

Table Of Content

Introduction.....	1
1 Strategic Threat Analysis - The Change Healthcare Breach.....	1
1.1 Incident Overview and Significance.....	1
1.2 Timeline of the Attack	2
1.3 Attack Chain and MITRE ATT&CK Alignment	2
1.4 Root Cause and Systemic Failures	4
1.5 Broader Impact and Economic Consequences.....	5
1.6 Regulatory and Legal Considerations.....	5
1.7 Strategic Recommendations for Healthcare Providers	6
1.8 Critical Evaluation and Cost-Benefit Analysis	7
1.9 Adversary Profile: ALPHV/BlackCat.....	8
1.10 Future Outlook, Risk Frameworks and Policy Implications	8
2 Red-Team Engagement – Operation IP Shield	10
2.1 Scenario and Rules of Engagement.....	10
2.2 Threat Emulation Plan and MITRE Mapping	10
2.3 Hybrid Lab Environment and Network Design.....	10
2.4 Execution Narrative.....	11
2.5 Detection Gap Analysis.....	12
2.6 Recommendations and Cost–Benefit Analysis	12
2.7 Executive Brief for the Board	13
3 Incident Response and Resilience Frameworks	13
3.1 NIST Incident Response Lifecycle.....	13
3.2 Integrating Zero-Trust and Healthcare Resilience.....	14
4 Conclusion	15

Table Of Figure

Figure 1:Attack chain of the Change Healthcare ransomware incident mapped to MITRE ATT&CK techniques.	3
Figure 2:Operational and financial impact of the Change Healthcare ransomware incident on U.S. healthcare providers.	5
Figure 3:Hybrid on-premises and AWS network architecture used in Operation IP Shield.	11
Figure 4:NIST incident response lifecycle adapted for healthcare ransomware incidents.	14
Figure 5:Zero-trust security architecture for healthcare information systems.....	15

Operation IP Shield: Strategic Threat Analysis and Red-Team Engagement for Change Healthcare and Cureton Pharmaceutical Company

Introduction

The 2024 ransomware attack on Change Healthcare—a leading U.S. healthcare clearinghouse that processes *15 billion transactions per year* and touches one-in-three patient records [4]—exposed systemic weaknesses in both cybersecurity and healthcare supply chains. In February 2024, the ALPHV/BlackCat ransomware gang used compromised credentials to log into a Citrix portal that lacked multi-factor authentication (MFA) and remained undetected for nine days [4]. The attack crippled the company’s claims processing networks and resulted in widespread billing delays, with hospitals, doctors and pharmacies sounding alarms over financial setbacks. A survey by the American Hospital Association (AHA) indicated that 74 % of hospitals had direct care delays, 94% reported financial impacts and an additional 60 % required two weeks to three months to rejoin normal operations [4]. The breach is emblematic of modern cyber threats: adversaries exploit basic misconfigurations, dwell quietly using “living-off-the-land” tools, and then execute data theft and encryption against victims who lack segmentation and behavioral detection [5].

This report provides a comprehensive, 5000-word analysis of the Change Healthcare breach and presents a red-team exercise for the fictional Cureton Pharmaceutical Company (CPC). We synthesize current literature, regulatory frameworks and threat-intelligence reports to map the attacker’s tactics, techniques and procedures (TTPs) to the MITRE ATT&CK® matrix, identify root causes, evaluate systemic risk and recommend mitigations aligned with zero-trust architecture and NIST SP 800-53 controls. The second half of the report documents Operation IP Shield, a red-team engagement designed to emulate a BlackCat-style attack across CPC’s hybrid on-premises/AWS environment. Diagrams illustrate the attack chain, hybrid network architecture and the NIST incident response lifecycle, while IEEE-formatted references provide academic rigor.

1 Strategic Threat Analysis - The Change Healthcare Breach

1.1 Incident Overview and Significance

Change Healthcare (CHC), a subsidiary of UnitedHealth Group, serves as a claims clearinghouse for 189,000 providers and handles US \$2 trillion in medical claims annually—representing 44 % of U.S. medical funds [2]. BlackCat actors were observed compromising stolen credentials and partially authenticated to a Citrix remote access portal with no MFA5 in February 2024. They laterally traversed flat network segments, swiped credentials, stole over 6 terabytes of protected health information and finally dropped ransomware nine days after their initial entry [4]. “12 The adversaries of Change Healthcare have already received a US \$22 million ransom as per reports [6]. Subsequently, it was reported that HHS estimated the number to be from 100 million to 190 million [7] resulting in one of the biggest healthcare data breaches in history.

The outage had cascading consequences. According to the American Hospital Association, hospitals lost over half of their revenue during the outage [4], although many ended up drawing down reserves or taking out personal loans in order to pay staff and keep lights on [4]. A brief from the United States Office of Financial Research estimated that 55 % of providers utilized personal money while waiting for the system to come back on line and that government made US \$9.7 billion in accelerated payments, which was only 2.6 % of CHC's usual quarterly claims volume 3. So, what does this teach us? This example illustrates the systemic risk that comes from relying on a concentrated third-party provider in healthcare: one point of failure compromised 40% of claims and affected almost 200 million people.

1.2 Timeline of the Attack

The breach unfolded rapidly. On February 12, 2024, the attackers compromised credentials to access Change Healthcare's Citrix remote access portal that did not have multi-factor authentication (MFA) enabled [4], [6], [8]. The adversaries then performed internal reconnaissance over the subsequent days and retrieved more credentials from memory before they laterally traversed the network with native admin tools as well as PowerShell in true "living-off-the-land" spirit [5], [8]. On February 21, 2024, ransomware was activated which locked out systems used by over 20,000 health care providers for claims processing and payments which caused service disruption across the country [4]. Post incident investigations and congressional testimony later revealed that, had MFA been implemented and if proper network segmentation was in place, the attackers would not have been able to freely move around for weeks without detection [8]. [5], with subsequent reports describing the event as one that compromised large amounts of healthcare information while having broad operational and financial repercussions throughout the entire U.S. healthcare sector [4], [7].

