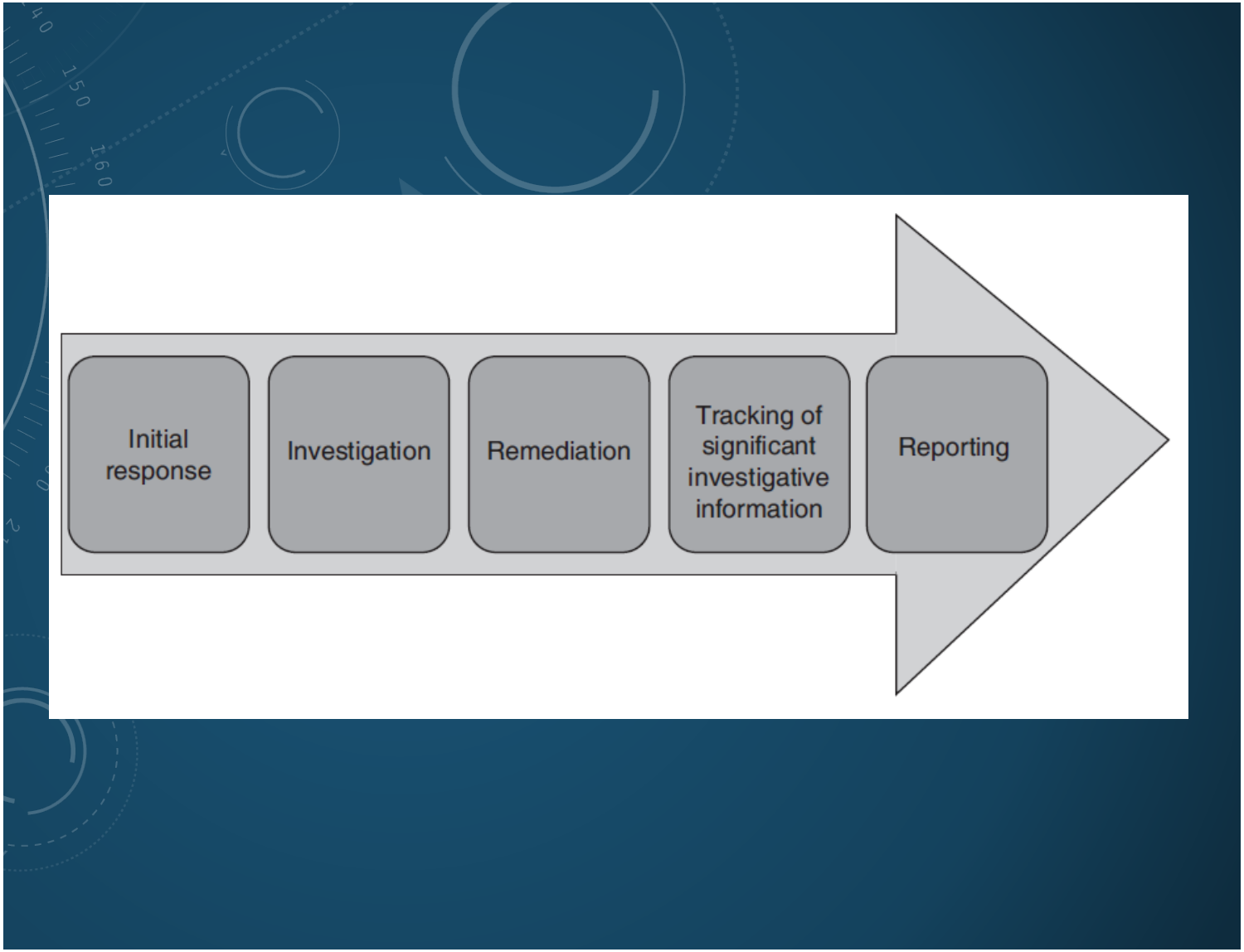
3.2 People Involved in Incident Response Process.

