COHESITY

WHITE PAPER

How to formulate a “wartime” response strategy to destructive cyberattacks

Recover from ransomware and other cyber threats securely and rapidly with Cohesity

TABLE OF CONTENTS

Executive summary 3

Situation analysis: Why your organization operates differently in "peacetime" and "wartime" 4

Why destructive cyberattacks differ from business continuity 6

Investigating and remediating traditional malware vs. ransomware 7

The indicators of compromise (IOCs) misconception 8

Winning the war: Investigation, threat mitigation, and secure recovery 9

Cybersecurity digital forensics and incident response best practices 10

Achieving operational best practices with Cohesity 11

- Identification 11
- Containment 12
- Revisiting identification: How the Cohesity Clean Room solution helps 14
- Eradication and recovery 16

Lessons learned 18

Summary 19

About Cohesity 20

Recommended reading 21

Executive summary

Destructive cyberattacks, like ransomware and wiper attacks, require a different approach from IT operations—compared to traditional business continuity and disaster recovery scenarios. Cybersecurity operations teams face several challenges in ensuring that appropriate investigations and threat remediations are undertaken. It is not enough to just restore the delivery of its products and services as quickly as possible. Organizations must also ensure that the recovery is done securely to prevent further downtime due to reinfection or reattack.

This white paper documents the best practices for dealing with destructive cyberattacks and highlights how Cohesity can help your organization achieve those operational outcomes.

Situation analysis: Why your organization operates differently in "peacetime" and "wartime"

"Peacetime" is the normal day-to-day operations of your organization. Alerts from security tooling typically make their way onto the consoles of your Security Operations Center (SOC) or managed security service provider (MSSP). These alerts are triaged for prioritization, and for tuning out false positives, while further evidence is gathered to identify signs of intrusion inside your organization's infrastructure. When SOC analysts are confident that an adversary is attacking the organization, they declare an incident and continue their investigation. At this stage, the organization is in "wartime" mode.

During the investigation, if analysts discover that the confidentiality, integrity, or availability of the organization's systems and data has been compromised, they declare a breach and continue with their incident response process.

The time the adversary spent inside the organization before discovery is defined as their dwell time. The adversary may be discovered through security tooling alerts. But all too often, organizations only become aware of an attack when systems become unavailable. Dwell time can vary significantly—ranging from as little as four to five days in attacks using Ransomware-as-a-Service (RaaS), to hundreds of days in human-driven ransomware attacks, or even years in the case of nation-state actors.

Examples of how confidentially, integrity, or availability are compromised include:

- **Confidentiality**: The organization's data has been disclosed to unauthorized parties. This includes data exfiltration for criminal purposes by ransomware gangs or for espionage by nation-state actors before launching a wiper attack.
- **Integrity**: During the multiple stages of a destructive cyberattack, adversaries will change configuration files, registries, identity management systems, and potentially even firmware to maintain persistence within victim organizations. All these changes affect the integrity of systems.
- **Availability**: A destructive cyberattack aims to make the organization's IT infrastructure—which is needed to deliver products and services to customers—unavailable. They do this by encrypting data and/or systems, as seen in ransomware attacks, or deleting them, as in wiper attacks.

It is important to understand that not all incidents escalate into breaches, and a SOC continually detects and responds to incidents in their early stages to prevent them from becoming breaches. Some breaches are contained in the pockets of the organization and can be managed using standard incident response playbooks.

However, certain incidents—especially ransomware and wiper attacks—can have a broad impact. They can disable systems needed to deliver products and services to customers, and internal IT systems essential for managing the incident. These may include systems for physical access to facilities, communicating with regulators and impacted parties or data subjects, or coordinating with insurers, law enforcement, and the press. In such cases, the organization may declare a cyber **crisis** and undertake a different workflow to ensure they can manage the incident.

Once the security and IT teams have dealt with the incident, breach, or crisis, restored systems to a trusted state, and mitigated threats of recurrence, the organization can return to "peacetime" operations.

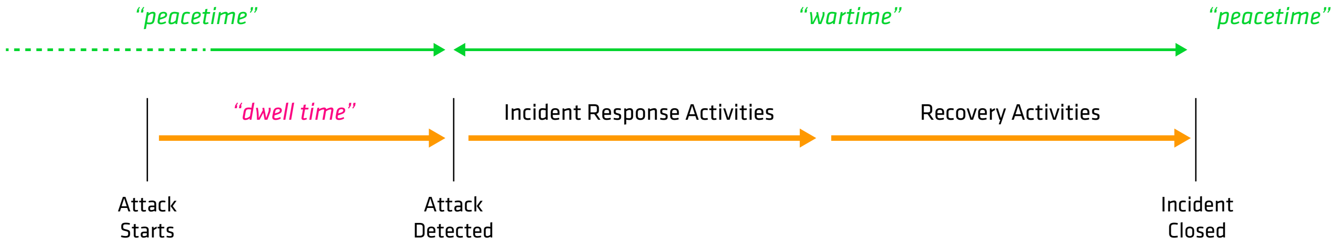


Figure 1. "Wartime" and "peacetime" stages in a destructive cyberattack.

Why destructive cyberattacks differ from business continuity

Before the advent of destructive cyberattacks, you could count on one hand the root causes of IT outages: flood, fire, equipment or software failure, misconfiguration, or power outage. These incidents required minimal investigation, and the standard response was simply to restore the last backup snapshot.

Ransomware, however, is far more complex. Unlike traditional viruses or worms, it isn't a single binary you can scan. Adversaries attack across a chain of 14 stages, choosing from hundreds of techniques to achieve their aims at each stage. They're constantly innovating, making yesterday's security control configurations ineffective today.

Compounding the threat, the current global geopolitical situation has increased the risk of wiper attacks by nation-state actors. With their unparalleled operational capability, funding, and motivation, these threat actors require organizations to build cyber resilience beyond that needed by criminal ransomware gangs.