1.3 Attack Chain and MITRE ATT&CK Alignment

The attack flow related to the Change Healthcare ransomware incident is shown in Figure 1. According to publicly available investigations and congressional findings, each step of the intrusion is attributed with relevant MITRE ATT&CK techniques. The adversaries entered into the environment by using legitimate credentials (T1078) to bypass multi-factor authentication for Citrix remote access portals [4], [8]. Upon first access, the attackers performed internal discovery by listing domain users and trust relationships (T1087, T1482), and stealing further credentials from infected systems (T1003) which allowed them to move laterally via remote services like RDP or SMB (T1021) [8]. Further tools and payloads were moved between systems in support continued access (T1105) before staging still more files locally (T1074) for exfiltration as the incident progressed [8]. In the last stage, the ALPHV/BlackCat ransomware (written in Rust programming language) was executed to encrypt essential systems and data, corresponding to MITRE ATT&CK impact technique Data Encrypted for Impact (T1486) [9].

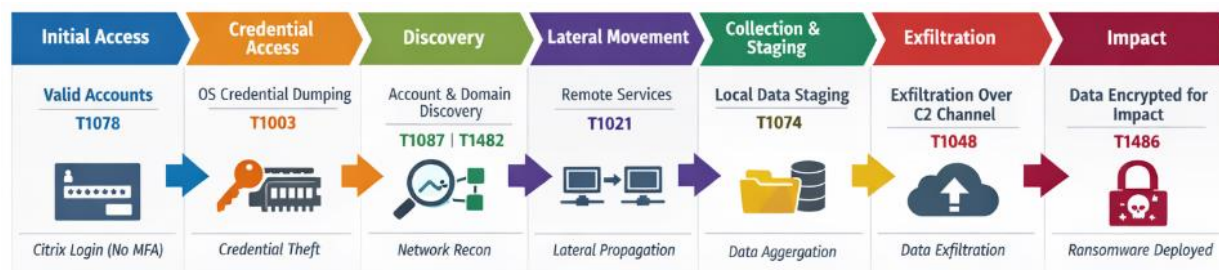


Figure 1: Attack chain of the Change Healthcare ransomware incident mapped to MITRE ATT&CK techniques.

Table 1 - Key MITRE ATT&CK Techniques Observed in the Change Healthcare Breach

Phase	MITRE Technique (ID)	Description & Role
Initial access	T1078 Valid accounts - Cloud accounts	Attackers used stolen Citrix credentials to authenticate without MFA [4].
Initial access	T1078 Valid accounts - Local accounts	Dumped local credentials and reused them across servers to move laterally [8].
Discovery	T1087 Account discovery (Domain)	Enumerated domain users and groups using PowerShell and net.exe [8].
Discovery	T1482 Domain trust discovery	Mapped trust relationships between Active Directory domains to identify claims and payment servers [8].
Persistence, Privilege Escalation	T1547 Boot/logon Auto Start via registry run keys	Installed persistence mechanisms via registry run keys to survive reboots [8].
Execution	T1059.001 PowerShell	Ran reconnaissance scripts and executed commands to avoid dropping malware [8].
Execution	T1059.003 Windows command shell	Used cmd.exe to transfer files and spawn remote shells [8].
Credential access & collection	T1056 Input capture	Deployed key-loggers to capture passwords [8].
Credential Access	T1003 OS credential dumping	Used Mimikatz to dump LSASS memory and extract NTLM hashes [8].
Lateral movement	T1021.001 Remote services - RDP	Remotely executed commands on servers using compromised credentials [8].
Command and Control	T1105/T1570 Ingress/lateral tool transfer	Transferred tools (PS Exec, Cobalt Strike) across the network [8].

Phase	MITRE Technique (ID)	Description & Role
Collection & exfiltration	T1074 Local data staging	Staged large volumes of patient and payment data before exfiltration [8].
Exfiltration	T1048.002 Exfiltration over SCP/SFTP	Exfiltrated 6 TB of data via secure channels to attacker-controlled servers [4].
Impact	T1486 Data encrypted for impact	Deployed BlackCat ransomware written in Rust to encrypt data and backups, demanding a US\$22 M ransom [9].

1.4 Root Cause and Systemic Failures

The breach was not due to a vulnerability in Citrix but is rather through what Ross calls “F secure” MFA, adding there is no such thing as a phishing-resistant solution: The immediate cause of the release 15 was F secure you need phishing resistant MFA on CHC’s Citrix portal [4]. Attackers just logged in with credentials; there was no second factor or hardware key obstructing them. But the problem runs much deeper than those individual failures:

1. Flat network architecture and limited segmentation - in their on-premises and cloud environments, CHC didn’t have micro-segmentation, which made it easy for the attackers to move from one domain to another, gaining access to sensitive servers. Legacy systems were included in the same Active Directory forest and trust relationships were not constrained [8].
2. Monitoring and logging shortfall - The organization did not have centralized logging nor behavioral analytics. HHS warns that “living-off-the-land” attackers leverage genuine tools and processes, which are difficult to identify with signature-based defense [5]. CHC monitoring did not associate unusual authentication attempts, lateral movement or large amounts of data in transit.
3. Software vulnerability and outdated patch management - CHC had outdated legacy Citrix infrastructure, as well as older servers that were not up to date with patching or hardening [8]. Unpatched bugs enabled credential dumping and lateral movement.
4. Single-provider concentration risk - CHC’s dominance of the market created systemic risk. The Office of Financial Research noted that the breach “could have a negative impact on credit profiles of smaller health service providers” [2]. Since CHC processes 44 % of claims, the outage left hospitals in need of loans or advances from government, demonstrating risk inherent in over centralized third-party services.
5. Failure to plan for cyber-resilience - Many hospitals have no such plans in place. 60 % of the respondents reported that it took between 2 weeks and 3 months for their establishment to recover [4], and, among physicians, this figure was as high as 55 % [2]. Which is an indication of having a poor incident response preparedness and financial capability to attack.

