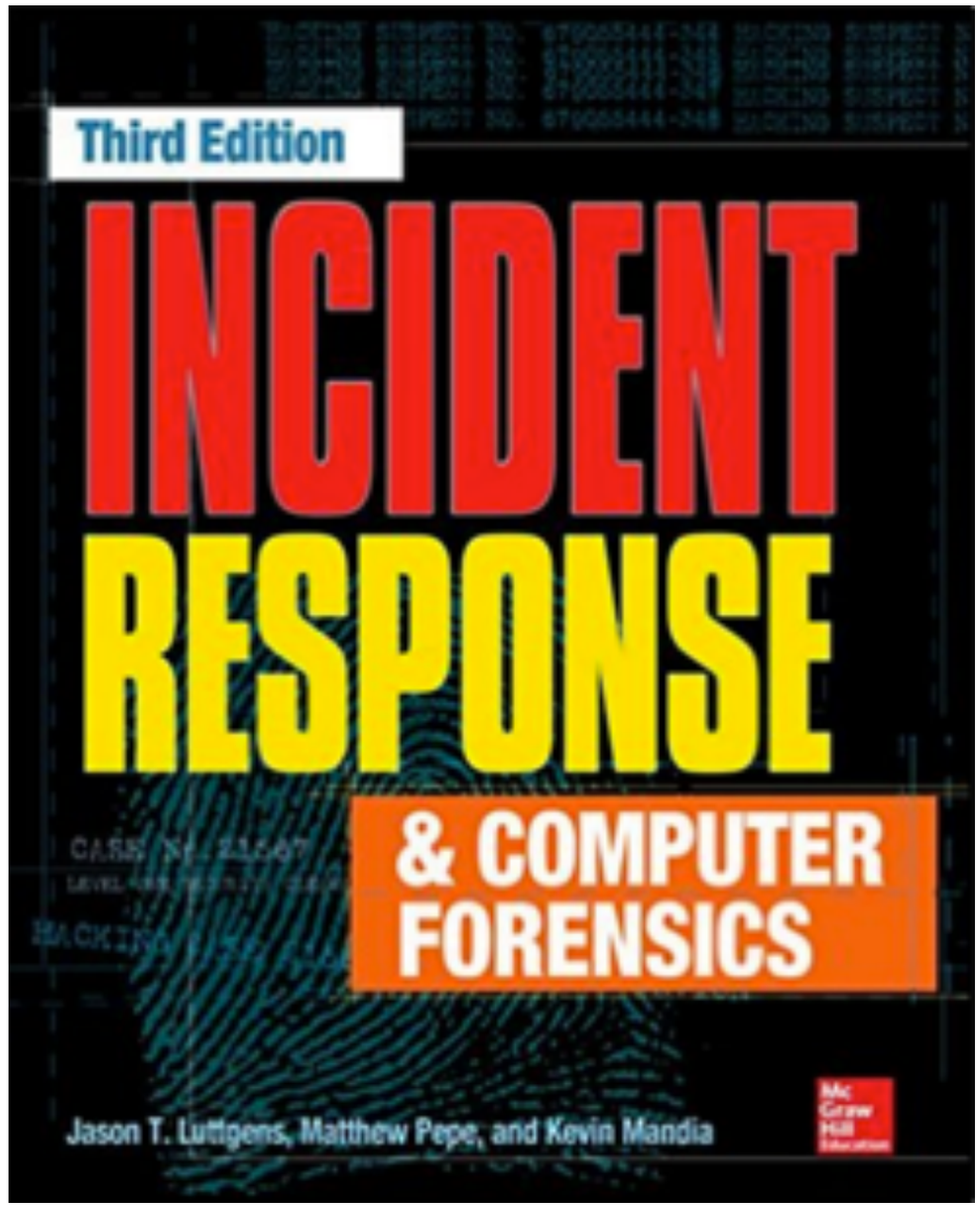
CNIT 121: Computer Forensics



17 Remediation Introduction Part 1

Basic Concepts

- **Remediation plan has two parts**
- **First part**
  - **Remediating the current incident**
    - **Posturing, containment, and eradication**
- **Second part**
  - **Improving security posture**
  - **Strategic actions**

Revisions

- **Draft remediation plan will be revised many times**
- **Action items that seem easy turn out to be more difficult**
- **Shift those items into strategic recommendation**
- **Example: switch to two-factor authentication (2FA)**
  - **Very difficult to do for whole organization, so do a subset of users first**