Investigating and remediating traditional malware vs. ransomware

Traditional malware, such as viruses and worms, is detected by scanning systems for malicious binaries. Once identified, security teams can simply quarantine or delete the malicious binary. In contrast, ransomware or wiper attacks involve a chain of events that allow attackers to gain access within days of a newly announced vulnerability. These attacks can leverage your IT infrastructure to "live off the land," take advantage of authorized accounts, alter configurations to escalate privileges or maintain persistence, stage sensitive data for exfiltration, and use native scripting and macros built into your operating systems and applications—all while evading controls to hamper your ability to detect, respond, and recover. Unlike traditional malware, there is no single binary to scan for and remove.

Recovering securely from a ransomware or wiper attack requires investigating how the incident occurred. Organizations must remediate the threats and vulnerabilities found to prevent reinfection and further downtime. This is the essence of every best-practice cybersecurity incident response framework.

Organizations must remediate three critical areas to ensure you can resist a similar attack in the future and prevent the reinfection of recovered systems from the current attack:

1. **Attack surface**: The most common ransomware initial access vectors, in order of prevalence, are: vulnerabilities on internet-facing infrastructure, reused legitimate access credentials, and social engineering tactics, such as phishing emails. You need to understand how "patient zero"— the initial point of entry or the first identified victim—was compromised and then remediate the threat in recovered systems. This may involve patching vulnerable systems, placing the vulnerable systems behind some form of protection like a Web Application Firewall (WAF), and removing the phishing email that allowed initial access from a user's inbox.

2. **Evasion techniques or gaps in security controls**: Preventing or detecting security incidents early—before they impact confidentiality, integrity, or availability—incurs an operational cost but helps avoid revenue loss, reputational damage, and potential costly regulatory fines and litigation from business partners or impacted data subjects.

Ransomware gangs build evasion techniques into their RaaS platforms for common security controls, including endpoint detection and response (EDR) and extended detection and response (XDR). They also have a first-mover advantage to act before cyber threat intelligence feeds can be updated and disseminated to include their attack techniques.

Before resuming production, you must understand why existing security controls failed to stop or detect the attack before it interrupted the delivery of IT services. Then, you can ensure security tooling is restored to a trusted state and its rules updated to prevent or detect future attacks early.

3. **Persistence mechanisms**: In a typical ransomware or wiper attack, attackers often leave behind dozens of artifacts. These could implant a foothold, allowing attackers continued access if systems are recovered without fully understanding and removing what has been left behind. It is common for organizations to spend days recovering systems, only to have them infected within minutes, and go down, again due to an overlooked persistence mechanism. Due to the multi-stage nature of destructive cyberattacks, a combination of threat hunting and forensic analysis is typically needed to build an attack timeline to identify a comprehensive list of artifacts that must be addressed.

The indicators of compromise (IOCs) misconception

The concept of indicators of compromise (IOCs) is key to tactical cyber threat intelligence. Before discussing the wartime activities that organizations must undertake to deal with a destructive cyberattack, it is important to define an IOC.

IOCs provide clues indicating that a system ***may*** have been compromised. While they serve as a starting point for looking for adversary behavior, IOCs are often just signposts—not the destination. To recover securely, organizations must build a picture of the attack and analyze it to undertake the appropriate mitigations outlined in the previous section. For example, a changed configuration file that re-executes specific code on reboot is an IOC, as is a malicious DLL with the same name as a legitimate one that has been dropped into a directory. Similarly, manipulating the PATH variable to execute this malicious DLL before the legitimate one is also an IOC. While these IOCs tell us something is happening, they don't paint the full picture of the attack.

Hunting for IOCs is critical to cybersecurity incident response, but organizations must apply them in the right context. Relying solely on IOCs can lead to inappropriate actions. Further, prematurely restoring from backups without deeper investigation will allow reinfection or cause other availability issues.

Blindly quarantining files, or restoring to previous versions of the file from a backup snapshot containing the IOC, doesn't address the root cause. You still don't know how the attackers got in to make those changes in the first place —leaving them free to attack your systems and again and again. Additionally, reverting to older, incompatible configurations could create availability issues, especially if, for instance, binaries have been patched to later versions since the start of the attack.

Likewise, the absence of IOCs in a backup snapshot does not guarantee it is "clean." Since IOCs simply serve as signposts to malicious activities, removing the signposts still leaves the "destination" intact. In cases of automated reversion to older snapshots, this approach may leave the incident response team unaware of the underlying attack.

Detecting IOCs also relies on collecting, analyzing, and disseminating cyber threat intelligence, which often lags behind evolving adversary tactics. This means there is a delay between the adversary changing their behavior and our security tooling being aware of the new attack techniques. This explains why some of the world's largest organizations, despite having extensive cybersecurity budgets and teams that are certainly using the latest and greatest cybersecurity tooling, are still impacted by ransomware. The adversary changes their behavior before the current cybersecurity tooling becomes aware of that change, allowing them to get inside the organization undetected. Once inside, their defense evasion capability renders the endpoint security controls blind. By the time the security tool vendor becomes aware of the adversary's new behavior – and the relevant threat intelligence is fed into their tooling, it is too late. The tool has already been evaded, and it won't fire.

To mitigate these challenges, consider adopting a peacetime activity like periodic proactive threat hunting using a solution like **Cohesity DataHawk**. The solution operates independently of traditional security controls and can't be evaded. DataHawk allows you to find attacks that may have slipped through the net when cyber threat intelligence sources were unaware of them.

Winning the war: Investigation, threat mitigation, and secure recovery

The best approach is to build resilience and preparedness by having the right technological solutions as force multipliers for your incident responders, defining clear processes, and an operating model so everyone knows exactly what they need to do. Use automation and orchestration where possible. Additionally, staff must be properly trained and participate in realistic exercises to respond, rather than react, when the worst happens.

Cyber resilience isn't a product you can buy. It's an emergent property that arrives when your organization is prepared to do the right things after a cyber incident. To achieve cyber resilience, you must work with a vendor who is realistic about the challenges organizations face after a destructive cyberattack, and offers the right technology, and the necessary support for you to build a robust incident response strategy.

