Incidents Response

Prepared By:
Kazim Ali Obad

Supervisor:

Anmar Mohammed

MOHAMMED .B. HASSAN

Contents

Containment Limiting the Damage

Containment refers to actions taken by the IR team to limit the incident's scope and prevent the threat from causing further damage. It comes directly after Detection and Analysis the moment you have confirmed an attack is happening.

There are always two goals that must be balanced at the same time:

1. Prevent the attack from spreading further
2. Preserve the digital evidence (forensic artifacts) for investigation

NOTE: These two goals can conflict. Some containment actions that stop the attack also destroy the evidence. The order you take actions in is therefore critical always ask before every action: 'Will this impact the attack evidence?'

The Challenge of Evidence Preservation

Some of the most natural first instincts during an incident are the most damaging to your investigation:

- Shutting down a compromised machine erases volatile memory (RAM), which contains running processes, active network connections, encryption keys, and attacker tools that only exist in memory
- Disabling services may alter registry keys or log files
- Deleting suspicious files destroys forensic artifacts before they can be imaged
- Wiping the disk permanently removes all evidence

The Three Containment Stages

Containment is broken into three sequential stages. Follow this order every time.

Stage 1 Pre Evidence Collection Containment (Non Destructive Actions)

These are actions that limit the attack's spread without altering or destroying forensic evidence. You act at the network level not on the machine itself.

- Block malicious IPs at the firewall create a policy to deny outbound connections to the C2 (Command and Control) server
- Isolate infected network segments use firewall zone rules to prevent lateral movement to other parts of the network
- Sinkhole malware traffic redirect the malicious domain (e.g., xyz.attacker.com) to a controlled dummy IP
- This disrupts C2 communication while allowing you to capture and analyse the malware's traffic patterns

> **Sinkhole Technique:** Instead of simply blocking the C2 domain, you update your internal DNS to point the domain to an IP you control. The malware connects to your dummy machine instead of the real C2 server. You can now observe exactly what commands the malware sends, what data it tries to exfiltrate, and how it behaves without the attacker knowing.

Stage 2 Evidence Collection

With the machine still running and isolated, you now collect all available forensic evidence before taking any action that could alter or destroy data.

Collection priority order always follow this sequence:

- Memory (RAM) capture MOST CRITICAL and most time sensitive. Use Velociraptor (Windows.Triage.ProcessMemory), FTK Imager, or Magnet RAM Capture. RAM contains running processes, network connections, encryption keys, and injected code that disappears forever the moment the machine is shut down.
- Triage artifacts use KAPE (Kroll Artifact Parser and Extractor) to collect high value forensic artifacts: event logs, registry hives, prefetch files, browser history, scheduled tasks, malware files. KAPE does this without imaging the full disk.
- Disk image create a raw bit for bit copy of the hard drive using FTK Imager or dd. This preserves all files, deleted data, and malware binaries for deep analysis.
- Network traffic capture export packet captures from Wireshark, tcpdump, or SPAN port mirrors for the relevant time window of the attack.

Why Full Forensic Imaging Is Not Always Possible

In real world IR, you will face scale and resource constraints that make full disk imaging impractical:

- 200 infected systems × 500GB per drive = 100TB of storage required
- Imaging each machine takes hours during a live attack, time is critical
- Network bandwidth may not support transferring large images quickly

> **Key Point:** This is exactly why triage tools like KAPE exist. They extract only the most critical evidence not the entire disk allowing investigators to work fast at scale.

Key tools for evidence collection:

- KAPE (Kroll Artifact Parser and Extractor) fast, targeted artifact collection from live or offline systems. Extracts logs, registry, prefetch, and more without a full disk image.
- Velociraptor remote artifact collection across hundreds of machines simultaneously. We used this in the Wazuh section. It can push collection jobs to all machines and return results centrally.
- Volatility memory forensics. Analyses RAM dumps to identify malicious processes, injected code, network connections, and hidden artifacts.
- FTK Imager full disk imaging and file acquisition.
- Autopsy / X Ways Forensics disk analysis, deleted file recovery, attack timeline reconstruction.
- Wireshark / tcpdump network packet capture for traffic analysis.