Figure 17-1. Remediation process flowchart

1. Form the Remediation Team

- **After incident has been declared an incident ownership is assigned**
- **Remediation team needs representatives from**
  - **Legal, IT (both infrastructure and help desk), security, and business line managers**

2. Determine Timing

- **Business leaders must decide what actions begin immediately, and what is delayed until the investigation is over**

- **In coordination with legal, remediation, and investigation teams**

- **Timing varies widely depending on the incident, rate of investigation, and type of information that could be in jeopardy**

3. Remediation Posturing Actions

- **Posturing actions are implemented while the incident is ongoing**
  - **Enhancements to system and network monitoring**
  - **Mitigating critical vulnerabilities**
  - **Preparing support teams for enterprise-wide changes such as password resets or 2FA deployment**
- **Looks like normal maintenance to an attacker**

4. Incident Containment Actions

- **Designed to deny the attacker access to specific environments or sensitive data during an investigation**

- **Often disruptive short-term solutions implemented quickly**

5. Develop Eradication Action Plan

- **Goals: remove attacker's access and mitigate the vulnerabilities the attacker used to gain access**

- **Clearly document and rehearse actions**

- **This step will be executed near the end of the investigation, once the attacker's Tools, Tactics, and Procedures (TTP) are well understood**

6. Determine Eradication Event Timing and Implement Eradication Plan

- **Investigation reaches "steady state"**
  - **No new tools or techniques are being discovered**
- **Perform this step at the right time**
  - **When investigative team has a good grasp of the TPP being used**
- **This step also includes post-monitoring and verification of eradication activities**

7. Develop Strategic Recommendations

- **Throughout the investigation and remediation process**
  - **Document areas for improvement**
- **Strategic recommendations consist of**
  - **Remedial actions that cannot be implemented prior to, or during, the investigation**
- **They may disrupt business and be expensive**
- **Typically occur months or years after eradication**

8. Document Lessons Learned

- **Store documentation in a central location**
  - **Restricted to incident responders only**
    - **Because information is sensitive**
  - **Examples: reports developed, notes about the environment**

Remediation Effort

- **Should be concise and effective**
- **It's risky to enact significant changes in a tactical situation**
  - **Result may be rushed and incomplete**
- **Understand what your team and organization can do quickly**
  - **Push other tasks into the strategic recommendations documentation**

Factors to Consider

Incident Severity

- **Determines remediation implemented**
- **A bank experiencing real-time loss requires more immediate containment than a defense contractor breached by an unknown attacker**
- **Breached web server containing only public information is much less severe than an attacker who gained domain admin credentials**

Remediation Timing

- **Efforts to immediately remove attacker's access to sensitive systems or data**
- **Efforts designed to allow investigative team time to gather information**
  - **So they can comprehensively remove the attacker and strengthen defenses**

The Remediation Team

- **Three concerns: size, skill level, and management support**
- **Large teams are harder to coordinate**
- **Experienced teams are more comfortable taking customized approaches**
  - **Less skilled teams may want to stay within their comfort zone**
- **Management support controls authorization and available resources**

Technology

- **Security technology and enterprise management technology**
- **Software may be available to assist changing local administrator passwords throughout the enterprise**
  - **Otherwise, you must develop a script**
- **Implementing new technology during an incident usually causes more problems than it solves**

Budget

- **Remediation effort must make sense**

- **Spending more money protecting assets than the assets are worth is bad business**

Management Support

- **Remediation will affect day-to-day operations**
  - **Changing password policies will change how administrators interact with systems**
- **Management support helps ensure that even painful remediation actions are implemented and supported by the organization**

Public Scrutiny

- **Legal or PR team may be required to disclose information due to regulatory requirements**
- **Sometimes information is leaked, or discovered by third parties**
- **Attacker may try to extort the company by threatening to make compromise or stolen data public**
- **Carefully review public statements**
- **Hasty statements that are revised later may cause embarrassment and public backlash**

Example: HIPAA

- **Health Insurance Portability and Accountability Act**
- **Loss of Protected Health Information (PHI) or Personally Identifiable Information (PII) triggers notifications**
- **Often it helps to also disclose containment or eradication steps to reassure the public**
- **Include legal and PR from the beginning of the incident**

Remediation Pre-Checks

- **1. Ensure organization has committed to a formal incident response**
  - **Response will require staff and time commitments**
- **2. An incident owner has been assigned**
  - **Provides leadership for key stakeholders, incident investigation team, and incident remediation team**

1 Form the Remediation Team

When to Create the Remediation Team

- **As soon as an investigation is initiated**
- **Start planning the remediation effort immediately**
- **Run investigation and remediation teams in parallel**