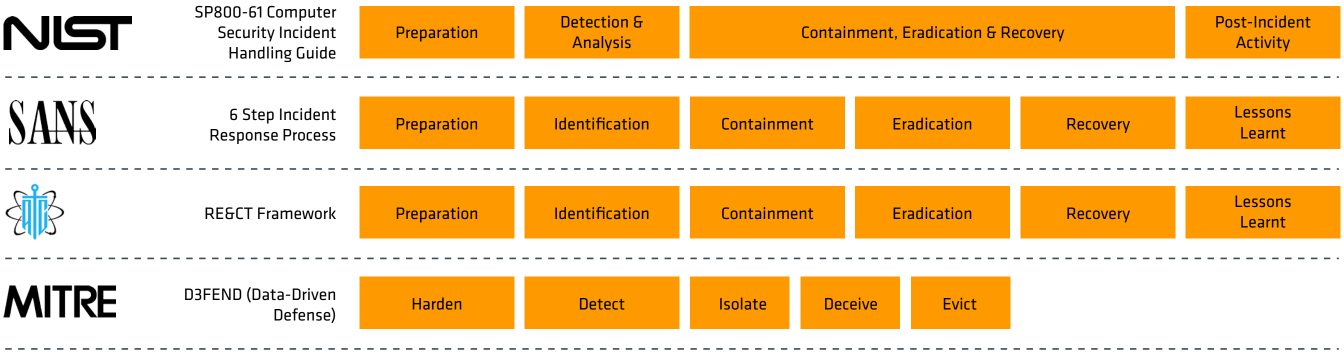
Cybersecurity incident response is a complex activity. Success comes from acknowledging that complexity—not ignoring it. Pretending otherwise will only come back to bite the organization at the worst possible time: during an incident.

Cybersecurity digital forensics and incident response best practices

There are four main widely-adopted frameworks for digital forensics and incident response:

1. NIST SP800-61 Computer Security Incident Handling Guide
2. SANS Institute Six-Step Incident Response Process
3. RE&CT ("React") Framework
4. MITRE D3FEND ("Data-Driven Defense")

In this whitepaper, we will focus on using the SANS Institute model. That said, all the frameworks are largely aligned on the steps needed to be taken to prepare for and respond to a cyberattack:



NIST	SP800-61 Computer Security Incident Handling Guide	Preparation	Detection & Analysis	Containment, Eradication & Recovery			Post-Incident Activity
SANS	6 Step Incident Response Process	Preparation	Identification	Containment	Eradication	Recovery	Lessons Learnt
	RE&CT Framework	Preparation	Identification	Containment	Eradication	Recovery	Lessons Learnt
MITRE	D3FEND (Data-Driven Defense)	Harden	Detect	Isolate	Deceive	Evict	

Figure 2. Cyber digital forensics and incident response best practices.

Achieving operational best practices with Cohesity

For wartime situations, all best practice cybersecurity incident response frameworks include the stages of containment, investigation, mitigation of threats, and, finally, recovery. Organizations that shortcut the containment, investigation, and mitigation stages and rush to recovery leave the vulnerabilities that allowed the attack in situ.

The gaps in defenses that did not detect or prevent the attack remain open, and often, the persistence mechanisms and other attack artifacts are brought back. This frequently results in reinfection or reattack and subsequent extended downtimes. It is not unusual to see organizations that take a recovery-centric approach to responding to ransomware attacks having to recover over a dozen times.

Identification

There are two stages involved in identification:

1. **Initial awareness that a potential incident is underway**: This can take the form of a report from a user or third party, which needs to be triaged to confirm its validity and scope, or an alert from some form of technical control.
2. **Understanding how the attack happened**: This ensures the appropriate eradication of the threat, removal of the vulnerabilities exploited, and bolstering controls, allowing systems to be recovered in a secure and resilient state.

Let's review each stage in more detail.

Initial awareness

Initial awareness is technically a peacetime activity, as wartime cannot be declared until the organization detects an attack is underway. Therefore, it is important to discuss the mechanisms to detect attacks like ransomware to understand how this can affect the incident response workflow.

RaaS platforms have commoditized the evasion of popular security tools such as EDR and XDR, rendering them blind to attack. In the MITRE ATT&CK framework, the most popular taxonomy for describing how cyberattacks are carried out, the Defense Evasion tactic has nearly double the number of techniques than the next nearest of the 13 tactics. These mechanisms used by ransomware attackers cannot evade Cohesity DataProtect's anomaly detection, and DataHawk's threat-hunting capabilities.

Alerts, such as those from DataProtect's AI-based anomaly detection, have a high degree of **confidence**, which trust that the alert isn't a false positive, as well as high **fidelity**, which is the amount of information about what is happening the SOC analyst receives by looking at the alert. This speeds up the triage and investigation process, decreasing the time needed to recover systems into production securely.

If, during triage, it becomes apparent that the systems required to respond to the incidents have been impacted, or that encryption or deletion of systems across the organization are above a certain predefined threshold, the organization can declare a **cyber crisis**. A predefined cyber-crisis workflow allows an organization to establish different escalations and pre-prescribed authority for incident responders to conduct certain actions beyond those they normally do for a cyber breach.

It may be discovered that the systems needed during incident response are impacted, unavailable, or untrustworthy. The issues in this situation may include:

- Contact lists for incident response stakeholders may be unavailable, such as executives, regulators, cyber insurance providers, retained incident response companies, supply chain partners, and the press.

- Incident response workflows may be unavailable.
- Contracts for your cyber insurance policy and retained incident responders may be unavailable.
- Management servers and configurations for physical access control systems or environmental controls for buildings may be down.
- Communications systems, such as email or Voice-over-IP, required to contact stakeholders may be down or in an untrusted state.
- Routers and switch configurations or firmware may be untrusted, making any connection to the internet for Software as a Service applications or communications subject to eavesdropping or disruption.
- Security tooling may have been evaded or rendered unusable.

Understandably, most organizations prioritize restoring the most critical applications first—those essential for resuming product and service delivery, also known as the Minimum Viable Company (MVC). However, organizations that suffer a destructive cyberattack realize that a subset of accounts, applications, and infrastructure is also needed to manage the incident effectively. These systems ensure that critical production systems can be not just recovered, but recovered into a **secure state** while satisfying the organization's regulatory obligations can be satisfied.

