



Module: Ethical Hacking

Module Code: ACCA7033

Submitted to:

Dr. Carlene Campbell

Associate Professor

University of wales trinity saint david

Submitted By:

MD IMRAN BISWAS

Student ID: 2436882

University Of Wales Trinity Saint David

Submitted Date: 14-01-2026

Contents

Introduction.....	1
1. Strategic Analysis of the Change Healthcare Ransomware Attack.....	1
1.1 Incident Overview.....	2
1.2 MITRE ATT&CK Campaign Mapping.....	2
1.3 Root Cause Analysis.....	6
1.4 strategic recommendations for prevention and detection.....	7
2. Operation IP Shield: Simulating Real-World Attacks to Assess Risk.....	8
2.1 Engagement Overview and Scope.....	8
2.2 Rules of Engagement (RoE).....	8
2.3 Threat Emulation Plan.....	9
2.4 Virtual Lab Environment Design.....	12
2.5 Campaign Execution.....	13
2.6 Reporting and Analysis.....	14
2.6.1 Technical Report & Detection Gap Analysis.....	14
2.6.2 Executive Brief & Strategic Investment.....	16
Conclusion.....	19
Reference:.....	20

Figure 1: Strategic mapping of the ALPHV/BlackCat Ransomware-as-a-Service (RaaS) attack lifecycle. 5

Figure 2: diagram illustrating the root causes of the ALPHV compromise. 6

Figure 3: The proposed Zero Trust architecture, illustrating the use of an Identity Proxy and micro-segmentation to isolate critical assets and prevent unauthorized access 8

Figure 4: Network Topology of the Virtual Lab	14
Figure 5: Step-by-step breakdown of the Red Team methodology	16

Introduction

In the current era of cybersecurity, software vulnerabilities can no longer be checked and the organisations remain safe. It has shifted to the concept of "Adversary Emulation: the defenders are now forced to be able to think and behave just like the highly sophisticated attackers they are attempting to counter. This assignment will discuss these advanced concepts in two different yet related parts. First, it takes an in-depth analysis of a real-life strategic threat analysis, an intensive analysis of a recent advanced ransomware attack on the healthcare sector. Through mapping this attack to the industry-standard Mitchell ATT&CK framework, the report examines the underlying causes of the breach, including the failure in managing identities, and generalises strategic advice to avoid future occurrences of such disasters. After this analysis, the report shifts to practice through the case of an operation named IP Shield, which is a simulated Red Team operation ordered by Cureton Pharmaceutical Company (CPC). The goal in this case is to simulate an attacker of a nation-state against a complex hybrid network comprising of office computers, CI/CD pipelines, and AWS cloud systems. It is not only to crack in but to do so without being noticed with clandestine methods such as the Living-off-the-Land proving that even a secure network is not immune to attacks. In the end, this piece of work shows that technical hacking expertise should be integrated with strategic business planning in order to effectively safeguard the most valuable intellectual property of an organisation.

1. Strategic Analysis of the Change Healthcare Ransomware Attack

Technology is currently a part of the healthcare sector. Consequently, there has been an increase in the number and sophistication of cybersecurity attacks than ever in the sector. There are such high-profile instances as WannaCry that brought down a section of the National Health Service in the UK and the 2016 ransomware attack on a hospital in Hollywood Presbyterian Medical Center. But cyber threats have developed since 2017 (Tully et al., 2020). The change in this direction can be observed in the February 2024 ransomware attack on Change Healthcare at UnitedHealth Group. The report will therefore entail a strategic threat analysis of the Change Healthcare incident. It will map the campaign of the adversary to the MITRE ATT&CK(r) Enterprise Matrix, describe the major tactics followed by the attacker, comment on the root causes of the breach, namely the failures in identity governance, and generalize strategic

suggestions to improve the security of the organization against the similar Advanced Persistent Threats (APTs).

1.1 Incident Overview

Change Healthcare was attacked by the ALPHV group, also referred to as BlackCat. This organization follows a Ransomware-as-a-Service (RaaS) approach to complete the attack. Under this structure, the main developers create the malware, however, they contract other affiliate hackers to do the actual attacks on the companies. ALPHA has a reputation of having superior strategies. They were the initial large-scale organization to code in the Rust programming language their ransomware. It is a very big step since Rust enables its malware to execute on Windows and Linux. It is consequently extremely difficult that security tools detect or reverse engineer the malware.

Besides that, they apply the methods of Triple Extortion(Kanter et al., 2024). Triple extortion is a sophisticated technique that ransomware attackers resort to that is based on not only encrypting information but also threatening to disclose it and address third parties. This makes them not only encrypt the data to halt operations. They also steal sensitive patient records (PHI) to threaten a public release, and they can also institute Denial-of-Service (DoS) attacks to place additional strain on the victim to pay.

