CS 798: Digital Forensics and Incident Response

Lecture 22 - Incident Handling and Remediation

Diogo Barradas

Winter 2025

University of Waterloo

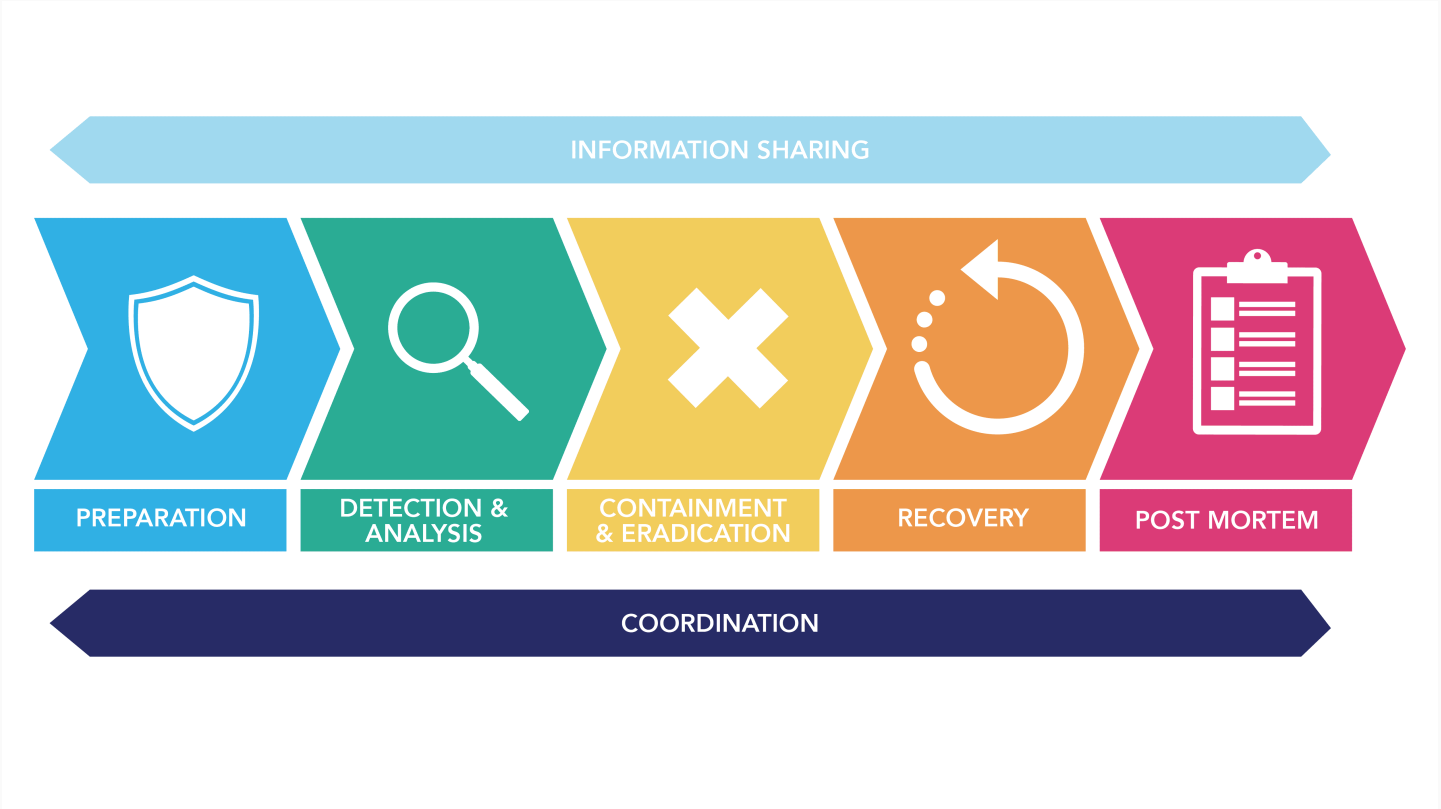
Outline

1. Incident Handling

2. Incident Remediation

Incident response

- The last class focused on the adequate preparation for responding to an incident
- Today, we will take a look on how to handle an incident and conduct remediation actions



Incident Handling

Shouldn't we just call for an investigation?