Cohesity defines this subset of essential infrastructure and resources for managing response and recovery efforts as the Minimum Viable Response Capability (MVRC). Suppose any components of the MVRC have become untrustworthy or unavailable. In that case, organizations need a rapid way to make these resources available and rebuild a trusted set of tooling to manage the response actions. The **Cohesity Clean Room solution** allows organizations to rapidly rebuild their MVRC to a trusted state and make the resources required to manage the incident available in minutes.

Understanding how the attack happened

Once the initial triage is completed, and there is confidence that a destructive cyberattack is underway, the analyst declares an incident and continues a deeper investigation. Typically, deploying encryptors to servers and endpoints is the last task ransomware gangs undertake, as it is the noisiest stage of the attack—both in terms of triggering detective controls and creating impacts visible to end users.

Focusing investigations and remediations only on encrypted systems is unlikely to uncover the root cause of the attack. Instead, the investigation needs to extend beyond these systems. Unencrypted systems are often of greater interest to the investigator, as they may contain persistence mechanisms that adversaries can use to return after any recovery attempt.

Before we look at this deeper level of identification in detail, it is important to understand how another aspect of all best-practice incident response processes can impede our ability to conduct this task: containment.

Containment

Containment is a requirement of all the incident response frameworks, as it prevents the spread of the attack and interrupts any command-and-control or data exfiltration activities. However, containment also presents some challenges for security operations teams:

- **Remote imaging doesn't work in isolation**. Most organizations have moved from physically acquiring hard disk contents to remote forensic imaging. However, isolating an infected host—or host's network—can suddenly remove the organization's capability to undertake this task. **DataProtect** provides a user interface and API that allows the incident responder to perform file-level forensics on not just the last snapshot, but across a whole time series of snapshots up to the organization's retention period. This provides digital forensic analysts the superpower of time travel, allowing them to look for binaries and other artifacts that the adversary has already cleaned up, and quickly identify malicious deltas made to configurations and other files. Unlike endpoint security solutions and SIEMs that typically only retain a short timeline of logs, Cohesity allows incident responders to examine events and log contents over the entire period for which backups are held for that system, all delivered by an immutable platform to ensure a strong chain of custody. Best of all, these capabilities are provided without a network connection.

It is immune to eavesdropping and disruption, as DataProtect uses an offline copy of the filesystem for this task.

- **Endpoint solutions become isolated, and query/response becomes impossible.** While the architecture of different endpoint solutions, such as EDRs and XDRs, may differ, almost all have a central management server that receives telemetry from endpoint clients. If containment severs the connection between the management server and endpoints, analysts are left with only the information previously sent to the management server. They can no longer work in a query-and-response fashion to drill deeper into what is happening on the endpoints in real time.
- Containment also includes establishing isolated environments where incident response and recovery techniques can occur. The Cohesity Clean Room solution provides a flexible approach to creating such environments. It helps organizations align with incident response best practices and adopt an appropriate shared responsibility model between security and IT operations. This approach helps organizations avoid extended downtime and prevent reinfection after recovery.
- The Cohesity Clean Room solution:
- Allows for the rapid restoration of the MVRC or impacted or evaded infrastructure, which is essential for investigating and remediating the incident.
- Establishes an isolated investigatory environment that allows security operations teams to use the native security capabilities of the **Cohesity Data Cloud platform** alongside their other security tooling to understand the end-to-end attack and plan the appropriate remediations to prevent future attacks.
- Creates an isolated mitigation environment where the results of the security operations team's investigation inform remediations, such as rapidly rebuilding systems from known-good install images and configurations, recovering systems and patching their vulnerabilities, bolstering controls so they can't be evaded and successfully preventing or detecting future similar attacks. Finally, systems can be tested for functionality and performance—before being restored to production systems.

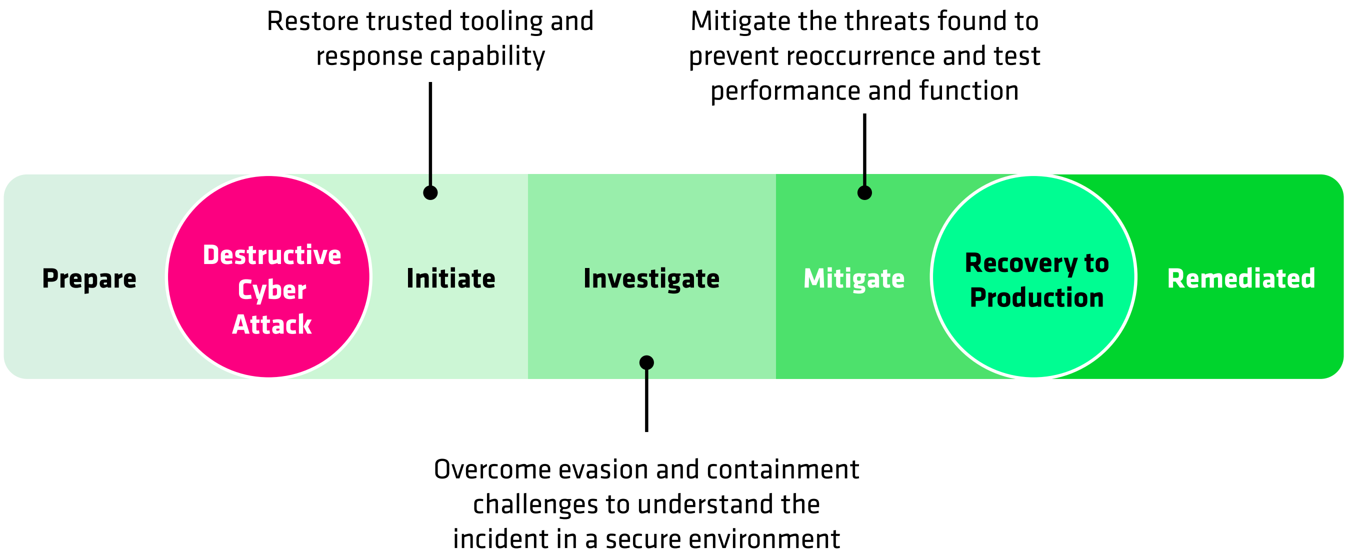

Restore trusted tooling and response capability
Mitigate the threats found to prevent reoccurrence and test performance and function
Prepare
Destructive Cyber Attack
Initiate
Investigate
Mitigate
Recovery to Production
Remediated
Overcome evasion and containment challenges to understand the incident in a secure environment

Figure 3. The four stages of the Cohesity Clean Room solution taking customers to remediation of cyberattack.