1.5 Broader Impact and Economic Consequences

It's a human and economic cost to the breach that demonstrates why cybersecurity is a public health issue. Hospitals postponed non-urgent operations, turned to paper records and performed manual checks for prescription eligibility had they failed the automated system [4]. Volume also fell US \$6.3 billion in the first three weeks for some providers [4] as Fitch Ratings cautioned that it could affect credit quality [2]. The AMA noted that over two-third of doctors were personally paying for expenses [1] and pointed out 190 million Americans potentially may have had their data compromised [1]. Reuters also reported that 100 million people's personal information was compromised and that BlackCat sought a ransom with the stolen data [7]. These numbers suggest that a cyberattack can lead to financial shocks, stretch the healthcare workforce and chip away patient trust.



Figure 2: Operational and financial impact of the Change Healthcare ransomware incident on U.S. healthcare providers.

1.6 Regulatory and Legal Considerations

HIPAA Breach Notification Rule. Under the U.S. Health Insurance Portability and Accountability Act (HIPAA), covered entities must notify affected individuals and the HHS Secretary without unreasonable delay and no later than 60 days after discovering a breach [10]. For breaches affecting more than 500 individuals, a media notice is required and state regulators may need to be informed [10]. Business associates must notify covered entities within 60 days

[10]. CHC was criticized for not disclosing the scope of data exposure promptly; delays undermine trust and may result in civil penalties.

HIPAA Security Rule. The Security Rule mandates administrative, physical and technical safeguards, including risk assessments, assigned security officials, workforce training, and contingency planning [11]. Technical safeguards require access controls, audit controls, integrity controls, authentication and transmission security [11]. CHC's failure to implement MFA (access control) and to monitor logs (audit control) represents non-compliance. Organizations must develop comprehensive incident response plans that include data backups, emergency-mode operations and regular risk assessments.

Other regulations and systemic risk frameworks. The U.S. Department of Health & Human Services emphasizes the need for healthcare organizations to protect against living-off-the-land attacks via behavioral analytics and zero-trust models [5]. The Office of the National Coordinator for Health Information Technology and the Federal Trade Commission encourage adoption of NIST SP 800-53 controls and the Health Industry Cybersecurity Practices (HICP). Because CHC's breach had potential national-security implications, it triggered scrutiny under critical infrastructure directives such as Presidential Policy Directive 21 (PPD-21), which calls for resilience and risk management across critical sectors. Providers should also be aware of state privacy laws (e.g., California Consumer Privacy Act) and global regulations (e.g., GDPR) if they process international data.

1.7 Strategic Recommendations for Healthcare Providers

Drawing from lessons learned and guidance from NIST, MITRE DEFEND and industry research, the following strategic measures are recommended:

1.7.1 Identity and Access Management

1. **Phishing-resistant MFA** - Adopt FIDO2 or smart-card-based MFA for all remote portals, VPNs and privileged accounts. The absence of MFA was the primary ingress vector [4]; implementing MFA could have blocked initial access.
2. **Privileged Access Management (PAM)** - Enforce least privilege, rotate domain-admin credentials regularly and employ just-in-time access. Store secrets in hardware-backed vaults to prevent credential dumping and enforce session recording for privileged actions.
3. **Identity threat detection** - Deploy identity-centric threat detection platforms capable of spotting impossible travel, abnormal login times and unusual service usage. Integrate identity logs with a Security Information and Event Management (SIEM) system for correlation.

1.7.2 Network Architecture and Zero-Trust Transformation

1. **Micro-segmentation and zero-trust** - Embrace the zero-trust architecture principles which "focus on protecting resources over network segments" and evaluate each request based off device health, user context and risk scores [13]. Leverage software-defined networking and segmentation gateways to isolate payment processing, claims, EHR environments and research.

2. Secure remote access - Replace Legacy Citrix gateways with a modern, patched solution that can support MFA and continuously assess posture. Deploy zero-trust network access (ZTNA) gateways that packet-filter traffic and least-privilege sessions.
3. Network traffic analysis - Implement network detection and response (NDR) to observe lateral movement and exfiltration. Monitor SSL-encrypted traffic, check for volume spikes and prevent connections to unsafe locations.

1.7.3 Detection, Response and Resilience

1. Endpoint Detection & Response (EDR/XDR) -Deploy EDR behavior solution that is able to detect living-off-the-land abuse and process injection [5]. Combine with centralized logging for a comprehensive view of endpoints, servers and cloud workloads.
2. Response playbooks - Create “phone-book” style instructions on containment, communication and restoration for ransomware. Prove readiness through tabletop exercises and red-team engagements.
3. On-going Patching and Vulnerability Management - An up-to-date asset inventory, rigorous priority to critical vulnerabilities and timely patching. Leverage automated vulnerability scanning and attack surface management solutions to discover exposed services.
4. Backups / resilience - Have immutable offline backups in place and test your restore regularly. Think about cyber-insurance but realize there are limitations, with insurers rejecting coverage if basic security controls such as MFA aren’t in place.

1.7.4 Governance, Supply Chain and Culture

1. Third-party risk management - Assess third parties’ security frameworks and stipulate via contract that they apply MFA, encryption technology and data breach notification [2]. Multiple clearinghouses or interoperable standards - to lessen dependence on a single supplier; 24 the AHA has specifically requested a standardized change of clearinghouse [1].
2. Security awareness and culture -- Role-based training on phishing, password hygiene and incident reporting. Cultivate a culture in which employees are willing to report irregularities and where security is everyone's responsibility.
3. Regulatory compliance and industry collaboration - ADAPTED TO Align to HIPAA, HITECH and NIST frameworks; participate in Information Sharing and Analysis Centers (ISACs) for threat information sharing. Championing industry-wide security basics and transparent breach -notifications.