> **Best Practice Document System Details:** Before imaging, always record: IP address, hostname, MAC address, physical location, owner name, and collection time. This is required for chain of custody ensuring the evidence is admissible in legal proceedings.

Stage 3 Post Evidence Collection Containment (Disruptive Actions)

Only after all forensic evidence is secured can you take actions that modify or destroy data:

- Terminate malicious processes using your EDR or Velociraptor
- Shut down infected systems if necessary
- Patch exploited vulnerabilities
- Disable and revoke compromised accounts
- Remove malware files, registry keys, and persistence mechanisms

> **Business Continuity:** If taking a critical production server offline is not feasible, implement temporary containment measures such as blocking specific ports or user accounts and plan a maintenance window for full remediation. Business continuity is always a factor in the containment decision.

The Malware Auto Destruct Problem

Some malware contains a self destruct mechanism. When it detects that its C2 connection is severed, or that the machine has been moved to a new network, it automatically deletes itself from disk. This is called 'sinkhole behaviour' the malware disappears when it knows it has been caught.

This is why the containment sequence matters so much:

NOTE: If you move the infected machine to a completely new IP range, the malware detects the network change and triggers self deletion. You lose all your forensic evidence. Always use VLAN isolation with the SAME IP address the machine moves to a new VLAN but keeps its original IP, so the malware does not detect the isolation.

Before isolating any machine:

- Check how the malware behaves read its code or known analysis reports if available
- Determine whether it has auto destruct or network detection logic
- Choose the correct isolation method accordingly VLAN with same IP is almost always safer than full disconnection

Determining the Order of Containment Actions

This was a question posed to the class. When deciding the order of containment actions, what should be your primary consideration?

The three options given:

- Benefit to business operations
- The required effort and time
- Action impact on digital evidence

> **Key Point:** The correct answer is: Action impact on digital evidence. The order of containment actions must first be determined by whether the action will destroy or alter forensic evidence. Evidence preservation drives the sequence not convenience, speed, or business preference.

Compromised Website Example

A company website (Scholarkazim.com) has been compromised. Detection and analysis are complete. What are your containment steps?

ANSWER

- Confirm the attack is on the web server hosting the site check whether other servers connected to it are also at risk and ensure the attack has not spread
- Use the WAF (Web Application Firewall) to identify source IPs, destination ports, and attack patterns block those specific IPs and ports
- Isolate the web server into a separate VLAN prevent lateral movement to the rest of the infrastructure
- Do NOT shut down the server this would destroy RAM evidence
- Capture memory, process list, active connections, and event logs using Velociraptor or KAPE
- Only after evidence collection take the server offline for remediation if necessary

Eradication Removing the Attacker & Fixing the Root Cause

Eradication means permanently removing the attacker's access, all tools and backdoors they left behind, and closing the security gaps that allowed them in. The goal is not just to stop the current attack it is to ensure it cannot happen again through the same path.

Three things must be accomplished:

- Root Cause Analysis (RCA) understand exactly how the attacker entered
- Remove all attacker artifacts malware, backdoors, persistence mechanisms, rogue accounts
- Fix the vulnerabilities patch systems, reconfigure controls, harden defences

Root Cause Analysis (RCA)

RCA goes beyond blaming the victim. It finds the real technical and procedural weaknesses that made the attack possible. Only by identifying every root cause can you ensure the same attack path is completely closed.

Example: Phishing Attack

Surface cause: 'A user clicked a malicious email link.'