Revisiting identification: How the Cohesity Clean Room solution helps

Following digital forensics and incident response best practices, the organization has now contained the infected networks and hosts. At this stage, any impacted infrastructure needed to investigate and remediate the incident would be re-established to a trusted state: you can trust your connection to the internet and use your cloud-based IT, business, and security services. Also, your communication capability with stakeholders would be reestablished. Most importantly, all the documentation and resources needed to support incident response and recovery are at the fingertips of your security and IT operations teams.

We will now examine how Cohesity helps with the deeper level of investigation while the assets you're investigating have been isolated by containment.

Discovering vulnerabilities exploited in the attack

Ransomware gangs and nation-states prepositioning for wiper attacks most commonly gain initial access through vulnerabilities in internet-facing assets. Adversaries have even been known to gain initial access through vulnerabilities, and install persistence mechanisms, allowing them to remain and then patch them to prevent other attackers from gaining access to those systems.

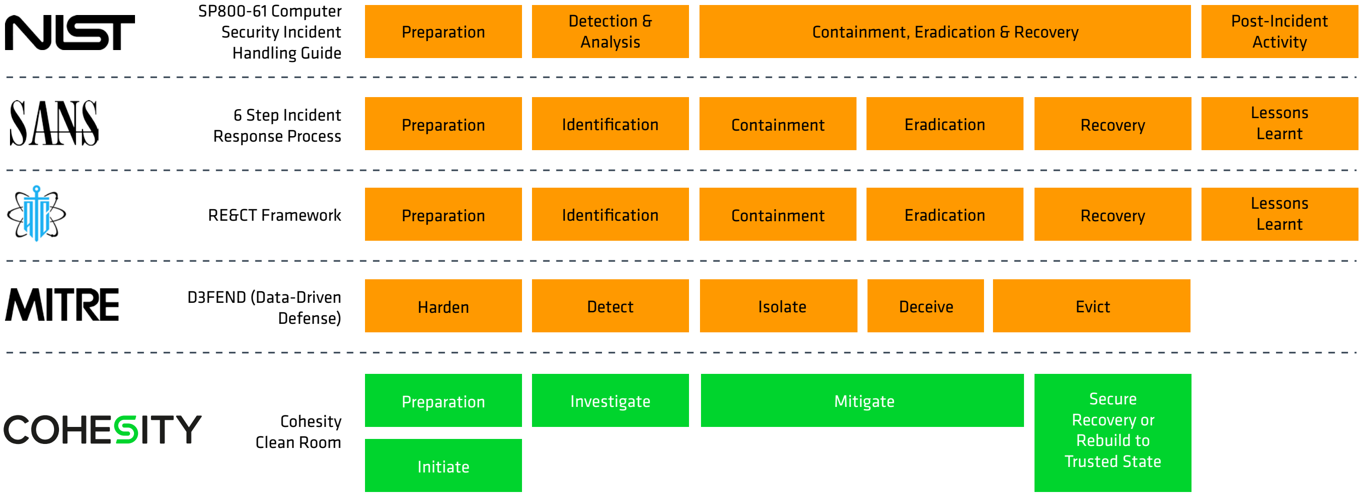
How can organizations establish which vulnerabilities existed at the time of an attack? This becomes even more challenging if the adversary has wiped the system or if containment measures prevent access to the system for a vulnerability scan.

The **Cohesity CyberScan** provides a solution by allowing organizations to scan backup snapshots for vulnerabilities using their Tenable Vulnerability Management license. This allows security teams to identify vulnerabilities during an attack, even if a system is unreachable due to containment, has been wiped, or was patched by an adversary after an intrusion.

Performing file system forensics

File system forensics is a core discipline of incident response. Many organizations use remote acquisition tools for forensic imaging. However, once containment measures are in place, the systems requiring forensic imaging are often no longer accessible.

DataProtect provides analysts access to not just a single volume snapshot of the file systems but also an entire time series of snapshots. This allows forensic examiners to look back at an incident timeline and across the entire backup retention period. A time series of volumes



NIST	SP800-61 Computer Security Incident Handling Guide	Preparation	Detection & Analysis	Containment, Eradication & Recovery			Post-Incident Activity
SANS	6 Step Incident Response Process	Preparation	Identification	Containment	Eradication	Recovery	Lessons Learnt
	RE&CT Framework	Preparation	Identification	Containment	Eradication	Recovery	Lessons Learnt
MITRE	D3FEND (Data-Driven Defense)	Harden	Detect	Isolate	Deceive	Evict	
COHESITY	Cohesity Clean Room	Preparation Initiate	Investigate	Mitigate		Secure Recovery or Rebuild to Trusted State	

Figure 4. Cohesity Clean Room alignment to incident response best practices

can be rapidly mounted and compared to identify malicious deltas. File objects can be extracted for reverse engineering, detonation in sandboxes, or analysis by sending them to cloud-based services.

In traditional digital forensics, incident responders typically gather a single image of the system post-attack, form a hypothesis on how the system got to that end state, and then work back to gather evidence to support or debunk that theory. In contrast, using DataProtect, incident responders can now see file system changes laid out across much more of the incident timeline, which continues to work even if containment efforts have isolated the infected host.

Threat hunting

Hunting for IOCs is another task that incident responders typically must do. This wartime hunting fits into two categories:

Scanning for IOCs supplied by a third party. These third parties can include a cyber threat intelligence vendor, government agency, or peer organizations. Cohesity customers using DataHawk can take advantage of the frequently updated feed of over 117,000 IOCs in use by ransomware and nation-state actors. DataHawk's threat scanning capability also supports commercial CrowdStrike threat intelligence feeds that the organization has licensed and can consume any IOC supplied in YARA format from other third parties.