3.3 Incident Response Process.

3.4 Incident Response Methodology.

3.5 Activities in Initial Response.

3.6 Phases after Detection of an Incident.



3.1 Introduction.

3.2 People Involved in Incident Response Process.

3.3 Incident Response Process.

3.4 Incident Response Methodology.

3.5 Activities in Initial Response.

3.6 Phases after Detection of an Incident.

Incident Response Methodology :

1. Pre-incident preparation: Before an incident occurs, take necessary actions to prepare the organization
and the CSIRT.
2. Detection of incidents: Recognizing a probable computer security incident.
3. Initial response: By recording the basic particulars of surrounding the incident, collecting the incident response team, and informing the individuals who need to know about the incident, the initial response team performs an initial investigation.
4. Formulate response strategy: Regulate the best response team and gain the management approval
based on the outcomes of all the known facts. On the basis of conclusions, try to regulate the civil,
criminal, administrative, or other actions which are appropriate to be drawn from the investigation.
5. Investigate the incident: Perform a comprehensive collection of data, to determine what happened,
when it happened, who did it, and how it can be prevented in the future.
6. Reporting: Flawlessly report information about the investigation in such a manner that it becomes
useful to decision makers.

3.1 Introduction.

3.2 People Involved in Incident Response Process.

3.3 Incident Response Process.

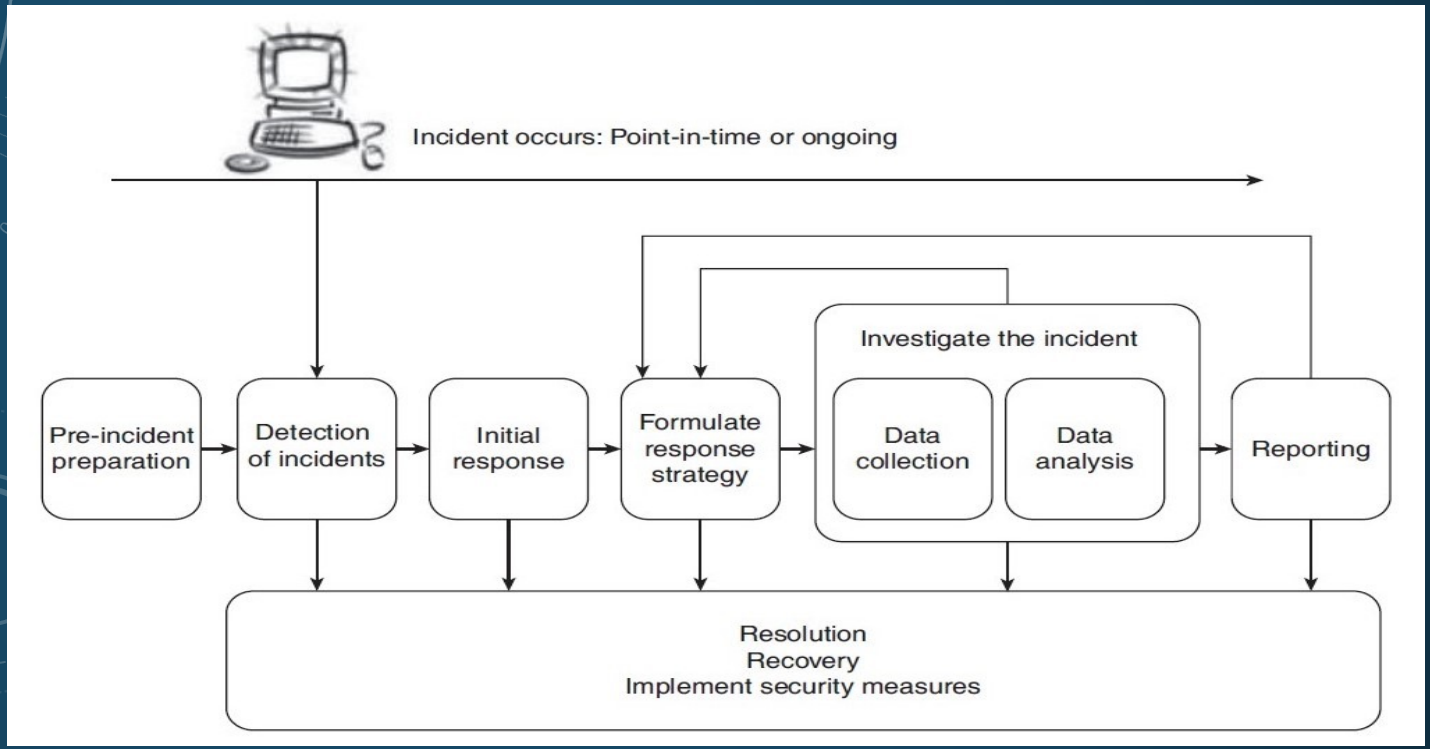
3.4 Incident Response Methodology.