- Once an incident is ongoing, it must be properly handled
- Before initiating an investigation, it is important to verify facts
  - Failure to do so often results in waste of time and resources
- For instance, it is important to establish context on events
  - e.g., is the detection system misrepresenting/ommiting an event? Why?
- Investigators must act quickly at this stage, eventually keeping track of information in flexible checklists

Useful checklists

- Checklists can be useful for verifying facts and validate suspicions before launching an investigation
- Some guidelines include the following lists:
  1. Incident summary
  2. Incident detection
  3. System details
  4. Network details
  5. Malware details

1. Incident summary

- Gathers basic, high-level information of an incident, such as:
  - Date and time an incident was reported
  - Date and time an incident was detected
  - Contacts of who reported/detected the incident
  - The nature of the incident
  - The type and identification of affected resources
  - A list of who accessed the resources since detection
  - Who is aware of the incident
  - Whether the incident is still ongoing

2. Incident detection

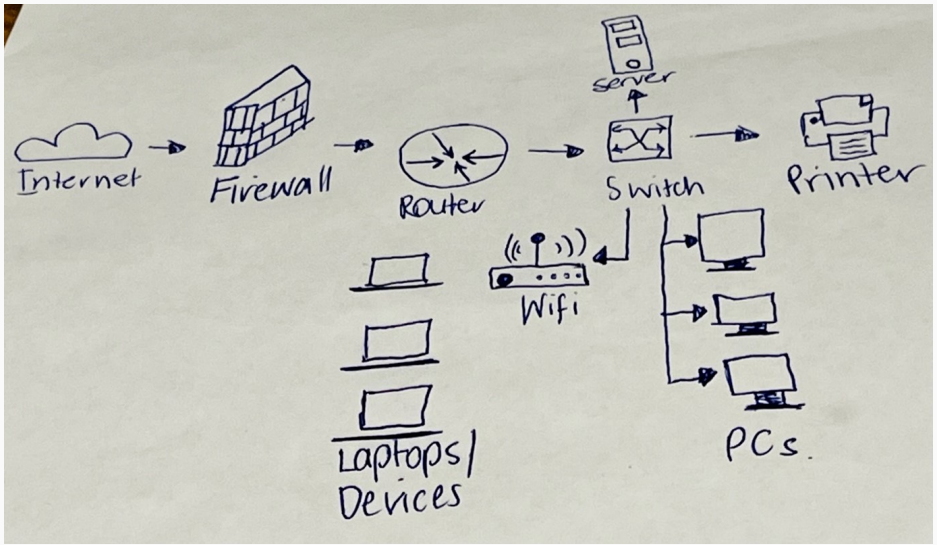
- Collect details about the detection system and how an incident was detected. May include information such as:
  - Was the detection manual or automated?
  - What information is part of the initial detection?
  - What sources provided the data used for detection?
  - Has someone validated whether the data source is accurate?
  - Did data sources change recently?
  - How long has the detection system been in operation?
  - What is the detector's accuracy?

3. System details

- Collect details about the individual systems implied in the incident detection. May include information such as:
  - What is the physical location of the system?
  - What is the system's make and model?
  - What operating system and applications are running?
  - What is the primary role of the system? Is it critical?
  - Who is the responsible administrator?
  - Where is the system located in the network?
  - Are there back-ups?

4. Network details

- Collect details about the network implied in the incident detection. May include information such as:
  - A list of external IP addresses involved
  - Is network monitoring being conducted?
  - Is any traffic monitoring data being preserved? If so, where?
  - Network diagrams and configuration information