Mean Time to Remediate (MTTR)

- **Time to Remediate**
  - **Time from incident discovery to eradication**
- **If malware is discovered on Jan 25**
  - **Investigation finds the system was compromised on Jan 15**
  - **System rebuilt on Jan 26**
- **Time to remediate is 24 hours**

Assigning a Remediation Owner

- **Responsible for the overall remediation effort**
- **Interacts with both technical and nontechnical personnel**
- **Usually a senior technical person is the best choice**
- **Needs full management support**

Remediation Efforts

- **Often difficult and disruptive**
  - **Such as coordinated login password changes throughout the environment**
- **Unpopular, creates pushback**

Remediation Owner Desirable Qualities

- In-depth understanding of IT and security
- Focus on execution
- Understanding of internal politics
- Proven track record of building support for initiatives
- Ability to communicate with technical and nontechnical personnel

Members of the Remediation Team

- **Required**
  - **Someone from investigation team**
  - **System, network, and application representatives**
  - **Other subject matter experts (as applicable)**
- **Ancillary**
  - **Legal, compliance officers, business line managers, HR, PR, and executive management**

- An investigative team member will be able to offer valuable insight about the attacker's activities and what mitigation steps can be taken. They will also know what immediate remediation actions would alert the attacker (if the delayed remediation approach is taken).
- System, network, and application owners will best understand the feasibility of recommended actions and their effects on the organization. Their understanding of systems and applications will allow them to offer alternative suggestions if the initial recommendation is not feasible.
- Various subject matter experts (SMEs) will be crucial when a nonstandard system, such as a classified system or Industrial Control System (ICS), is involved in the remediation.
- Representatives from the ancillary functions will be able to provide valuable insight and support to the nontechnical issues the remediation team is expected to encounter.

2. Determine Timing of the Remediation

- **Three types: immediate, delayed, and combined action**

- **Usually the best choice is delayed action**

Immediate Action

- **Used to stop the incident from continuing (containment)**
- **Often alerts the attacker that the organization is aware of his activities**
- **Appropriate for incidents with an active attacker**
  - **Organization is losing money in real time**
  - **Malicious insider is stealing data right now**
  - **Incident is small, such as a single compromised system**

Immediate Action

- **Not appropriate if attacker has compromised hundreds of systems and installed multiple backdoor families**
- **Immediate action would only cause the attacker to change tools and techniques**
- **Cause the investigation team to re-scope the compromise**

Delayed Action

- **Allow investigation to conclude before any direct actions are taken against the attacker**
- **Appropriate when the investigation is at least as important as the remediation**
- **Most common approach for incidents involving Intellectual Property (IP) theft**
- **Where intelligence gained from monitoring attacker's activity outweighs need to contain the activity**

Delayed Action

- **Law enforcement may ask you to delay remediation**
- **In order to allow their investigation to continue. so they may learn more about the attacker, or to provide time to make an arrest**
- **This may be beneficial because it may allow you to delay public notifications**

Combined Action

- **Implements containment on only a specific aspect of the incident**
    - **Letting the rest of the incident continue**
- **Used when containment is more important than remediation**
    - **However, full investigation and remediation is still warranted**

Combined Action

- **Example**
  - **Near real-time theft of money or critical business data**
    - **Attacker has credentials used for ACH (Automated Clearing House) transactions**
    - **Organization needs to immediately remove attacker's access to the system**
    - **Also needs to fully scope the compromise and implement a comprehensive remediation effort**

3. Develop and Implement Remediation Posturing Actions

- **Posturing actions**
  - **Additional logging and monitoring**
  - **Intended to have little impact on the attacker**
  - **Enhance the investigation and decrease time spent on later phases of remediation**

3. Develop and Implement Remediation Posturing Actions

- Enhance logging, including the following logs:
  - System-specific logs
  - Application-specific logs
  - Networking logs
  - Central authentication logs
- Centralize log files and management (security information and event management [SIEM] implementation)
- Enhance alerting
- Patch third-party applications
- Implement multifactor authentication for access to critical environments
- Reduce locations where critical data is stored
- Enhance the security of native authentication

3. Develop and Implement Remediation Posturing Actions

- **Can be implemented by improving the type of data retained by endpoints**
- **On Linux**
  - **Enabling command history and process auditing**
  - **Ensure that all authentications are properly logged**

3. Develop and Implement Remediation Posturing Actions

- **On Windows**
  - **Configure Windows auditing to log success and failure events for**
    - Audit account logon events
    - Audit account management
    - Audit logon events
    - Audit object access
    - Audit privilege use
    - Audit process tracking
    - Audit system events