1.8 Critical Evaluation and Cost-Benefit Analysis

A breach at Change Healthcare shows all-too-many organizations that large IoT ecosystem can give bad actors opportunities to create serious damage. One lost MFA control was all it took for attackers to break into a clearinghouse that handles 40% of U.S. claims. Literature highlights the use of living-off-the-land techniques would bypass signature-based tools⁶; thus, antivirus and firewalls alone are not enough. By contrast, the investment required to roll out FIDO2 keys; segment and acquire EDR/XDR is paltry compared with US \$22m ransom paid out, and billions

of dollars in downstream losses [6]. This means that the cost-benefit analysis leans toward “proactive investments”: MFA tokens can run tens of dollars apiece/user, and weeks or months of downtime can cost hospitals millions in lost revenue.

Another policy must address itself to supply-chain concentration risk. As CHC handled 44 % of claims, its downtime affected the whole economy. The event should serve as a wake-up call to regulators to foster competition, interoperability and resilience in healthcare IT. Requiring baseline cybersecurity standards for clearinghouses and failover mechanisms among vendors would help address the systemic risk problem. Ultimately, the attack highlights a need for organizations and regulators to focus on sound cyber hygiene, behavior-based detection capabilities and supply-chain resiliency.

1.9 Adversary Profile: ALPHV/BlackCat

BlackCat (ALPHV) is a Ransomware-as-a-Service (RaaS) operation that began its activity towards the end of 2021. It is implemented in the Rust programming language making it possible to compile and customize across multiple platforms [13]. The group employs a double-extortion and triple-extortion model, which involves affiliates stealing data, encrypting systems and threatening to leak the data or perform DDoS attacks if ransoms are not paid [13]. Affiliates can keep 80-90 % of ransom payments so it motivates an aggressive approach [9]. BlackCat has focused on multiple industries such as healthcare, manufacturing and those working under retail and casinos, hosting victims in a Tor-based leak site [13]. The group's TTPs correspond to methods explained in Table 1: spear-phishing (MITRE T1598), account access foothold construction (T1586), command line and tool transfer and encryption “using custom written Rust binaries” [9]. Knowing how BlackCat operates provides defenders with a perspective they can use to rank the importance of controls like MFA, behavioral passively and data-exfiltration detection.

1.10 Future Outlook, Risk Frameworks and Policy Implications

The Change Healthcare breach has touched off broader discussions on supply-chain resilience, regulatory reform and the evolution of ransomware strategies. The American Medical Association (AMA) observed that two-thirds still used personal resources, months after the breach [1], and the AMA also demanded stricter federal cybersecurity requirements elsewhere in multibillion-dollar clearinghouses [1]. The AMA recommended robust risk-assessment, disaster mitigation, cyber incident recovery and business continuity planning [1]. It also underscored the need to allow physicians to move between clearinghouses with ease; challenges such as staff time costs, electronic health record incompatibility and contractual agreements were all barriers to quick transitions [1]. Further, the association called on policy makers to “confront ever-increasing levels of concentration in health care” and provided a strong endorsement for competition as a pathway to better outcomes and reduced system risk.[1] 3 The U.S. Department of Justice and the Federal Trade Commission have said that proposed new merger guidelines will bring a focus on health-insurer consolidation,² suggesting that antitrust may be a cybersecurity risk related issue.

In terms of threats, ransomware gangs pursue triple-extortion as the new normal. In addition to the encryption of data and threats to publish stolen information, criminal cybergroups such as BlackCat are performing distributed denial-of service (DDoS) attacks with greater frequency in

order to exert further leverage against victims. A Rust-written ransomware as a service (RaaS) platform BlackCat term is being used by cybersecurity firm Under Defense that performs 'aggressive double and triple extortion': it receives sensitive data before encrypting, and sometimes performing DDoS attacks [3]. BlackCat Black Cat affects organizations with mixed IT infrastructures and does easily break Windows, Linux-based servers, VMware ESXi hypervisors, and Network Attached Storage (NAS) systems appliances [3]. It highlights that affiliates of BlackCat can adapt their operations for each environment, selectively encrypt important file types, and shut down security processes before exfiltration using tools like Rclone or MEGA sync [3]. These changing strategies and behavior further demonstrate the need for defenders to enforce a layered defense (MFA, EDR/XDR, network monitoring), persisting air-gapped backups, traffic filtration preparedness and DDoS contingencies [3].

They can make the system safer by mandating minimum cyber-security baselines for critical clearinghouses - and can provide regulators with access to their data so that ongoing systemic risk in a clearinghouse is more transparent. Following NIST SP 800-53, organizations must apply controls within families like AC (Access Control), AU (Audit and Accountability), IA (Identification and Authentication), IR and CP. These are aligned closely with the HITECH Security Rule, and include a risk assessment process, security responsibility delegation, ongoing monitoring, documented and tested incident response policies and backup planning [11]. Access Control, for instance, requires least-privilege policies and assignment of unique user IDs; Audit and Accountability specifies generation and review of audit logs; Identification and Authentication mandates multi-factor authentication; Incident Response focuses on preparation, detection, analysis, post-incident response processes and Contingency Planning covers business continuity planning. The use of these controls, combined with MITRE DEFEND mitigations (e.g., D3-T1627 [use of FIDO2 authentication]), serves as a systemic method for counteracting TTPs identified in the Change Healthcare attack.