Scanning for IOCs discovered by your organization. As your incident responders find artifacts during an investigation, they will want to hunt to see if these IOCs exist across the organization's infrastructure. From there, they will determine whether additional systems should be brought into the scope of the incident response.

This is commonly done by creating YARA rules that describe the found artifact in a way that allows detection but avoids unnecessary false positives. With Cohesity, you could conduct forensic analysis (as discussed in the previous section), extract file system artifacts, and detonate them in sandboxes like Cuckoo, which, through a plugin, can automatically generate YARA rules for any IOCs related to that file. The DataHawk hunting capability is not reliant on endpoint agents. It continues to function even if the organization has isolated systems for containment. It isn't vulnerable to the common defense evasion techniques that render end-point security solutions unable to hunt effectively.

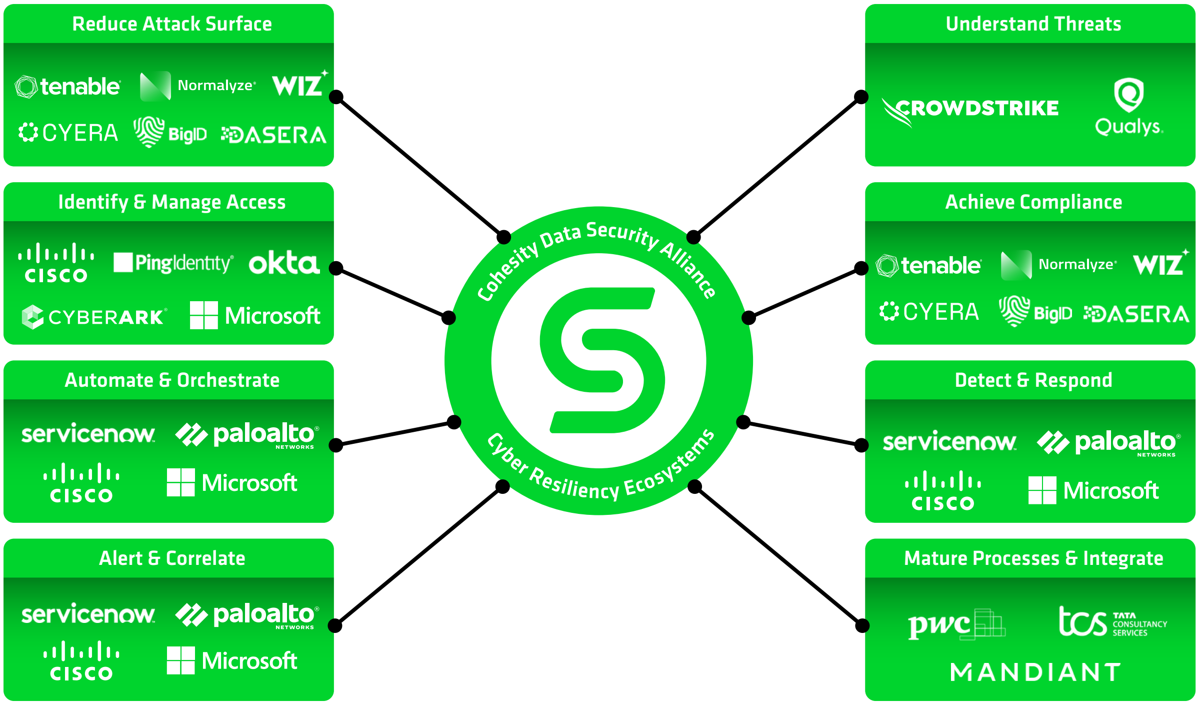


Figure 5. Cohesity Data Security Alliance: An ecosystem for cyber resilience.

Capabilities such as the **Cohesity Global Search** allow incident responders to quickly hunt files across all the backed-up infrastructure, which can help direct investigation efforts when looking for a particular artifact or file.

Achieving regulatory compliance

In addition to mandating solid incident response processes, many recently updated compliance regulations—such as HIPAA, DORA, and NIS 2—require organizations to notify regulators and impacted data subjects in the event of a cybersecurity breach. Understanding the nature of the breach is a part of the identification stage, as is understanding its impact and ensuring timely notification.

If the incident has impacted communication, Cohesity, as part of the MVRC, helps restore this capability. Communication templates can be held in the **Digital Jump Bag**™ —the foundation of a clean room. Additionally, DataHawk can **scan backups to identify sensitive and regulated data**, helping organizations meet regulatory requirements. This is especially valuable after a destructive cyberattack when critical data stores become encrypted or wiped.

Security operations tooling integration

Cyber resilience is a team sport—no single vendor's solution can investigate and remediate an incident in its entirety. This is why Cohesity established the **Data Security Alliance**. This collaborative ecosystem allows the power of data and data over time to be brought to wider security tooling and services through integrations for common governance, investigation, and recovery.

Automation and orchestration

Cohesity supports API integration, which allows a security orchestration and automated response (SOAR) platform to drive these investigatory tasks, further increasing analyst efficiency.

Eradication and recovery

We've merged the stages of eradication and recovery into mitigation because, to Cohesity, no organization should be looking to recover from a destructive cyberattack without taking the appropriate steps to ensure that the adversary attacking the organization cannot reinfect systems or that a future attack of the same nature won't be successful.

The Cohesity Clean Room solution supports rapid volume recovery, enabling an entire file system to be recovered before applying mitigations to eradicate threats. This ensures secure system recovery while also facilitating the fast rebuilding of systems from trusted software images and known-good configurations. Each approach has its pros and cons:

Recover and clean approach	
Pro:	**Con:**
It is simpler to manage ahead of an incident.	Investigations must dive deeper.
	The time to remediate is typically longer than that needed for rebuilt systems.
Rebuild approach	
Pro:	**Con:**
Opportunity to recover data, rebuild systems, and investigate incidents in parallel, providing the shortest possible recovery of systems into a secure state.	The investigation typically does not need to be as in-depth as systems are in a trusted state.
The remediation is shorter, typically only validating the security of configurations, bolstering controls and patching any vulnerable systems.	It requires skills to build reinstallation scripts.
	Installation media, license keys, configuration files, and scripts must be maintained in the digital jump bag.