Windows Logging

- **Enabling "success" events for audit policies**
  - **Audit object access**
  - **Audit process tracking**
- **May quickly fill the local Security event log file**
- **May need to increase size of log files or send events to a central auditing system**

Windows Logging

- **Enabling "failure" events only is not enough**
- **Once attacker succeeds in getting credentials, their activities are now successes**

3. Develop and Implement Remediation Posturing Actions

- **Posturing: increase security of an application or system without alerting the attacker**
- **Check with investigation team before implementing these changes, to get their opinion on whether it will alert the attacker**

- Remove LANMAN hashing throughout a Windows environment.
- Strengthen password security requirements.
- Patch commonly targeted third-party applications.
- Implement multifactor authentication to a critical environment the attacker has not yet compromised or discovered.
- Fix an application flaw the attacker used to gain initial access into the environment.

3. Develop and Implement Remediation Posturing Actions

- **Removing a compromised system may go unnoticed, seeming like normal maintenance**

- **Another posturing action:**

  - **Stop all legitimate use of known compromised credentials, issue new accounts to users who were compromised, and implement monitoring and alerting for the known compromised accounts**

Implications of Alerting the Attacker

- **Attacker changes Tools, Tactics, and Procedures**
  - **Investigation team must now track the changed TTP while also continuing to investigate the past activity**
    - **They may lose visibility into attacker's activity entirely**
    - **Organization may be forced to remediate activity immediately instead of continuing investigation**
    - **Attacker may install new mechanisms of access, compromising the entire effort**

Implications of Alerting the Attacker

- **Attacker may go dormant**
  - **Incident responders may miss evidence of malicious activity**
  - **Allowing the attacker to remain hidden during the eradication event**
  - **Only to become active later**

Implications of Alerting the Attacker

- **Techniques to go dormant**
  - **Implant malware that calls Command & Control (C2) server every few months**
  - **Remove all malware and use remote access instead, such as business peer connection or a VPN to implement webshells in the DMZ that are not used until the attacker believes the incident response is finished**

Implications of Alerting the Attacker

- **Park all malicious domain names in innocuous-looking IP addresses, such as an IP address belonging to Google**

  Some attackers like to “park” their domains by resolving them to IP addresses such as the localhost (127.0.0.1), broadcast address (255.255.255.255), multicast addresses (224.0.0.0–239.255.255.255), or Class E (IANA reserved) IP addresses (240.0.0.0–254.255.255.255). However, some of this activity is easily detected by any IDS/IPS and is not considered stealthy. More skilled attackers will resolve their domains to IP addresses that do not stand out.

Implications of Alerting the Attacker

- **Become destructive**
  - **Rare but some attackers do it**
  - **Delete files, deface web pages, crash systems**
  - **Forces responders to focus on recovering from damages**

Implications of Alerting the Attacker

- **Attempt to overwhelm the organization with compromised systems**
  - **One attacker used scripts to implant multiple malware families on each of 40 domain controllers every night**
  - **Organization was forced to remediate every night, an unsustainable level of work**
  - **Organization rebuilt all servers and implemented application whitelisting on all domain controllers and critical servers**

4 Develop and Implement Incident Containment Actions

- **Extreme short-term measures to stop an attacker's action that cannot be allowed to continue**
- **Does not remove attacker's access to environment**
- **Prevents attacker from performing a specific activity**
  - **Example: take PII database offline to stop data theft**

4 Develop and Implement Incident Containment Actions

A containment plan should never be treated as an eradication event because a containment plan is meant to be a temporary and often drastic solution to prevent malicious activity that is considered too unacceptable to be allowed to continue. A comprehensive investigation and remediation are still required to fully remove the attacker from the compromised environment.

4 Develop and Implement Incident Containment Actions

- **Teams need to understand data or resources that need to be protected**

- **Example**

  - **Attacker breached a restricted financial environment**

  - **Created unauthorized ACH transfers for large sums to an overseas bank account**

4 Develop and Implement Incident Containment Actions

- **Remediation team constrained by these factors**

- **Also, the company would like to announce a data when the network is safe to use again**

- The company could not tolerate a loss in business functionality.
- The attacker would still have access to the environment, so the containment plan must address alternate methods the attacker could initiate ACH transfers or access financial applications.