The real root causes are a chain of missing controls:

1. **Security Awareness Gap** the employee did not recognise phishing indicators: spoofed sender address, mismatched URLs, unusual urgency in the email
2. **No Multi Factor Authentication (MFA)** if MFA was enabled, stolen credentials would be useless without the second factor

3. **Email Address Exposure** the employee's work email was used on public platforms (LinkedIn, Facebook, breached forums), making it an easy spear phishing target
4. **Weak Email Security Controls** no email security gateway (SEG) filtering; no SPF, DKIM, or DMARC records configured; dangerous attachment types (.exe, .scr, .vbs) were not blocked
5. **No External Threat Intelligence Feed** no subscription to services like Proofpoint or Mimecast that would have flagged the malicious sender domain before the email reached the inbox
6. **No MFA on VPN** if the attacker used stolen credentials to access the network via VPN, MFA would have stopped them at that point too

> **Key Point:** Root cause is never a single thing. It is always a chain. Your job is to find and break every link in that chain.

Tracing the Full Attack Timeline

A complete RCA traces the attacker's path from the very first foothold to their final action:

1. **Analyse past email logs** examine sender IP, email headers, and attachments
2. **Check for earlier failed attacks** were there blocked phishing attempts or exploit attempts before this one succeeded?
3. **Review firewall logs** look for C2 traffic and unusual outbound connections, especially to newly registered domains
4. **Identify other impacted systems** did the attacker move laterally to other departments or servers?
5. **Correlate SIEM logs** search for hidden persistence mechanisms, unusual scheduled tasks, and privilege escalation events

Identifying Other Vulnerable Systems

After finding the root cause, check whether other machines, accounts, or network segments are affected by the same weakness. Assume the attacker tested multiple entry points do not assume only one system was compromised.

Technical Vulnerability Scanning

- Use Nessus, OpenVAS, or Qualys to scan all systems for the same exploited vulnerability
- Examine SIEM logs for repeated exploit attempts across multiple endpoints
- Run Velociraptor across all machines to identify attacker traces

Checking for Persistence Mechanisms

These are the specific locations and commands to check:

Scheduled Tasks:

```
schtasks /query /fo LIST /v
```

Registry Run Keys (common persistence location):

```
reg query HKCU\Software\Microsoft\Windows\CurrentVersion\Run
```

All running services:

```
sc query state= all
```

PowerShell execution history:

```
Get-History
```

Hidden or unauthorised admin accounts:

```
net user /domain
net localgroup administrators
```

DLL injection requires memory analysis with Volatility. Look for:

- Legitimate processes (svchost.exe, explorer.exe) with injected foreign DLLs
- Memory regions marked executable that should not be
- Processes running from unusual locations (e.g., AppData instead of System32)

Non-Technical (People & Process) Checks

- Password reuse if passwords were stolen, were they reused on other systems or external services?
- Access log audit who accessed sensitive systems in the last 30 days? Any unusual access times or locations?
- MFA enrollment review were compromised accounts missing MFA?

Remediation Fixing the Gaps

People Fixes

- Require employees to remove work email addresses from public platforms (LinkedIn, Facebook, public forums)
- Run phishing simulation training using tools like KnowBe4 send fake phishing emails to employees, track who clicks, provide targeted training

Process Fixes

- Enforce MFA on all accounts email, VPN, cloud applications, privileged accounts
- Subscribe to external threat intelligence feeds (Proofpoint, Mimecast) these provide real-time indicators of newly registered malicious domains and known attacker infrastructure
- Enable DKIM, SPF, and DMARC DNS records these prevent email spoofing and ensure only legitimate servers can send email from your domain
- Filter dangerous email attachment types at the gateway (.exe, .scr, .vbs, .ps1)

Technical Fixes

- Deploy Canary Tokens on login pages these alert you if attackers clone your login page for phishing

- Block newly registered domains at the network level Cisco Umbrella and Palo Alto can block DNS queries to domains registered in the last 30 days, which is when most malicious domains are used
- Deploy Sysmon + Elastic Stack (or Sysmon + Wazuh) to increase endpoint visibility every process creation, network connection, and file modification is logged
- Enable application allow listing (Microsoft Defender Application Control) only approved applications can run; unknown executables are blocked

> **Canary Tokens:** A canary token is a fake login page or credential that you plant deliberately. If an attacker clones your login page and tricks a user into entering credentials there, you receive an immediate alert showing the attacker's IP, browser, and timing. It is an early warning system embedded in the attack itself.

