Carnegie Mellon University
Software Engineering Institute

Response and Recovery

Foundations of Incident Management (FIM)

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

Notices

This material is based upon work funded and supported by the Independent Agency under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center sponsored by the United States Department of Defense.

The view, opinions, and/or findings contained in this material are those of the author(s) and should not be construed as an official Government position, policy, or decision, unless designated by other documentation.

NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN "AS-IS" BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

This material is distributed by the Software Engineering Institute (SEI) only to course attendees for their own individual study.

Although the rights granted by contract do not require course attendance to use this material for U.S. Government purposes, the SEI recommends attendance to ensure proper understanding.

DM19-0875

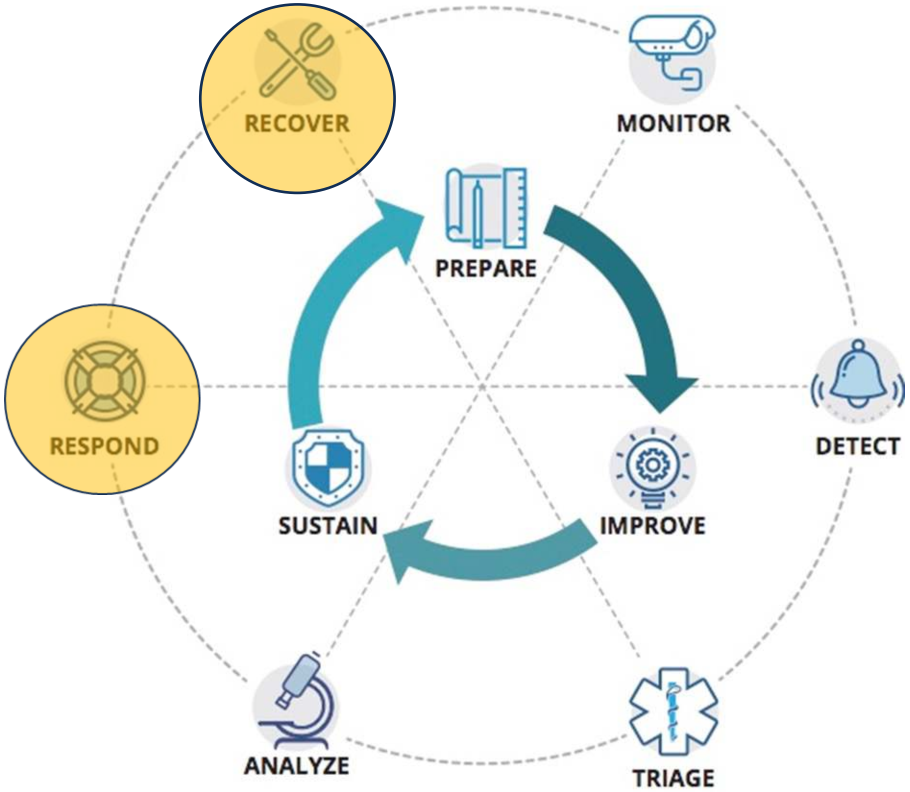
Purpose

To build on the skills and abilities discussed in coordinating response

To discuss in more depth, some of the response and recovery steps such as

- containment
- eradication
- restoring operational status

Overview [Reminder] of Analysis in the Incident Management Lifecycle



Primary Objectives of Response

The primary objectives for the response process is to

- halt or minimize attack effects or damage while maintaining operational mission continuity
- ensure the effective and timely recovery of systems in a way that prevents similar incidents from occurring again
- strengthen the organizations' defensive posture and operational readiness
- ensure response activities occur in a manner that protects any data according to its level of sensitivity
- support rapid, complete attack characterization
- develop and implement courses of action (COAs)

Criteria for Developing Courses of Action

NIST, in its “Computer Security Incident Handling Guide,” provides a list of criteria for determining appropriate courses of action or what it calls “strategies”. These criteria include