4 Develop and Implement Incident Containment Actions

- **Containment actions**

  1. Remove attacker's network access to financial application

  - **Use access control lists to prevent all systems, except one "jump system, from interacting with the server**

  - **Require two-factor authentication on jump system and only allow local accounts for a small number of users who absolutely must use it**

4 Develop and Implement Incident Containment Actions

- **Containment actions**

2. Remove attackers's ability to authenticate to financial application

- **Change all passwords for user accounts that have access to the financial application**

4 Develop and Implement Incident Containment Actions

- **Containment actions**

3. Require two-person integrity to create and authorize ACH transactions

- **Separation of duties**
  - **Some accounts can create ACH transactions**
  - **Other accounts can authorize them**
  - **No account can do both**

4 Develop and Implement Incident Containment Actions

- **Containment actions**

4. Implement notifications for all ACH transactions

- **Via email to a defined set of users**

4 Develop and Implement Incident Containment Actions

- **This approach uses defense in depth (layered protection)**

- **But a control was missing**

  - **If attacker had a backdoor into the financial environment with direct Internet access, new credentials could easily be stolen to bypass the new defenses**

  - **Access control lists should be implemented to limit the financial system's network traffic to only the systems explicitly required for business**

4 Develop and Implement Incident Containment Actions

Once a containment plan has been implemented, the incident response team should expect a reaction from the attacker. The remediation team should work on implementing appropriate logging, monitoring, and alerting in parallel to implementing the containment plan in order to detect and react to the additional malicious activity outside of the contained environment.

4 Develop and Implement Incident Containment Actions

- **When something goes wrong**

- **Suppose, five days after containment was implemented, investigation team discovers that attacker still has access to the financial application**

- **Must develop new containment actions**

- **And revise any public statement that environment was contained at the earlier date**

5 Develop the Eradication Action Plan

- **Implemented during a short period to remove the attacker from the environment**
- **Eradication event should result in complete recovery from the compromise**
- **Removing all of the attacker's access to the environment**
- **Relies heavily on results of investigation team to fully scope the incident and on organization's ability to fully implement the eradication plan**

5 Develop the Eradication Action Plan

- **Goals**

- Remove the attacker's ability to access to the environment.
- Deny the attacker access to compromised systems, accounts, and data.
- Remove the attack vector the attacker used to gain access to the environment.
- Restore the organization's trust in its computer systems and user accounts.

5 Develop the Eradication Action Plan

- **Expect attacker to try to regain access**
- **Account for attempts the attacker may make both during and after eradication event**
- **Attacker may search for and exploit other vulnerabilities**
- **Attacker may perform aggressive actions in retribution for losing access**

5 Develop the Eradication Action Plan

- **Common eradication actions**

  - Disconnecting the victim organization from the Internet during the eradication event
  - Blocking malicious IP addresses
  - Blackholing (or sinkholing) domain names
  - Changing all user account passwords
  - Implementing network segmentation
  - Mitigating the original vulnerability that allowed the attacker initial access to the environment
  - Rebuilding compromised systems

5 Develop the Eradication Action Plan

- **Weekends are good for eradication, because disruption to business is minimal**

- **Consider attacker's standard working hours, if known**

  - **Eradicate during period of low attacker activity**

- **Commonly organizations disconnect from the Internet during eradication**

5 Develop the Eradication Action Plan

- **Attacker may re-compromise during eradication**
- **Responses:**
  - **Quickly investigate and contain the re-compromise**
    - **Investigate in parallel to determine method used and mitigate it**
    - **Once it's mitigated, continue with eradication event**

5 Develop the Eradication Action Plan

- **Another response**
  - **Delay eradication event and start incident response process over**
  - **More appropriate when attacker gains access for a significant period and compromises more systems than could be realistically remediated during the planned eradication event**

5 Develop the Eradication Action Plan

- **Eradication plan is often easy to design**
- **Because a limited number of actions are possible to comprehensively remove an attacker**
- **To remediate a compromised system:**
  - **Rebuild from known good media, or**
  - **Implement detailed cleaning instructions to clean malware from system**

5 Develop the Eradication Action Plan

- **To recover from compromised credentials**
  - **Change password, or**
  - **Delete/disable account and issue a new one**

5 Develop the Eradication Action Plan

- **Improper planning is the biggest contributor to incomplete or failed eradication**
- **Organization may plan to disconnect from Internet during eradication event**
  - **But most organizations cannot tolerate completely disconnecting from the Internet**
  - **Some business applications must remain operational 24/7**
  - **Must implement extra measures on next two slides**

5 Develop the Eradication Action Plan

- Ensure that those business-critical systems do not have access to systems outside of their specific DMZ.
- Network connectivity between various geographical sites will need to remain intact to allow the various IT teams to implement the eradication actions.
- Business-to-business connections will have to be evaluated to see which connections can be disconnected and which need to remain operational. For those business-to-business connections that need to remain operational, the remediation team needs to ensure that Internet-bound traffic cannot traverse the link.