Some Cohesity customers choose to support both volume-level backups and rebuilds. This gives them the option of choosing the most appropriate method of secure recovery for each compromised host depending on the level of effort involved in cleaning that system and the degree of confidence that the cleaning will not leave attack artifacts.

Customers often repurpose their development environment to use as the Cohesity Clean Room mitigation environment. This approach allows production servers to be flattened in parallel with the mitigation activities happening inside of the isolated Clean Room mitigation environment. The mitigation environment is configured to mimic the structure of the production environment using configurations stored in the digital jump bag.

Systems can be tested once the threats discovered in the investigation stage are mitigated through recovery and cleaning or rebuilding to a trusted state. This can take the form of functional testing and/or performance testing to ensure that the remediation, patching and bolstering of controls have not impacted the system's ability to deliver.

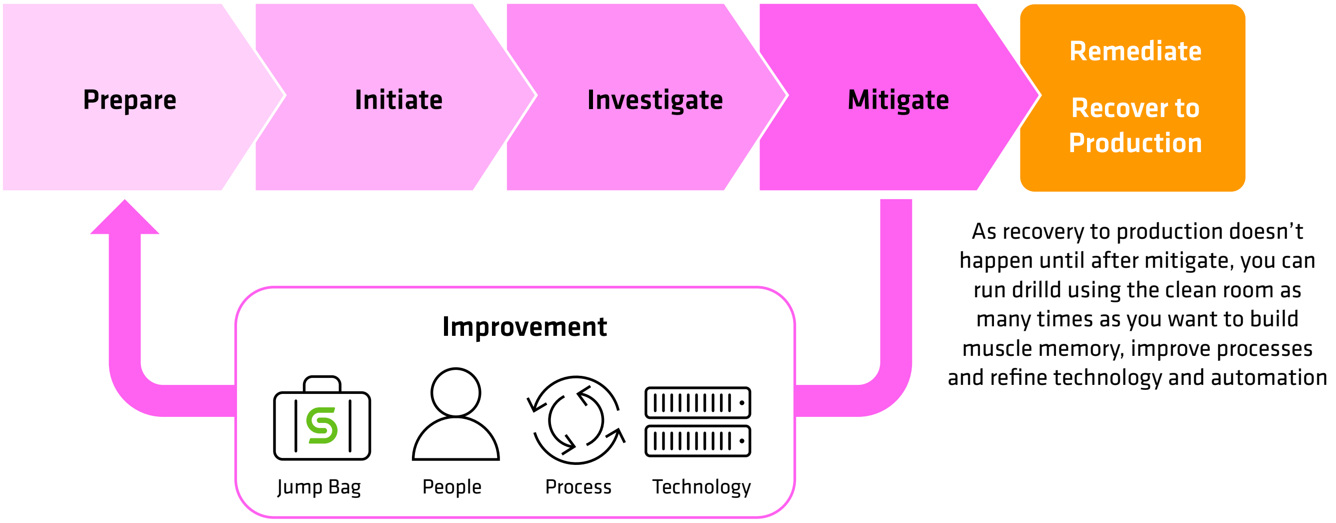
Finally, a snapshot of these systems is taken for two purposes:

1. If any attack artifact is missed, you do not need to return to square one. The snapshot taken after remediation will serve as the new baseline for investigation and further remediation and will be passed on to the investigation stage.
2. As the mitigation environment was configured to look like production, this snapshot can simply be "lifted and shifted" onto the production network.

Lessons learned

Any organization looking to establish cyber resilience should follow a mantra of continual improvement. Understanding what worked, what didn't, and what could be improved is critical to ensuring the organization doesn't suffer continued downtime and can handle future incidents more effectively and efficiently. As the adage says, "No plan survives contact with the enemy." Simulating real-world attacks is important to test technical recovery, and drive process improvement, identify opportunities for automation, and build muscle memory in your analysts and incident responders.

One of the greatest advantages of the Cohesity Clean Room solution is that it allows organizations to simulate an entire incident end-to-end without impacting production systems. DataProtect allows the cloning of production systems, which can then be attacked by an internal red team or external penetration testing company to simulate an end-to-end ransomware or wiper attack. The entire response and recovery workflow can be undertaken right up to immediately after taking the baseline snapshot of the remediated systems. This offers organizations a real-world scenario that ensures the right people, skills, processes, and supporting technology are in place to minimize the impact of a destructive cyberattack when the inevitable happens and the organization becomes a victim.