3.5 Activities in Initial Response.

3.6 Phases after Detection of an Incident.

Incident Response Methodology :

7. Resolution: Various resolutions must be taken such as employing security measures and procedural
changes, recording of lessons learned and development of long-term fixes for any problems identified.



3.1 Introduction.

3.2 People Involved in Incident Response Process.

3.3 Incident Response Process.

3.4 Incident Response Methodology.

3.5 Activities in Initial Response.

3.6 Phases after Detection of an Incident.

Incident Response Methodology :

Pre-Incident Preparation :

1. Preparing the organization: Developing all of the corporate-wide strategies you need to employ to
get better position of your organization for incident response is what all is required for preparation.

Preparation of an organization includes:

(a) Host-based security actions should be implemented.
(b) Network-based security procedures should be implemented.
(c) Training for eventual users.
(d) Intrusion detection system (IDS) should be active.
(e) Formation of strong access control.
(f) Performance of timely weakness assessments.
(g) Safeguarding backups which are achieved on a regular basis.

3.1 Introduction.

3.2 People Involved in Incident Response Process.

3.3 Incident Response Process.

3.4 Incident Response Methodology.

3.5 Activities in Initial Response.

3.6 Phases after Detection of an Incident.

Incident Response Methodology :

Pre-Incident Preparation :

2. Preparing the computer security incident response team: During the pre-incident preparation
phase, the CSIRT is defined. Your organization needs to assemble a team of experts to handle any
incidents that occur. Preparing the CSIRT includes:

(a) To investigate computer security incidents, hardware is needed.

(b) To investigate computer security incidents, software is needed.

(c) To investigate computer security incidents, documentation (forms and reports) are needed.

(d) To implement your response strategies, there should be appropriate policies and operating
procedures.

e) To perform incident response in such a manner that it promotes successful forensics, investigations,
and remediation; train your staff or employees.

3.1 Introduction.

3.2 People Involved in Incident Response Process.

3.3 Incident Response Process.

3.4 Incident Response Methodology.

3.5 Activities in Initial Response.

3.6 Phases after Detection of an Incident.

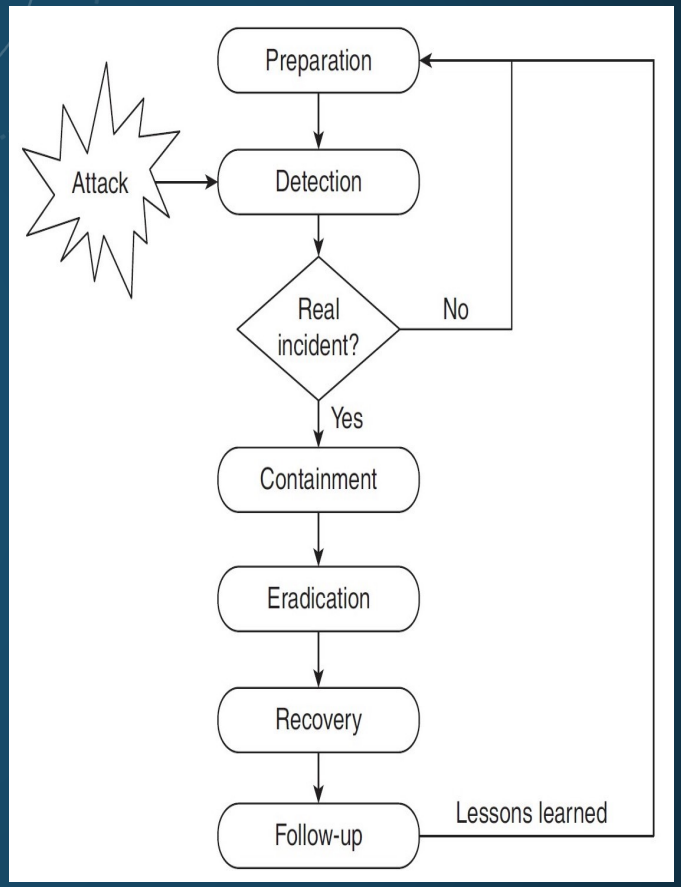
Incident Response Methodology :

Detection of Incident :

It cannot be successful in response to incidents if an organization cannot notice or sense incidents successfully.