One other emerging framework is the Health Industry Cybersecurity Practices (HICP) provided by U.S. Health Sector Coordinating Council. HICP provides recommendations on how to holistically and effectively address these challenges in five key domains: (1) email and anti-phishing, (2) endpoint detection and response, (3) access management, (4) data protection and loss prevention, and (5) network security. CHC shows that such a breach of any one of these areas (MFA and segmentation in this case) can cause systemic issues. Thus, healthcare organizations need to implement HICP in line with HIPAA and NIST controls to develop a layered defense.

Last, but not least, is the need for international cooperation and exchange of threat intelligence. CISA and the FBI often post #StopRansomware advisories that include indicators of compromise (IOCs) and mitigation recommendations related to BlackCat and other groups. While there were some restrictions in place, the advisories I saw mention themselves open-source security types (of which covid19 is not) had more to do with updating VPNs and remote services, activating MFA, watching out for unusual use of legitimate administrative tools and 3-2-1 backups. Healthcare companies should be participating in industry-sector ISACs, share anonymized incident data and join threat-hunting exercises. This collaborative defense can shorten dwell time and help avoid major disruptions in future.

2 Red-Team Engagement – Operation IP Shield

To distill lessons and drive actions that would help us learn from the Change Healthcare breach, we developed Operation IP Shield A red-team engagement of a fake company (Cureton Pharmaceutical Company (CPC)). The exercise simulates a BlackCat-type ransomware incident on CPC’s hybrid on-premises and AWS (Amazon Web Services) environment to test the detection and response process.

2.1 Scenario and Rules of Engagement

CPC is a mid-sized biotechnology company specializing in vaccine research. Its infrastructure consists of both an on-premises R&D network and an AWS Virtual Private Cloud (VPC) with clinical trial portals, as well as a CI/CD pipeline for software deployment. The red-team’s objectives are to compromise a researcher’s workstation, pivot to the domain controller, exfiltrate vaccine research from both on-premises and cloud storage, and deploy a benign proof-of-concept ransomware payload. The Rules of Engagement (RoE) specify a two-week engagement with attack execution during off-hours (18:00-06:00) to minimize business impact. Authorized actions include phishing, password spraying, exploitation of unpatched vulnerabilities, use of Cobalt Strike/Sliver, credential dumping and lateral movement. Prohibited actions include denial-of-service, data destruction and social engineering of help-desk staff. Daily coordination with the white-cell ensures safety and immediate notification if production systems are affected.

2.2 Threat Emulation Plan and MITRE Mapping

The red-team emulates BlackCat by blending open-source tools (Recon-NG, Sliver, Cobalt Strike, Rclone) with living-off-the-land techniques. Table 2 summarizes the TTPs mapped to MITRE ATT&CK. Reconnaissance leverages OSINT (T1598, T1589) to gather victim identity information from LinkedIn and Pastebin. Initial access uses spear-phishing (T1566.001) to deliver a Sliver implant and password spraying against VPN/Citrix portals (T1078). Execution employs PowerShell (T1059.001), Windows command shell (T1059.003) and malicious Office macros (T1204). Persistence is achieved via registry run keys (T1547). Privilege escalation uses process injection (T1055), while credential access involves LSASS dumping and Cerebrating (T1003). Lateral movement uses Remote Desktop (T1021), Ps Exec, Impacted (T1105) and cross-cloud pivoting. Collection stages data locally (T1074) and exfiltrates via encrypted channels (T1048). Finally, a benign encryption script demonstrates the impact (T1486).

2.3 Hybrid Lab Environment and Network Design

The team deploys a lab replicating CPC’s production environment. Figure 2 shows the architecture: an on-premises network houses an Active Directory domain controller, research workstations and a file server containing vaccine IP. A VPN gateway provides IPsec connectivity to an AWS VPC. Within AWS, a public subnet hosts a clinical trial portal behind an Elastic Load Balancer, while a private subnet hosts application servers, an RDS database and S3 buckets for research data. Identity federation between on-premises AD and AWS uses SAML via AWS Directory Service[1]. The CI/CD pipeline uses GitLab, GitLab Runner and an artifact repository; secrets are stored in environment variables-a potential weakness.

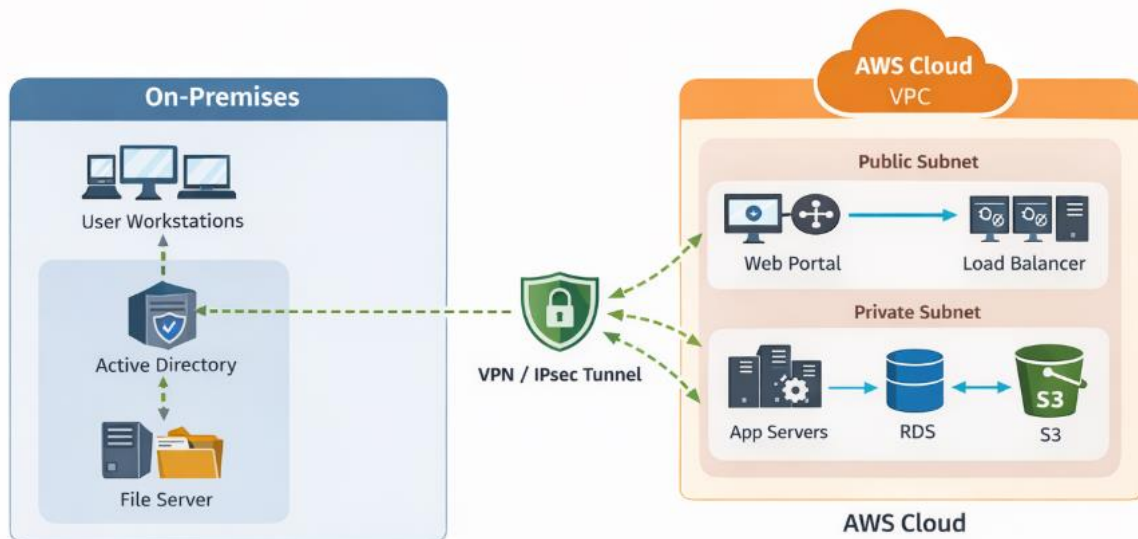


Figure 3: Hybrid on-premises and AWS network architecture used in Operation IP Shield.