- potential damage to and theft of resources
- need for evidence preservation
- service availability (e.g., network connectivity, services provided to external parties)
- time and resources needed to implement the strategy
- effectiveness of the strategy (e.g., partially contains the incident, fully contains the incident)
- duration of the solution (e.g., emergency workaround to be removed in four hours, temporary workaround to be removed in two weeks, permanent solution)

Containment

Consists of short-term, tactical actions to

- stop an intruder’s access to a compromised system
- limit the extent of an intrusion
- prevent an intruder from causing further damage

Primary objectives are to

- regain control of the systems involved in order to further analyze them and return them to normal operation
- deny an intruder access to prevent him or her from continuing the malicious activity and from affecting other systems and data

Containment Strategies

Vary based on the type of incident

Activity may include any of the following

- blocking
  - border gateway firewall block
  - mail and proxy block
  - URL/domain block
- network isolation
  - disconnect the system from any local network (LAN)
  - disconnect the system from the Internet or any other public networks
  - disconnect or isolate the affected network host and/or segment from the rest of the network
- shutdown
  - system
  - server
  - service

Other Containment Strategies

Other containment strategies presented by NIST SP 800-61, NIST Computer Security Incident Handling Guide include the following

- Eliminate the attacker’s route into the environment by preventing attacker from accessing nearby resources that might be targets.
- Block the transmission mechanisms for the malicious code between infected systems.
- Disable user accounts that may have been used in the attack.

Available at https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

Leaving System Online

Under certain circumstances, the decision may be made to leave an affected system's vulnerability accessible in order to monitor the attacker's activities.

If a compromised system is left running, NIST recommends "management and legal counsel should ensure there is no liability that can result."

NIST also cautions "not containing malicious activity can cause more malicious activity to occur because malicious code or actions continue which can cause further damage and loss of operations or critical data."

Caveats for Containment

Any changes to compromised systems, including containment actions may destroy information required to assess the cause of an intrusion.

Ensure that all necessary data for analysis is completely collected before making any system changes.

Also, collect and protect all evidence that may be needed in a subsequent investigation before performing any containment actions.

Eradication

Eradication consists of the steps required to eliminate the root cause(s) of an intrusion.

All threats and risks should be removed from systems and networks before returning them to service.

If the threat is not removed, then a system can be easily compromised or breached again.

Primary Objectives of Eradication

To ensure the

- removal of the cause(s) of the malicious activity and any associated files
- elimination of any access methods used by the intruder, including vulnerabilities, physical security problems, or human error

Executing Eradication

Execute eradication steps after the first round of containment actions occur and then interactively with any further analysis and containment activities.

Sometimes, full eradication can only happen after long-term policy and configuration management changes are put into place.

In that case, the threat should be mitigated to the extent possible before rebuilding and reconnecting any affected systems.

Eradication Strategies

Specific eradication actions depend on the nature of the incident.

- Remove malware.
  - Quarantine.
  - Delete or replace.
  - Restore integrity of files.
  - May require rebuilding systems from trusted media.
- Remediate or mitigate vulnerability.
  - Install updates or patches.
  - If system can not be patched due to certifications or criticality, mitigate by updating system configurations and surrounding defenses, or segment affected host.
- Modify access controls.
  - Update user and network access controls.
  - Remove any access mechanisms used by intruder.
  - Update baseline configurations.

Recovery

Consists of the steps necessary to

- restore the integrity of affected systems
- return the affected data, systems, and networks to an operational state
- implement follow-up strategies to prevent the incident from happening again

Primary Objectives of Recovery

The main objectives of recovery are to

- restore the integrity of the system by rebuilding it from trusted media when necessary
- implement proactive and reactive defensive and protective measures to prevent similar incidents from occurring in the future
- ensure all data and systems are operating in a normal fashion
- ensure the complete resolution and closure of the incident

Depending on your situation, recovery steps may be completed by another part of the organization.

Even if that is the case, you, as an incident handler will want to know when this process is complete.

You may also provide recommendations for how best to mitigate and recover.

Recovery Strategies

Depending on the nature of the incident, recovery actions can include, but are not limited to the following:

- **Rebuild from trusted media**. Reinstall the operating system and applications from a trusted backup, or from original distribution media.
- **Verify system data**. Review system data to ensure its integrity. **Change system passwords**. Change all passwords on the system and possibly on all systems that have trust relationships with the victim system.
- **Improve network and host security.**

To Finish Recovery

Remove any containment steps that are no longer needed.