Therefore, one of the most important features of incident response is the detection of incident's phase

It is also one of the most disjointed phases, in which incident response proficiency has only slight control.



3.1 Introduction.

3.2 People Involved in Incident Response Process.

3.3 Incident Response Process.

3.4 Incident Response Methodology.

3.5 Activities in Initial Response.

3.6 Phases after Detection of an Incident.

Incident Response Methodology :

Initial Response :

Initial response
phase involves:

1. Interviewing system administrators of an incident who might have an understanding of the technical
details.

2. Interviewing business unit human resource that may provide a context for the incident, which might
have an understanding into the business events.

3. To identify data-reviewing intrusion detection reports and network-based logs of the incident that
would support that an incident has occurred.

4. To determine if any avenues of attack can be ruled out, review the network topology and access control
lists of an incident.

3.1 Introduction.

3.2 People Involved in Incident Response Process.

3.3 Incident Response Process.

3.4 Incident Response Methodology.

3.5 Activities in Initial Response.

3.6 Phases after Detection of an Incident.

Incident Response Methodology :

Formulate Response Strategy :

1. Considering the totality of the circumstances
2. Considering appropriate responses
3. Taking action
4. Legal action
5. Administrative action

Incident	*Example*	*Response strategy*	*Likely outcome*
DoS attack	TFN DDoS attack (a popular Distributed Denial of Service attack).	Reconfigure router to minimize effect of the flooding.	Effects of attack mitigated by router Counter measures. Establishment of perpetrator's identity may require too many resources to be worth while investment.
Unauthorized use	Using work computers to surf pornography sites.	Possible forensic duplication and investigation. Interview with suspect.	Perpetrator identified, and evidence collected for disciplinary action. Action taken may depend on the employee's position or past enforcement of company policy.
Vandalism	Defaced web site.	Monitor, repair, and investigate web site while it is online. Implement web site "refresher" program.	Web site restored to operational status. Decision to identify perpetrator may involve law enforcement.
Theft of information	Stolen credit card and customer information from company database.	Make public affairs statement, forensic duplication of relevant systems, and investigation of theft.	Detailed investigation initiated. Law enforcement participation possible. Civil complaint filed to recover potential damages. Systems potentially offline for some time.
Computer intrusion	Remote administrative access via attacks such as CMSs buffer overflow and Internet Information Services (IIS) attacks.	Monitor activities of attacker. Isolate and contain scope of unauthorized access. Secure and recover systems.	Vulnerability leading to intrusion identified and corrected. Decision made whether to identify perpetrators.

3.1 Introduction.

3.2 People Involved in Incident Response Process.

3.3 Incident Response Process.

3.4 Incident Response Methodology.

3.5 Activities in Initial Response.

3.6 Phases after Detection of an Incident.

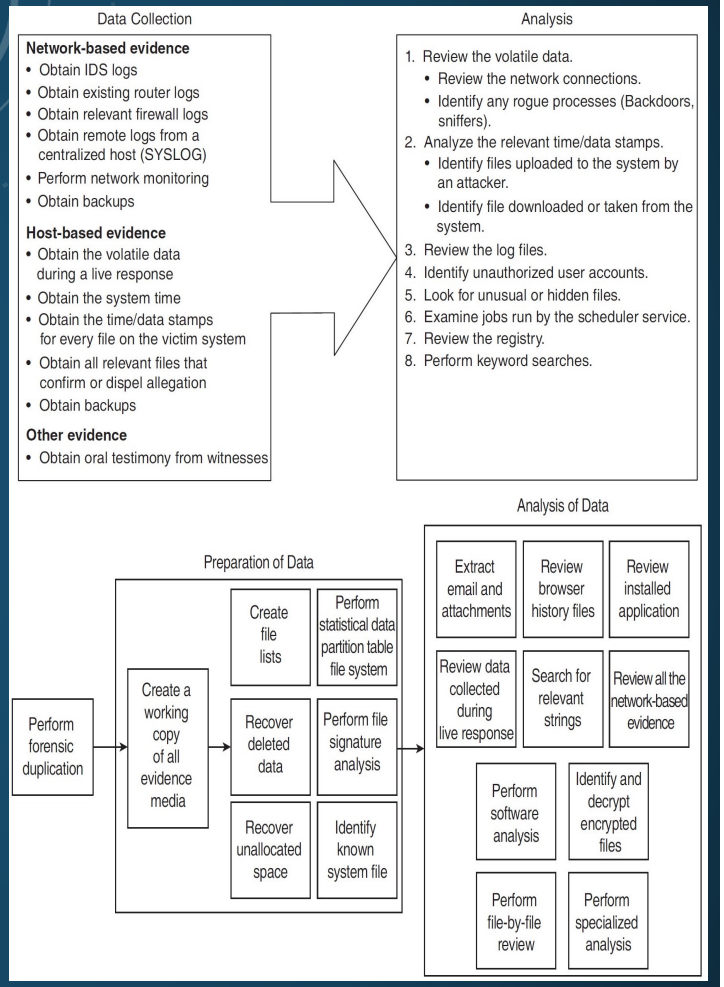
Incident Response Methodology :