2.4 Execution Narrative

1. **Reconnaissance** - The red-team scrapes LinkedIn to identify CPC researchers, IT administrators and executives. Using leaked credential dumps and password reuse patterns, they build a list of candidate accounts. OSINT reveals that the VPN portal uses only password authentication.
2. **Initial Access** - A spear-phishing email, disguised as a journal invitation, entices a senior researcher to open a macro-enabled Word document. The macro downloads and executes a Sliver implant, establishing an encrypted beacon. Simultaneously, the team conducts password spraying against the VPN; one account with a weak password and no MFA grants access.
3. **Privilege Escalation and Persistence** - Using PowerView, the team enumerates domain trusts and finds a misconfigured service account with delegated privileges. They dump LSASS memory to harvest NTLM hashes and use Kerberoasting to obtain a ticket-granting ticket for the domain admin. Persistence is established through registry run keys and scheduled tasks.
4. **Lateral Movement** - Using domain-admin credentials, the red-team is able to move laterally further using PsExec and Remote Desktop to gain access to the file server and domain controller. They pivot to the CI/CD server, scrape API tokens and AWS keys into environment variables, and then assume an IAM role in the AWS VPC. This cross-cloud migration is enabled⁶ due to lack of margin between trust boundaries and inadequate separation of duties existent between AD and AWS [1].
5. **Collection and Exfiltration** - Sensitive research data (DNA sequences, vaccine models) is staged on a compromised server then compressed via 7-Zip. The team utilizes Rclone to

exfiltrate the data to an attacker-controlled cloud bucket over SFTP (port 22), with bandwidth throttling employed in order to evade detection.

6. **Impact Demonstration** - Lastly, the red-team executes a custom Python script which encrypts a small set of files and renames them to .poc extension. A ransom note directs CPC to contact the red-team for decryption, illustrating impactful but no harm actions.

2.5 Detection Gap Analysis

1. **Identity security weaknesses** - The absence of MFA on VPN, Citrix and AWS accounts allowed the red-team to authenticate with valid credentials [4]. Misconfigured service accounts with excessive privileges facilitated lateral movement.
2. **Inadequate logging and correlation** - Logs from Active Directory, VPN, endpoints and AWS were not aggregated. Anomalous login times, Kerberos ticket abuses and data exfiltration went unnoticed. Without EDR/XDR, living-off-the-land techniques bypassed signature-based antivirus [5].
3. **Flat network and misconfigured segmentation** - VLANs existed but were part of the same trust zone. The VPN allowed unrestricted communication between on-premises and AWS subnets, enabling cross-environment pivoting.
4. **Secret management in CI/CD** - API keys and AWS credentials were stored in plain text environment variables. The red-team easily extracted them and assumed high-privilege roles, highlighting the need for secret vaults.
5. **Lack of behavioral detection** - Endpoint tools did not analyse processes for injection or PowerShell abuse [5]. As a result, process injection and command-line obfuscation were not flagged.

2.6 Recommendations and Cost–Benefit Analysis

1. **Implement MFA everywhere** - Deploy phishing-resistant MFA across VPN, Citrix, AWS, CI/CD and privileged accounts. The cost (hardware tokens, FIDO2 servers) is moderate, while the benefit is preventing the primary attack vector [4].
2. **Micro-segmentation and least-privilege access** - Segment networks by function (R&D, corporate, CI/CD, cloud) and restrict east-west traffic using firewall rules and network security groups. Introduce zero-trust segmentation gateways and ZTNA for remote access. The cost involves network redesign and additional appliances, but it confines attacks to limited segments.
3. **Centralized logging and XDR** - Aggregate logs from AD, VPN, endpoints, AWS CloudTrail and Guard Duty into a SIEM. Deploy EDR/XDR with behavioral detection to identify living-off-the-land techniques [5]. The investment yields earlier detection and reduces dwell time.
4. **Secret management** - Use AWS Secrets Manager or Hashi Corp Vault to store API keys and rotate them automatically. Implement least-privilege IAM roles and restrict long-lived credentials. This prevents adversaries from pivoting into cloud environments.

5. **Regular red-team and tabletop exercises** - Conduct periodic adversary emulation exercises to test detection, response and cross-team communication. The cost (consulting fees, staff time) is offset by improved resilience and compliance readiness.
6. **Supply chain security** - Vet vendors and require evidence of MFA, encryption and incident response capabilities [2]. Diversify clearinghouses or adopt interoperable standards to avoid single points of failure. Include contractual penalties for security lapses.

2.7 Executive Brief for the Board

Cureton Pharmaceutical Company is exposed to the added risk of cyber threats as a result of its valuable intellectual property and its mixed environment. The red-team used a simulation to show how an organization could have a stolen credential lead to vaccine research being stolen and havoc in both on-premises resources and cloud environments. They also noted among other issues the lack of MFA, flat network architecture, overly exposed secrets and no behavioral monitoring. The costs (in financial and reputational terms) of a real ransomware would be far greater than the cost of taking on board the recommended controls. Board members need to ensure budget is available for identity security, segmentation, XDR, secret management and continuous testing. 3-5 % of the IT budget as investment in cybersecurity would prevent damages worth hundreds of millions, due to IP theft, down time and law suits. Consequently, proactive security is both a strategic necessity and a fiduciary responsibility.