Removing the Attacker's Tools & Persistence

The attacker likely left multiple backdoors to ensure they can return even if their primary access is removed. Every one of these must be found and eliminated.

Malicious Files

Search for attacker tools left on the system:

```
dir /s /b C:\Users\Public\*.exe
dir /s /b C:\Windows\Temp\*.exe
```

Persistence Mechanisms — Remove All of These

Remove malicious scheduled tasks:

```
schtasks /delete /tn "<TaskName>" /f
```

Delete registry persistence keys:

```
reg delete HKCU\Software\Microsoft\Windows\CurrentVersion\Run /v "<ValueName>" /f
```

Disable and delete rogue services:

```
sc stop <ServiceName>
sc delete <ServiceName>
```

Clear PowerShell execution history:

```
Remove-Item -Path
"$env:APPDATA\Microsoft\Windows\PowerShell\PSReadLine\ConsoleHost_history.txt"
```

Compromised Accounts

- Reset all passwords, especially privileged accounts — do not just change the password, revoke all active sessions and tokens
- Rotate API keys and SSH keys if they may have been exposed
- Reset VPN credentials for all accounts active during the incident window

Network Cleanup

- Block all outbound connections to attacker-controlled domains and IPs at the firewall — permanently
- Remove any DNS entries the attacker may have modified

Recovery Safely Restoring Operations

Recovery is the process of bringing your systems back online in a verified clean state without introducing new risks. It is not just 'restore and restart.' It requires careful validation, controlled rollout, and intensive monitoring.

Data Recovery & System Restoration

Before restoring from backup, you must verify the backup itself was not compromised:

- Check backup integrity validate file checksums and compare against known good hashes
- Review backup access logs has anyone accessed the backup storage during the incident window?
- Verify the backup predates the initial compromise if the attacker had been in the environment for weeks, backups from that period may also be infected

Backup storage strategies discussed in class:

- On premises isolated backup stored on storage that is physically or logically separated from the main network
- Cloud backup stored in a separate cloud account (AWS, Azure, GCP) with no direct connection to the compromised environment
- Air gapped backup physically disconnected storage that cannot be reached remotely at all

> **Student Example from Class:** A student working at a company in Dubai described their approach: sensitive data stored on their own on premise servers, general data stored in a cloud subscription. This separation means that even if the cloud is compromised, the most sensitive data on the local servers remains safe and vice versa. This is a recognised best practice.

Schedule staged recovery do not bring all systems back online simultaneously:

- Restore the most critical systems first (those required for business operations)
- Verify each system is clean and functioning before moving to the next
- Gradually expand access as confidence grows

Security & Operational Testing

Before declaring a system fully recovered:

- Confirm all security patches are applied re run vulnerability scans (Nessus, Qualys) to verify
- Verify log retention policies SIEM should be retaining logs for at least 6 months to support future investigations
- Test critical workflows payroll processing, database queries, authentication flows confirm nothing is broken
- Verify your EDR agent is running and reporting to the central console
- Confirm Sysmon is active and events are flowing to the SIEM

Continuous Monitoring After Recovery

The moment a restored system comes back online, intensive monitoring begins:

- Deploy Network IDS (NIDS) and Host IDS (HIDS) specifically tuned to the techniques used in this attack
- Write custom SIEM rules based on the attacker's TTPs (Tactics, Techniques, and Procedures) observed during the incident

- Monitor for at least 30 days for signs of reinfection or a second stage attack

Periodic validation checks the instructor recommended:

- Every 6 months review and refresh SIEM detection rules
- Run penetration tests simulating the same attack vector confirm it is now blocked
- Subscribe to threat intelligence on the specific threat actor if identified track whether they are targeting similar organisations

Post Incident Review

The post incident review also called 'lessons learned' is the final phase and arguably the most valuable. Every attack you survive should make your organization measurably harder to attack next time. If you do not improve after an incident, you have wasted the experience.