5. Malware details

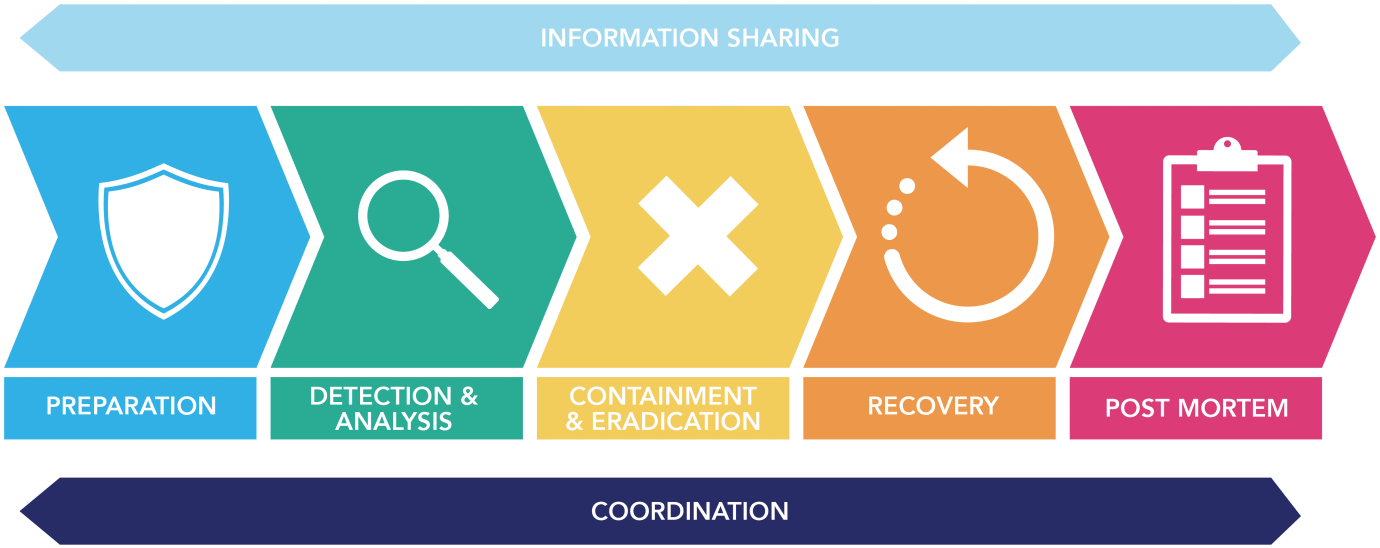
- Collect details about possible malware related to the incident:
  - Time and date of detection
  - List of systems where the malware was found
  - Information about the malware family
  - Whether a copy of the malware binary has been preserved
  - Has the malware been analyzed for host and network indicators of compromise?
  - Has the malware been submitted for analysis to 3rd party services?

Setting expectations with management

- Before approaching upper management with an investigation request, it is important to set expectations on the scope and scale of a potential investigation
- Several elements need to be considered:
  - Availability of evidence sources
  - Type of incident
  - Questions to be answered
  - Timeframe
- Effective communication will allow the incident response team to make their point across and allow upper management to take informed decisions

Conducting an investigation

- Once an investigation is approved, the investigation team will follow a sound forensic methodology to uncover and analyse evidence and understand the full extent of the incident
- Essentially, using the methods and techniques described earlier in the course



Incident Remediation

Don’t panic (too much)!

What is remediation?

- After an incident has been detected and being handled, the organization must prepare **incident remediation**
- A remediation plan is typically composed of two parts:
  - **Remediation**:
    - Includes posturing, containment, and eradication
  - **Improvement of the security posture**:
    - Preparing long-term strategic actions
- The plan can be revised on-the-fly, depending on the difficulties of implementing specific action items
  - Left-off items can end up in a strategic recommendations list

The remediation process

- The **remediation process** can be described in 8 stages:
  1. Form the remediation team
  2. Determine the timing of the remediation actions
  3. Develop and implement remediation posturing actions
  4. Develop and implement incident containment actions
  5. Develop the eradication action plan
  6. Determine eradication event timing and implement the eradication plan
  7. Develop strategic recommendations
  8. Document the lessons learned from the investigation

1. Form the remediation team

- **When to create the remediation team**
  - As soon as an investigation starts
  - Should work in parallel with the investigation team to ensure a short mean time to remediate (MTTR)
- **Assigning a remediation owner**
  - Takes responsibility for the overall remediation effort and interacts with both technical and non-technical personnel
- **Members of the remediation team**
  - An interdisciplinary team (just as the investigation team)
  - Should include an investigation team member and system, network, and application owners

2. Determine the timing of the remediation actions

- **Immediate action**
  - Stop the incident from continuing (incident containment)
  - Appropriate for small incidents with ongoing losses
  - May alert an attacker that the organization is aware of them
- **Delayed action**
  - Allow the investigation to conclude before taking action against the attacker
  - Appropriate when intelligence gained from monitoring the attacker's activities outweighs the need for containment
  - May allow an attacker to gain additional knowledge
- **Combined action**
  - Contain only specific aspects of the incident
  - Useful when containment is more important than the investigation
  - Allows attacker within the environment until eradication

3. Develop and implement remediation posturing actions

- **Posturing actions**
  - Designed to enhance the investigation team's visibility, providing additional sources of evidence
    - e.g., system, app, network logs, enhance authentication
  - Can decrease the time spent on the remediation effort
- **Increase the security of the organization's systems**
  - Prevent the attacker from compromising additional systems
    - e.g., strengthen password requirements, enforce 2FA
- **Implications of alerting the attacker**
  - Attackers may react in response to defensive actions:
    - Change tactics and procedures
    - Become dormant
    - Become destructive
    - Scale and overwhelm