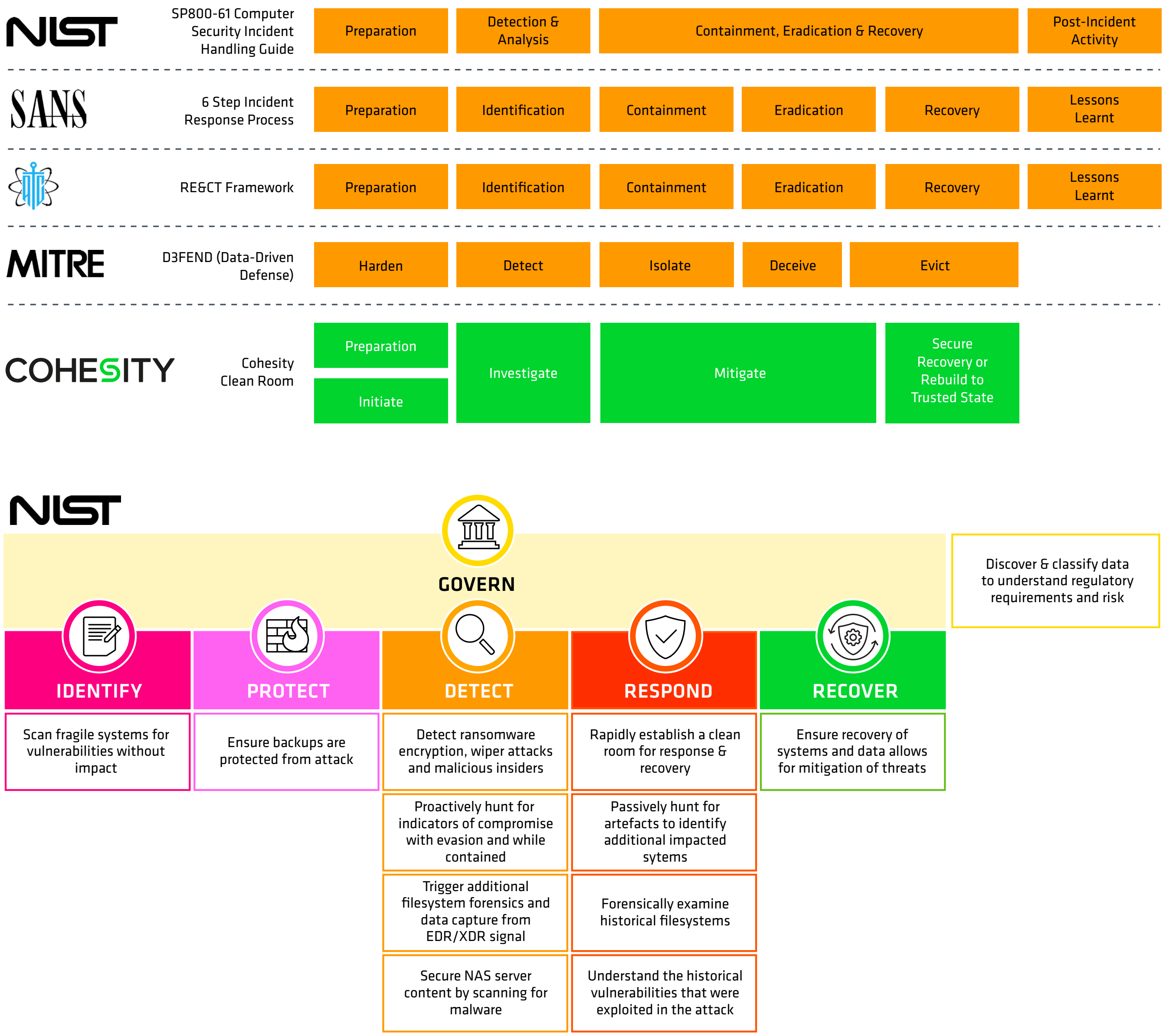


As recovery to production doesn't happen until after mitigate, you can run drilld using the clean room as many times as you want to build muscle memory, improve processes and refine technology and automation

Figure 6. The Cohesity Clean Room solution allows for continual improvement through realistic drills.

Summary

Cohesity can add tremendous value in recovery and make digital forensics and incident response stages of wartime both effective and efficient. Our unique approach to cyber resilience reduces the time it takes to achieve secure recovery and helps organizations be confident that a similar attack will not cause further downtime.



NIST	SP800-61 Computer Security Incident Handling Guide	Preparation	Detection & Analysis	Containment, Eradication & Recovery			Post-Incident Activity
SANS	6 Step Incident Response Process	Preparation	Identification	Containment	Eradication	Recovery	Lessons Learnt
	RE&CT Framework	Preparation	Identification	Containment	Eradication	Recovery	Lessons Learnt
MITRE	D3FEND (Data-Driven Defense)	Harden	Detect	Isolate	Deceive	Evict	
COHESITY	Cohesity Clean Room	Preparation Initiate	Investigate	Mitigate		Secure Recovery or Rebuild to Trusted State	

NIST

GOVERN: Discover & classify data to understand regulatory requirements and risk

IDENTIFY	PROTECT	DETECT	RESPOND	RECOVER
Scan fragile systems for vulnerabilities without impact	Ensure backups are protected from attack	Detect ransomware encryption, wiper attacks and malicious insiders	Rapidly establish a clean room for response & recovery	Ensure recovery of systems and data allows for mitigation of threats
		Proactively hunt for indicators of compromise with evasion and while contained	Passively hunt for artefacts to identify additional impacted sytems	
		Trigger additional filesystem forensics and data capture from EDR/XDR signal	Forensically examine historical filesystems	
		Secure NAS server content by scanning for malware	Understand the historical vulnerabilities that were exploited in the attack	

Figure 7. Achieving cyber incident response and NIST Cybersecurity Framework best practices with Cohesity

About Cohesity

Cohesity is the leader in AI-powered data security. Over 13,600 enterprise customers, including over 85 of the Fortune 100 and nearly 70% of the Global 500, rely on Cohesity to strengthen their resilience while providing Gen AI insights into their vast amounts of data. Formed from the combination of Cohesity with Veritas' enterprise data protection business, the company's solutions secure and protect data on-premises, in the cloud, and at the edge. Backed by NVIDIA, IBM, HPE, Cisco, AWS, Google Cloud, and others, Cohesity is headquartered in Santa Clara, CA, with offices around the globe. To learn more, follow Cohesity on **LinkedIn**, **X**, and **Facebook**.

Recommended reading

We think you'll find the following white papers, guides, and blogs helpful.

- Improve cyber resilience with a digital jump bag™
- Building cyber resilience in a world of destructive cyberattacks
- Introducing the Cohesity clean room design
- A field guide for AI-powered data security: How to deliver breakthrough business outcomes
- An executive's guide to modern data security and management
- Modern data security and management topologies: A guide for IT leaders

Learn more at Cohesity

Cohesity, the Cohesity logo, SnapTree, SpanFS, DataPlatform, DataProtect, Helios, and other Cohesity marks are trademarks or registered trademarks of Cohesity, Inc. in the US and/or internationally. Other company and product names may be trademarks of the respective companies with which they are associated. This material (a) is intended to provide you information about Cohesity and our business and products; (b) was believed to be true and accurate at the time it was written, but is subject to change without notice; and (c) is provided on an "AS IS" basis. Cohesity disclaims all express or implied conditions, representations, warranties of any kind.

COHESITY

cohesity.com
1-855-926-4374
2625 Augustine Drive, Santa Clara, CA 95054

2000058-002-EN 4-2025