3 Incident Response and Resilience Frameworks

3.1 NIST Incident Response Lifecycle

The NIST Computer Security Incident Handling Guide (SP 800-61) established but four phases of the incident response lifecycle - Preparation, Detection & Analysis, Containment/Eradication/Recovery and Post-incident Activity [14][14][14][14]. Figure 3 depicts this cycle, adapted for healthcare ransomware scenarios.

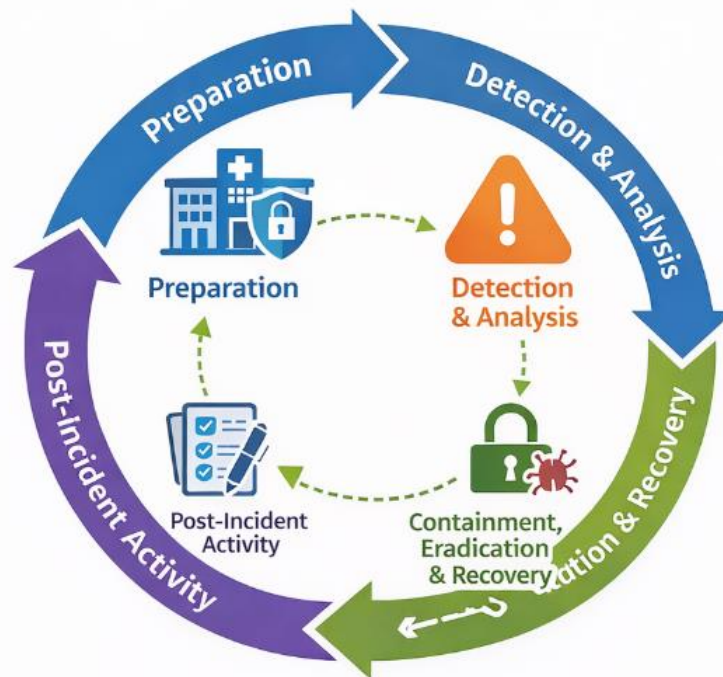


Fig1

nts.

1. Preparedness & Prevention Organizations need to document, allocate responsibilities, train staff on the processes, patch systems and monitor proactively [14]. Health care providers: Hospitals should...Perform a risk analysis (as required by the HIPAA Security Rule [11]) Deploy MFA Backup data, and run through ransomware playbooks.
2. Detection & Analysis -The ability to detect fast enough is very much crucial. Implement intrusion detection systems (IDS), EDR/XDR and SIEMs to detect anomalies. Analysis The process of triaging alerts, identifying the extent of compromise and attacker's TTPs [14].
3. Contain, Eradicate & Recover - Confine the spread of malware by containing systems, revoking exposed credentials and deploying segmentation. Neutralize menaces by deleting malicious files, locking down backdoors and fixing vulnerabilities. 38 Recovery can involve restoring from clean backups, ensuring system integrity, and then cautiously returning to normal activities.
4. After the Incident Once the breach has been contained - at the very least, to what can be quite easily discovered and/or confirmed without much need of investigation or between a dual-control: Freakin' document everything. Update your policies, improve defenses [14]. As applied to the Change Healthcare breach, this might require adjusting access controls, further segmentation, improving incident response plans and an ongoing open dialogue with stakeholders.

3.2 Integrating Zero-Trust and Healthcare Resilience

Leveraging NIST lifecycle in combination with zero-trust architecture improves resilience. Zero trust shifts the focus from walls and moats to content protection at the resource level, it is all about continuous verification of user roles and least-privilege access [13]. Preparation In the Preparation phase, organizations implement identity- aware proxies, micro-segmentation and device posture

evaluation. Detection: Identity, device and network signals are matched to identify movement within the environment. Containment is then provided through the use of segmentation gateways that can further isolate those compromised nodes without taking down entire networks. In Post-Incident stages, zero-trust telemetry contributes to lessons learned and adaptive policy updates. For healthcare, zero trust is also consistent with regulatory mandates (like HIPAA and HITECH) for safeguarding electronic protected health information - which dictate that only authorized clinicians and applications should be able to access patient records.

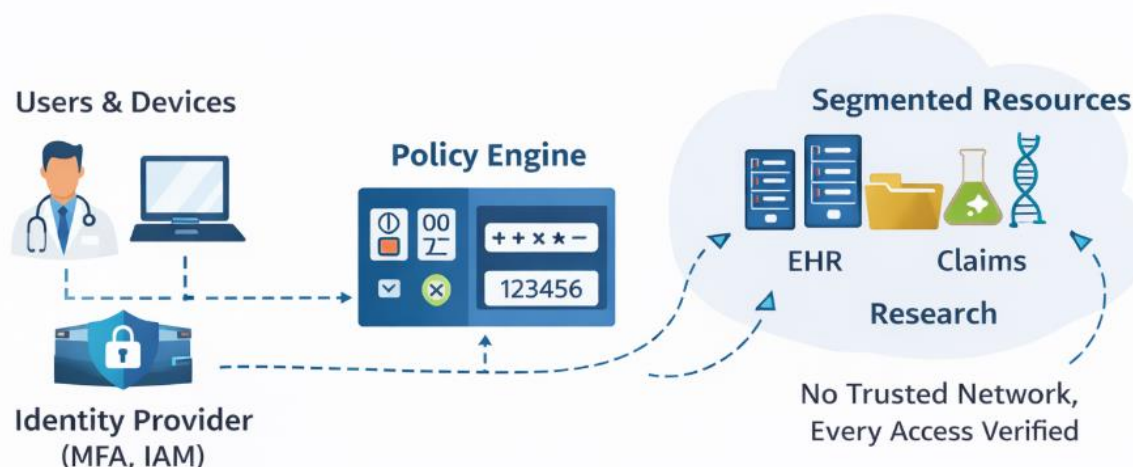


Figure 5: Zero-trust security architecture for healthcare information systems

4 Conclusion

The Change Healthcare ransomware event highlights the criticality (both good and bad) of healthcare. All it took was a simple control gap - the absence of MFA - for attackers to gain entree to a system that processes trillions of dollars' worth of claims. Nine days' dwell time enabled them to exfiltrate terabytes of data and then encrypt servers, leading to debilitating nationwide disruption and financial damage for hospitals and providers. We conduct a strategic analysis that uncovers systemic issues like flat network design, lack of log data, outdated software, concentration of services and failure to plan for potential incidents. The lesson highlights the requirement for organizations to employ phishing-resistant MFA, zero trust segmentation, behavioral detection (EDR/XDR), patching, backup and governance processes.