Investigate the Incident :

1. Data collection : The accumulation of facts and clues that should be considered during your forensic analysis is *data collection*.

The basis of your conclusions is the data you collect.

2. Forensic analysis : *Forensic analysis* consists of reviewing all the data collected. It also includes reviewing log files, system configuration files, trust relations, web browser history records, electronic mail messages and their attachments, installed applications, and graphic files.



3.1 Introduction.

3.2 People Involved in Incident Response Process.

3.3 Incident Response Process.

3.4 Incident Response Methodology.

3.5 Activities in Initial Response.

3.6 Phases after Detection of an Incident.

Incident Response Methodology :

Reporting :

1. Document immediately

2. Write concisely and clearly

3. Use a standard format

4. Use editors

Resolution :

To implement host-based, network-based, and procedural countermeasures to prevent an incident from
causing further damage and to return your organization to a secure, healthy operational status is the goal of
resolution phase.

3.1 Introduction.

3.2 People Involved in Incident Response Process.

3.3 Incident Response Process.

3.4 Incident Response Methodology.

3.5 Activities in Initial Response.

3.6 Phases after Detection of an Incident.

Activities in Initial Response :

1. Obtaining Preliminary Information :

One of the primary steps of any study is to gain enough information to determine an appropriate response this is the goal of the initial response phase.
It is necessary for your organization's initial response to include the following activities:

- **a.** An incident receiving the initial notification.
- **b.** After the initial notification, record the details, including an incident declaration, if appropriate.
- **c.** Assembling the CSIRT.
- **d.** Perform the traditional investigative steps.
- **e.** Interviews to be conducted.
- **f.** Determine whether the incident is escalated or not.

Again, to develop an appropriate response strategy, the idea is to gather enough information.

2. Documenting Steps to Take :

The other reason of the initial response phase is to document steps that must be taken. When an incident is detected, organization and discipline prevent "knee-jerk" reactions and panic.

3.1 Introduction.

3.2 People Involved in Incident Response Process.

3.3 Incident Response Process.

3.4 Incident Response Methodology.

3.5 Activities in Initial Response.

3.6 Phases after Detection of an Incident.

Phases after Detection of Incident :

1. Recording the Details after Initial Detection :

a. Initial response checklists : To record the circumstances surrounding a reported incident, use an initial response checklist as the mechanism.

b. Second section of the initial response checklist : The second part of the initial response checklist could be used by the members of the CSIRT to address the technical details surrounding the incident.

2. Incident Declaration : In most of the cases, it will be immediately obvious whether or not the activity is actually a computer security incident in which suspicious activity is reported.

3. Assembling the Computer Security Incident Response Team : Responding to incidents, many organizations have a CSIRT that is formed in response to a particular situation or incident rather than an established and dedicated centralized team.

4. Performing Traditional Investigation Steps :

a. Host-based evidence

b. Network-based evidence

c. Other evidence

3.1 Introduction.

3.2 People Involved in Incident Response Process.

3.3 Incident Response Process.

3.4 Incident Response Methodology.

3.5 Activities in Initial Response.

3.6 Phases after Detection of an Incident.

Phases after Detection of Incident :

5. Conducting Interviews : The first step is to start asking the "who, what, when, where, and how" questions, when your CSIRT learns of a suspected incident.

6. Formulating a Response Strategy : The most important aspect of incident response is arguably your response strategy. In this phase, you consider what remedial steps to take to recover from the incident.