4. Develop and implement incident containment actions

- Designed to remove the attacker's access to a specific network segment, application, or data
- **Identify the resources that must be protected**
  - Containment must assume all reasonable attacker activity and not just currently known malicious activity
- **Timeliness and scope of a containment plan**
  - Often devised and implemented prior to understanding the full scope of a compromise
  - Hence, tend to be overly cautious
- **Perform containment actions**
  - Implement stringent temporary measures (and relax later)
  - Revise and apply as needed (e.g., shall attacker regain access)

5. Develop the eradication action plan

- Designed to remove the attacker's access to the environment
- **Eradication actions**
  - Should be swift and allow for full recovery of the organization
    - e.g., rebuild systems, change passwords, segment the network
  - Require knowledge about the full scope of the environment
- **Timeframe for eradication**
  - Weekends are good for minimizing business disruptions
  - May also consider attacker's inactivity timeframe (if known)
- **Complications during eradication**
  - Failure to disconnect attacker from the environment
  - Operational difficulties in applying eradication actions
- **Common errors during eradication**
  - Back-up systems to a compromised state
  - Break production systems after password changes

6. Determine eradication timing and implementation

- **Too early**
  - The investigation team may not have time to adequately scope the compromise
  - The remediation is doomed to fail because the attacker's access to the environment may not have been removed
- **Too late**
  - The attacker may change their tools, tactics, and procedures, demanding new investigation efforts
  - The attacker may hit the jackpot before eradication
- **Just right (the "strike zone")**
  - The investigation team has correctly scoped the compromise and the remediation team is ready for conducting eradication
  - It's a fine line and may be tricky to get right
    - Requires visibility over the environment, attack detection mechanisms, and awareness of the attacker's activities

The importance of communication during eradication

- Communication is key throughout the eradication event
- **Establish a communication medium**
  - Established before the eradication event and available throughout the eradication
- **Keep tabs on progress**
  - e.g., establish periodic calls or keep a conference call open
- **Keep the right people in the loop**
  - All technical personnel should be present during an eradication event (or on call)
- **Communication is also important post-eradication**
  - Helpdesk personnel should be able to reach out to the remediation team shall suspicious activity be reported

7. Develop strategic recommendations

- Strategic recommendations are actions that are critical to your organization's overall security posture
- **Deployment of strategic recommendations**
  - Difficult to implement because they can be highly disruptive
  - Cannot be implemented prior to, or during, eradication
- **Document potential strategic action items**
  - Document even if current feasibility of implementation is low
  - Priority is important - most risk reduction listed first
- **Draft action items**
  - Should only be described in high-level by the remediation team
  - Cross-functional teams will plan proper implementation

8. Document the lessons learned from the investigation

- **Rely on structured documentation**
  - Enforcing structure (like using a template) will ensure content is captured in a consistent manner
- **Make documentation easy to find and prevent duplicates**
  - e.g., use tags, categories, etc.
  - Build wikis, or use document management systems
- **Create "lessons learned" documents soon after the incident**
  - Aggregate details over procedures and supporting scripts
    - e.g., how to determine all programs that have hardcoded usernames and passwords
    - e.g., how to create unique passwords for the local administrator account on all Microsoft Windows systems
  - Facilitates similar remediation actions in the future
    - You just need to "follow the script"

Common remediation mistakes

- **Lack of ownership**
  - e.g., issues understanding IT and security
- **Lack of executive support**
  - e.g., inability to communicate with non-technical personnel
- **Poor planning**
  - e.g., ignore part of the (potentially compromised) environment during the preparation of a containment plan
- **Remediation plan is too ambitious**
  - e.g., overlook the incident at hand and focus on long-term strategic planning
- **Poor timing**
  - e.g., remediation action alerts the attacker too soon

Takeaways

- Due to personnel and resources' costs, it is important to collect and verify potential indicators of compromise before calling for an investigation.
- A successful incident remediation process requires thoughtful planning, focus, attention to detail, and well-coordinated execution.
- Containment and eradication actions should be appropriately timed to ensure proper effectiveness.

Pointers

- **Textbook:**
  - Luttgens – Chapters 4–6, 17 [Luttgens]
- **Literature:**
  - NIST - Computer Security Incident Handling Guide