Once all recovery steps have been completed and systems have been tested to ensure they are operating normally, reconnect any hosts or networks that were disconnected.

Ensure all steps taken have been documented.

Ensure all stakeholders have been notified when recover operations are complete.

Example: Responding to a Compromise

Recommended steps include

- Consult your security policy.
- Document all the steps you take in recovery.
- Regain control.
- Analyze the intrusion.
- Contact the relevant CSIRT and other sites involved.
- Recover from the intrusion.
- Improve the security of your systems and networks.
- Reconnect to the Internet.
- Update your security policy.

Handling an “Insider” Incident

How is handling an incident perpetrated by an internal employee different than handling other types of incidents?

What processes need to be in place to properly handle such incidents?

Who needs to be involved in handling such incidents?

Response and Recovery Scenario Exercise

Purpose

To build on the skills and abilities discussed in response and recovery module

To discuss in more depth some of the response and recovery steps such as

- Containment
- Eradication
- Recovery

Incident Handling

Remember the steps:

- Preparation
- Detection
- Analysis
- **Containment**
- **Eradication**
- **Recovery**
- Post-Incident Activity, Root-Cause Analysis

Containment

Containment

Goal of containment is to halt the spread of the incident and stop further damage from occurring.

As part of this exercise, consider

- Which containment strategy or strategies will be effective?
- What actions will most quickly stop incident spread and damage?
- What impact to operations will the chosen containment strategy have?
- Will a forensic investigation be conducted? Why or why not?
- What pre-existing policies could make containment easier?

Containment Discussion

This is an example of a “blended threat” where several attack types are combined into a single attack in order to increase damage and make response more difficult.

Each attack type may require a different containment strategy.

It may be useful to decompose the attack into its component attack elements.

- What are the attack components in this exercise?
- What are some containment strategies by attack component?
- Response policies that assist in selecting containment strategies are important, preferably done in advance.

Eradication

Eradication

The goal of eradication is to eliminate components of the incident such as malicious code, compromised accounts and passwords, etc.

Eradication may not be necessary in some incidents.

As part of this exercise, consider

- Is eradication necessary in this exercise?
- What would an eradication strategy contain?
- Are there components in this incident that you would not eradicate?

Eradication Discussion

A primary goal of eradication is to identify vulnerabilities targeted by the malicious code and eliminate the vulnerability.

Not all malicious code targets software vulnerabilities.

What other components can be eradicated?

Recovery

Recovery

Goal of recovery is to restore systems to normal operation and to harden systems against future attack.

In this exercise, consider

- What specific steps would you take to recover from this incident?
- What hardening steps would you take to prevent this incident from re-occurring?

Recovery Discussion

Steps that may be used in recovery

- rebuild systems from clean backups
- rebuild systems from scratch
- changing accounts, passwords
- harden against re-occurrence, apply patches
- system updates, patches

Module Summary -1

Question:

What can be done in advance to make the process of containment, eradication and recovery easier and more effective?

Module Summary -2

Answer:

Incident response planning and policy development

- Containment strategies or boundaries can be determined calmly and rationally in advance rather than in the heat of a attack.

Module Summary -3

Examples of containment policy guidance?

- Under what circumstances and conditions is it permitted to disconnect systems from the network?
- Under what circumstances and conditions, if any, is it permitted to disconnect from the Internet?
- What actions can be pre-approved for administrators to take during an incident?
  - Install temporary network block at the firewall
  - Temporarily disable outbound web or inbound mail services if needed for containment

Next Steps

Post Incident Analysis

Lessons Learned

Plan of Action and Milestones (POA&M)

Key Points

Understand what role you play in the response and recovery phase.

Know what criteria should be followed to determine how best to develop the right course of action to handle the incident.

Ensure you have appropriate guidance and approval for any containment or eradication steps.

Do not reconnect systems or return to operational status until systems have been tested.

Questions