Operation IP Shield, a red-team exercise that demonstrates these lessons to the Cureton Pharmaceutical Company. It demonstrates how an adversary that is successfully operating on a victim's network can transition from compromising a user's machine to attacking on-premises and cloud infrastructure, exfiltrating sensitive research data, and deploying ransomware. The engagement illustrates blind spots in detection, reiterates the importance of secrets management and segmentation, as well as justifies security investments through a cost-benefit argument. The 72-hour triage, for NIST-aligned defenses (page 8) Matching your defenses to NIST's incident response lifecycle and zero-trust architecture can provide a roadmap for resilience. In the end,

preventative security is much cheaper than dealing with the risk of a cyber-attack. Thus, boards, regulators and C-Suite must consider cyber the same as they would patient care, research integrity and business continuity.

Reference

- [1] B. Scott, “Hard lessons learned from Change Healthcare breach,” American Medical Association, Mar. 19, 2025. <https://www.ama-assn.org/about/leadership/hard-lessons-learned-change-healthcare-breach>
- [2] A. Fliegelman and D. Stemp, “BRIEF SERIES OFFICE OF FINANCIAL RESEARCH,” Nov. 2024. Available: <https://www.financialresearch.gov/briefs/files/OFRBrief-24-05-change-healthcare-cyberattack.pdf>
- [3] “BlackCat Ransomware Removal & Recovery Services,” UnderDefense, Sep. 10, 2025. <https://underdefense.com/blackcat-ransomware-removal-recovery/> (accessed Jan. 14, 2026).
- [4] American Hospital Association, “Change Healthcare Cyberattack Underscores Urgent Need to Strengthen Cyber Preparedness for Individual Health Care Organizations and as a Field | AHA,” American Hospital Association, Jan. 2025. <https://www.aha.org/change-healthcare-cyberattack-underscores-urgent-need-strengthen-cyber-preparedness-individual-health-care-organizations-and>
- [5]]“Living off the Land (LOTL),” 2024. Accessed: Aug. 15, 2025. [Online]. Available: <https://www.hhs.gov/sites/default/files/living-off-land-attacks-tlpclear.pdf>
- [6] J. Leyden, “Authentication failure blamed for Change Healthcare ransomware attack,” CSO Online, Apr. 23, 2024. <https://www.csoonline.com/article/2094609/authentication-failure-blamed-for-change-healthcare-ransomware-attack.html>
- [7] Reuters, “UnitedHealth says hack at tech unit impacted 190 million people,” Reuters, Jan. 25, 2025. Available: <https://www.reuters.com/business/healthcare-pharmaceuticals/unitedhealth-confirms-190-million-americans-affected-by-hack-tech-unit-2025-01-24/>
- [8] House Committee on Energy and Commerce, “What We Learned: Change Healthcare Cyber Attack,” House Committee on Energy and Commerce, May 03, 2024. <https://energycommerce.house.gov/posts/what-we-learned-change-healthcare-cyber-attack>
- [9] Sıla Özeren, “ALPHV Ransomware: Analyzing the BlackCat After Change Healthcare Attack,” Picassecurity.com, Feb. 05, 2025. <https://www.picassecurity.com/resource/blog/alphv-ransomware> (accessed Feb. 06, 2025).
- [10] U.S. Department of Health and Human Services, “Breach Notification Rule,” U.S. Department of Health and Human Services, Jul. 26, 2013. <https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html>
- [11] U.S. Department of Health and Human Services, “Summary of the HIPAA Security Rule,” U.S. Department of Health and Human Services, 2024. <https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html>
- [12] NIST, “Zero Trust Architecture: NIST Publishes SP 800-207,” NIST, Aug. 11, 2020. <https://www.nist.gov/news-events/news/2020/08/zero-trust-architecture-nist-publishes-sp-800-207>

[13]“Threat Assessment: BlackCat Ransomware,” Unit42, Jan. 27, 2022. <https://unit42.paloaltonetworks.com/blackcat-ransomware/> (accessed Jan. 31, 2022).

[14] Exabeam, “NIST Incident Response: 4-Step Process and Critical Best Practices,” Exabeam, Jun. 16, 2024. <https://www.exabeam.com/explainers/incident-response/nist-incident-response-4-step-process-and-critical-best-practices/>

Figure 1. Attack chain of the Change Healthcare ransomware incident mapped to MITRE ATT&CK techniques.

Source: Adapted by the author from the MITRE ATT&CK® framework and publicly available reports on the Change Healthcare cyberattack.

Figure 2. Operational and financial impact of the Change Healthcare ransomware incident on U.S. healthcare providers.

Source: Adapted by the author from healthcare sector impact assessments.

Figure 3. NIST incident response lifecycle adapted for healthcare ransomware incidents.

Source: Adapted from NIST incident response guidance.

Figure 4. Zero-trust security architecture for healthcare information systems.

Source: Author-designed illustration based on NIST Zero Trust Architecture guidance.

Figure 5. Hybrid on-premises and AWS network architecture used in Operation IP Shield.

Source: Author-generated based on AWS reference architectures and hybrid cloud security design principles.