5 Develop the Eradication Action Plan

- Remote VPN connectivity will likely need to remain operational in order to allow IT staff to work from remote locations and yet still implement the eradication event action items. However, the number of user accounts allowed to connect to the VPN during the eradication event should be limited to necessary IT personnel, investigation, and remediation team members only. In addition, split-tunneling through the VPN should be disabled to provide an additional layer of caution.
- Before any system is allowed to connect (remotely or in-office) to the compromised environment to work on the eradication event, it should be verified to be clean.

5 Develop the Eradication Action Plan

- **Changing all passwords**
  - Standard Windows, Linux, and Mac user accounts
  - Service accounts
  - Local administrator or root accounts
  - Any other accounts integrated with the local credential database (whether Microsoft Active Directory, other LDAP solution, or NIS)
  - Application accounts
  - Networking gear accounts
  - Database accounts

5 Develop the Eradication Action Plan

- **Application, networking gear, and database accounts may not need to change**
- **Forcing password resets of users is easy**
  - **But attacker might be the one who changes the password**

5 Develop the Eradication Action Plan

- **Safer ways to change passwords**
  - **Generate random passwords for all accounts and distribute them to users via a trusted means**
  - **Require uses to call into help desk to grant them VPN access to change their passwords**

5 Develop the Eradication Action Plan

- **Changing service account passwords**
  - **Planning is required**
  - **Must determine which applications use a service account**
  - **Identify all systems with that application installed**
  - **Must change password on every system and central directory**
  - **Prepare contingency plan for systems that are missed in initial planning**

5 Develop the Eradication Action Plan

- **Changing all local administrator passwords to something unique is very challenging**
  - **Some organizations use the same password for all local administrator accounts**
  - **Some develop their own scripts to implement and track passwords for local administrator accounts**
  - **Others use credential vaults and management software that randomizes all the passwords on al systems and requires administrators to check out and check in passwords**

5 Develop the Eradication Action Plan

- **Plan how to back up user and critical data from the compromised systems being rebuilt**
- **Remediation team should sign off on the directories and files being backed up**
    - **Ton ensure that malware is not accidentally transferred to the new system**
- **In case that happens, also block malicious IP addresses and blackhole domain names (defense in depth)**

5 Develop the Eradication Action Plan

- **Common complications**

- A user is on vacation or traveling and does not change their password within a timely manner.
- A user account is no longer active but was never disabled, so the password is never changed.
- Systems that do not belong to the domain will not be affected by most types of automated password changes.
- Local user accounts that have administrative rights assigned, but are not the standard local administrator account.

6 Determine Eradication Event Timing and Execute Eradication Plan

- **Timing is critical**
- **Too early**
  - **Investigation team hasn't adequately scoped the compromise**
  - **Remediation fails because attacker's access is not completely removed**
  - **Ex: a backdoor was missed**

6 Determine Eradication Event Timing and Execute Eradication Plan

- **Too late**
- **Attacker may change Tools, Tactics, and Procedures (TTP)**
- **Or accomplish their mission**

6 Determine Eradication Event Timing and Execute Eradication Plan

- **Ideal time: "strike zone"**
  - **When investigation team has properly scoped the compromise**
  - **Remediation team has implemented all or most of the posturing/containment actions**
  - **Investigation team understands the majority of the attacker's TTP and can reliably detect malicious activity**