Lessons Learned Meeting

The meeting must be structured and produce concrete outputs:

- Analyse response speed calculate Mean Time to Detect (MTTD): how long between the attack starting and you detecting it? Calculate Mean Time to Respond (MTTR): how long between detection and containment?
- Identify security gaps what monitoring was missing? What controls failed? What did the attacker exploit that should have been blocked?
- Discuss what worked well and what did not during the response

Incident Report

The report must have three sections:

Executive Summary (for non technical stakeholders)

- What type of attack occurred? (Phishing, malware, ransomware, insider threat?)
- What was the business impact? (Downtime, financial loss, data exposure, reputational damage?)
- What has been done and what is the current status?

Technical Investigation Details (for security team)

- Detection method how was the attack detected? (SIEM alert, firewall log, user report, EDR alert?)
- Attack scope which systems were compromised? What data was accessed or stolen?
- Containment steps what was blocked, what was isolated, in what order?
- Evidence collected what artifacts were captured, from which systems, at what time?
- Eradication actions what malware was removed, what accounts were reset, what was patched?

Final Recommendations (action plan with owners and deadlines)

- Increase budget for security awareness training
- Invest in better phishing detection tools
- Deploy 24/7 monitoring if not already in place
- Specific technical hardening items identified during RCA

What the Review Tracks

The key metrics and questions to track:

- Detection timeline when was the first indicator? How long did it take to escalate and act?
- Was 24/7 monitoring in place? If not, why not?
- Were SIEM alerting rules properly tuned did we have false negatives?
- Were we using threat intelligence?
- Were MITRE ATT&CK techniques reflected in our detection rules?

- What was our patch status on affected systems?
- Was MFA enforced everywhere it should have been?
- What was the scope of data affected?
- What was the containment boundary what did we block, what did we isolate?

> **Key Point:** Tracking improvements based on lessons learned makes future incidents easier to manage. The documentation is not just a record it is a tool for continuous improvement and for justifying security investments to leadership.

Complete Incident Response Cycle Summary

Phase	Goal	Key Actions	Do NOT Do
Containment	Stop spread + preserve evidence simultaneously	Block C2 at firewall → VLAN isolate (same IP) → capture RAM → collect artifacts → then disruptive actions	Shut down first, change IP to new subnet, delete files before imaging
Eradication	Remove attacker completely + fix every root cause	Full RCA, check all persistence locations, reset accounts, patch vulns, harden email & endpoint	Assume a single fix is enough check every persistence location, scan all systems
Recovery	Restore verified clean systems with monitoring	Validate backup integrity, patch before restore, re enable EDR + SIEM, staged rollout, 30 day monitoring	Restore without verifying backup or bring system online without monitoring
Post Incident Review	Learn from the attack + measurably improve	Document full timeline, calculate MTTD/MTTR, identify all gaps, write action plan with owners + deadlines	Treat documentation as optional or skip the lessons learned meeting

Key Takeaways This Lecture

1. Containment = stopping the spread AND preserving evidence simultaneously. You cannot sacrifice one for the other.
2. The order of containment actions is determined first by impact on digital evidence not by speed or business preference.
3. Memory (RAM) capture is always your first evidence priority. It is the most time sensitive artifact. Never shut a machine down before capturing RAM.
4. VLAN isolation with the SAME IP is the correct isolation method. Changing the IP can trigger malware self destruct and wipe your evidence.
5. KAPE collects targeted forensic artifacts fast without a full disk image critical for large scale incidents.
6. Velociraptor deploys artifact collection across hundreds of machines remotely from a single console.
7. Root cause analysis must identify every missing control in the chain not just the final technical trigger.
8. Check every persistence location after an attack: scheduled tasks, registry run keys, services, DLL injection, admin accounts, login history.
9. Recovery is not complete when the system comes back online. It is complete after sustained clean monitoring.
10. Post incident review must produce a written action plan with named owners and deadlines not just a discussion.
11. No system is truly un hackable. The goal is to make attackers work harder, detect them faster, and respond better each time.
12. Document everything your documentation is your evidence, your defence, and your professional reputation.