6 Determine Eradication Event Timing and Execute Eradication Plan

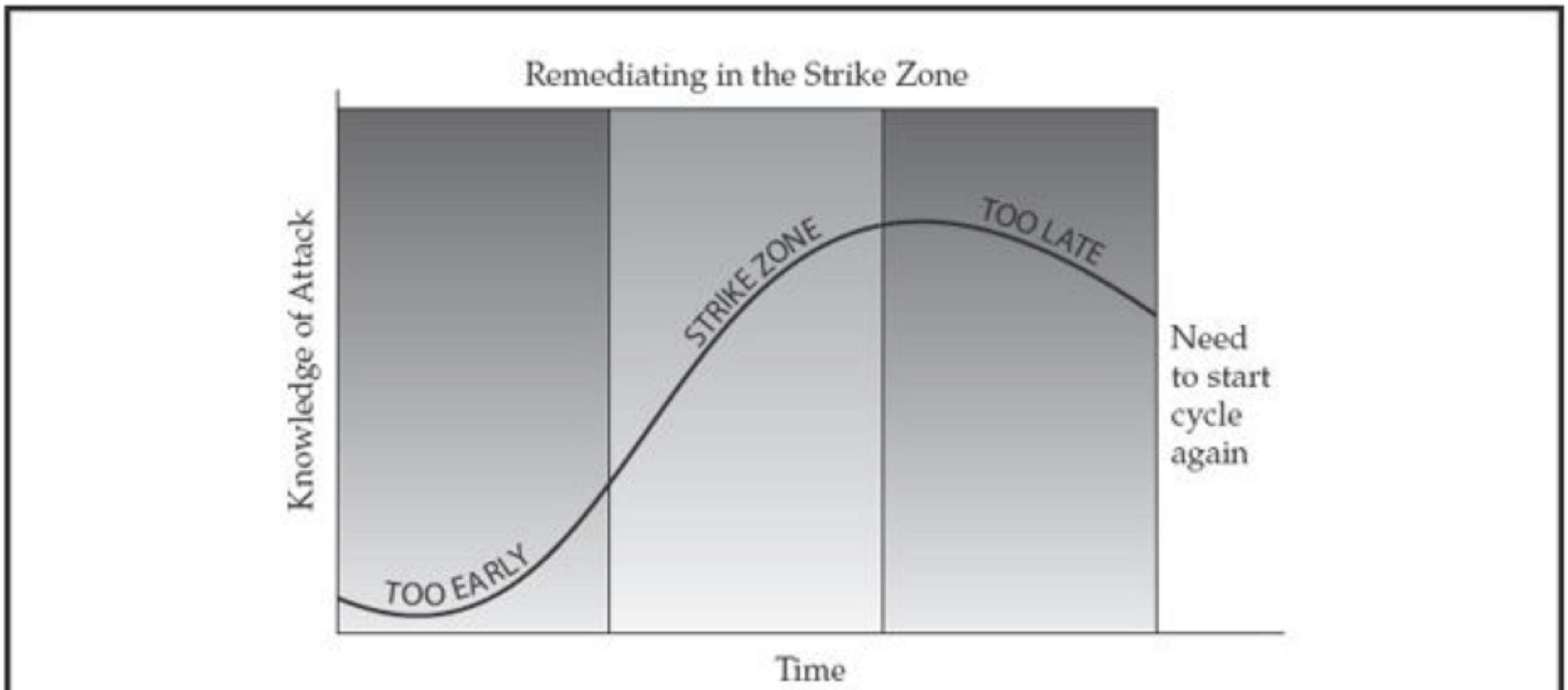


Figure 17-2. Remediating in the strike zone

Strike Zone Indicators

- The investigation team believes they have good visibility into the breached environment and they understand the attacker's TTPs.
- The number of compromised systems discovered per day (or other time period) has decreased significantly.
- Most of the compromised systems detected contain known indicators of compromise.
- The remediation effort has been thoroughly planned.

6 Determine Eradication Event Timing and Execute Eradication Plan

- **Timing of eradication event should be agreed upon by**
  - **Incident owner**
  - **Investigation owner**
  - **Remediation owner**
- **While the investigation and remediation efforts are ongoing**

6 Determine Eradication Event Timing and Execute Eradication Plan

- **It's an art, not a science**
- **Best way:**
  - **Choose a date that is considered a little difficult to achieve**
  - **Then force the teams to work hard to achieve the date**
- **Don't let the eradication date slip, or it may lost urgency and be delayed indefinitely**
  - **Organizations are never as prepared as they want to be**

6 Determine Eradication Event Timing and Execute Eradication Plan

- **Sample eradication event**
  - Disconnect from the Internet.
  - Block known malicious IPs and blackhole malicious domain names.
  - Remove compromised systems from the network and rebuild.
  - Change all user account passwords.
  - Verify all eradication event activities.

6 Determine Eradication Event Timing and Execute Eradication Plan

- **After disconnecting from Internet, blocking, and sinkholing**
  - **Test network connections**
    - **Browse to legitimate websites, try to FTP to legitimate FTP servers, attempt to access some blocked IP addresses**
    - **From all locations that have their own IP addresses**

6 Determine Eradication Event Timing and Execute Eradication Plan

- **Test from all logical and geographic sites**
- **Don't just PING**
- **You could use netcat and nmap**
- **Also implement alerts when known malicious IP addresses or domains are accessed**

6 Determine Eradication Event Timing and Execute Eradication Plan

- **Remediating compromised systems**
  - **Rebuilding or removing malware**
  - **Be careful when restoring data**
    - **Not to reintroduce malware**

6 Determine Eradication Event Timing and Execute Eradication Plan

- **Cleaning is not recommended**
  - **Removing known malware**
  - **It's difficult to be certain that all malware was discovered and removed**
  - **Rebuilding from known-good media is the best way to ensure a clean environment post-remediation**

6 Determine Eradication Event Timing and Execute Eradication Plan

- **Cleaning may be required when**
  - **Production servers are involved and downtime is not acceptable**
  - **Attacker compromised hundreds or thousands of systems**

6 Determine Eradication Event Timing and Execute Eradication Plan

- **Once compromises systems are offline, start changing user account passwords**
  - **This can proceed while other systems are being rebuilt**
- **Start early because use account password changes are the hardest part of the eradication event and take the most time**
  - **And cause the most unanticipated issues**

6 Determine Eradication Event Timing and Execute Eradication Plan

- **Verify that eradication was successful before reconnecting to the Internet**

- **Often a small number of systems are overlooked, improperly rebuilt, or not rebuilt at all**

- **Some administrators try to cut corners and clean malware from systems instead of rebuilding them**

- **Such systems may still have IOC's like registry entries or configuration files**

6 Determine Eradication Event Timing and Execute Eradication Plan

- **Verify that all user account passwords were changed**
  - **Usually by expiring them in Active Directory**
- **To verify that local administrator, database, and application passwords were changed**
  - **Test samples**

6 Determine Eradication Event Timing and Execute Eradication Plan

- **Communication is critical during eradication event**
  - **To let administrators know when they can start the next action item, and when previous action items are completed**
- **You will most likely encounter unexpected challenges**
- **Remediation owner should establish a communication medium prior to the eradication event**

6 Determine Eradication Event Timing and Execute Eradication Plan

- **Example communications strategies**
  - **Establish periodic set times for all administrators and members of the remediation to call in to discuss progress**
  - **Keep a conference bridge open throughout the eradication event**

6 Determine Eradication Event Timing and Execute Eradication Plan

- **Eradication team includes more people than the remediation team**
  - **All network, system and application administrators are required to participate, under the guidance of the remediation team**
- **In the days after the eradication event,**
  - **Ensure that your help desk personnel can contact the remediation team**
  - **In case suspicious activity or failed applications are reported**

7 Develop Strategic Recommendations

- **Actions that are critical to organization's overall security posture**
  - **But cannot be implemented prior to, or during, the eradication event**
- **Difficult to implement and disruptive**
  - **But offer significant security enhancements**

7 Develop Strategic Recommendations

- **Examples**

  - **Upgrading to a more secure OS throughout the environment**

  - **Reducing user privileges throughout the environment**

  - **Implementing strict network segmentation**

  - **implementing egress traffic filtering**

7 Develop Strategic Recommendations

- **Describe action items from a high level only**
- **Document all recommended strategic actions**
  - **Even if you don't believe organization is willing to implement them**
- **They may decide to implement them later**
- **Always document recommendations in order of priority**
  - **Put the ones that reduce risk the most first**

8. Document Lessons Learned

- **Only required for major remediation efforts**
  - **Not small actions like rebuilding a single system due to a virus**
- **Capture lessons learned in a standard, structured format in an easily accessible central location**
- **Use a template to ensure consistency**

8. Document Lessons Learned

- **Lessons should be easily searchable and browsable**

- **Wikis and document management systems work well**

8. Document Lessons Learned

- **Example: password change procedures**
  - **How to change all Unix passwords**
  - **How to create unique passwords for local administrator accounts on all Windows systems**
  - **How to determine all scripts and applications with hardcoded passwords**
  - **How to determine all service accounts**

8. Document Lessons Learned

- **Identification of all systems, applications, and scripts that use user accounts**
- **Winning executive and business-level support for this remediation action**
- **Getting standard users to comply with this action item**

8. Document Lessons Learned

- **Document lessons quickly**
  - **If you wait days or weeks, remediation team may forget information or have trouble compiling it**
- **Remediation owner should ensure that the team understands that creating lessons learned is a mandatory part of the remediation effort**

8. Document Lessons Learned

This may be an obvious point, but avoid storing information on prior investigations on systems connected to corporate domains or directories. This type of information, essentially blueprints for how your incident response (IR) team operates, would be incredibly useful to future attackers. If you must store it online, stand up independent servers and storage that is managed by the IR team.