1.2 MITRE ATT&CK Campaign Mapping

MITRE ATT&CK is an open-source knowledge base of cyber adversary behaviour made available to users all over the world and founded on actual observations. The framework categorizes adversary behaviors into hierarchical order and explains different tactics, techniques, and procedures (TTPs) employed by cyber experts, including those that are involved in ransomware attacks. MITRE ATT&CK (Grigorescu et al., 2022) is a valuable tool when it comes to the context of ransomware to study and protect against attackers. It gives a stepwise method of determining the phases of a ransomware attack, including first access and extortion. It also assists the cybersecurity professionals in preventing and predicting such threats. The next section traces their exact steps to the MITRE ATT&CK(r) Enterprise Matrix to see how they constructed the system (Manocha et al., 2021).

Table 1: MITRE ATT&CK Mapping of ALPHV Campaign

Source: (Al-Sada et al., 2023)

Tactic	Technique ID	Technique Name	Details of Use in Change Healthcare Incident
Initial Access	T1078	Valid Accounts	The attackers did not break in using a virus. They used stolen login details (username and password) to log into the company's Citrix portal.
Initial Access	T1133	External Remote Services	They targeted a specific gateway (Citrix) that allowed remote employees to connect to the network. This portal did not have Multi-Factor Authentication (MFA) turned on.
Execution	T1059	Command and Scripting Interpreter	Once inside, the attackers used PowerShell , a built-in Windows tool, to run commands. Because PowerShell is a legitimate tool, it is harder for security systems to notice it is being used for hacking.
Defense Evasion	T1562	Impair Defenses	The ransomware was programmed to find and disable security tools. It specifically tried to turn off antivirus software and delete system logs to hide its tracks.

Credential Access	T1003	OS Credential Dumping	The attackers used tools (like Mimikatz) to steal more passwords from the computer's memory (LSASS process). This allowed them to access higher-level "Administrator" accounts
Lateral Movement	T1021	Remote Services	Using the stolen administrator passwords, the attackers moved from the initial Citrix server to other critical servers in the network using legitimate Windows features like RDP (Remote Desktop Protocol).
Discovery	T1083	File and Directory Discovery	Before locking the computers, the attackers searched through the network folders. They were looking specifically for sensitive medical records (PHI) and payment information to steal.
Impact	T1490	Inhibit System Recovery	The malware deleted "Volume Shadow Copies" (automatic Windows backups). This ensured that the victim could not simply restore their files without paying the ransom.
Exfiltration	T1048	Exfiltration Over Alternative Protocol	The group stole terabytes of data. They used specialized tools (like Rclone or MegaSync) to upload this sensitive data to

			their own cloud storage servers before encrypting the network.
Impact	T1486	Data Encrypted for Impact	Finally, they ran the BlackCat encryption program. This locked up critical databases and patient records, causing the massive outage that stopped pharmacies from processing prescriptions.

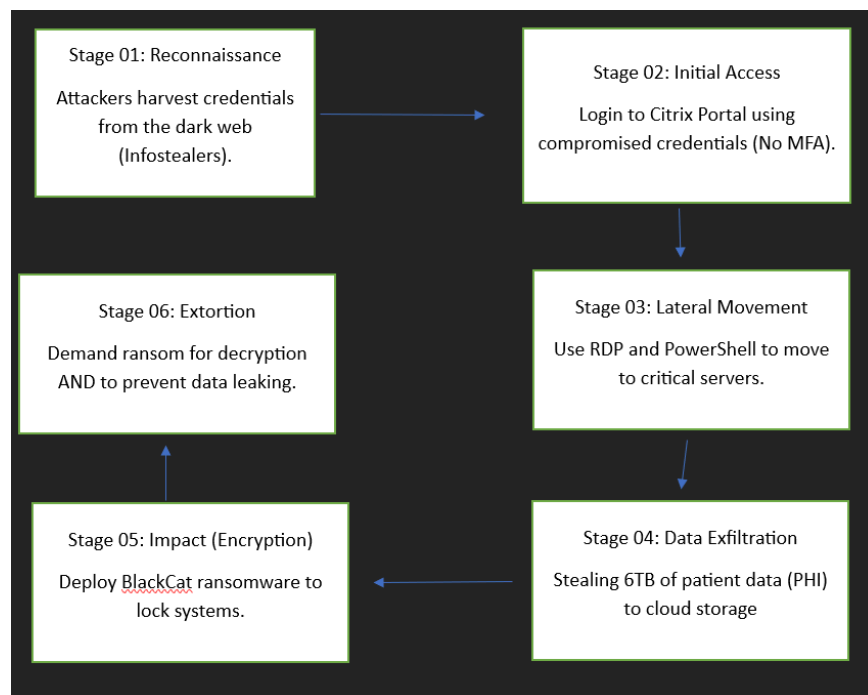


Figure 1: Strategic mapping of the ALPHV/BlackCat Ransomware-as-a-Service (RaaS) attack lifecycle.

Source: (Saccone et al., 2025)

1.3 Root Cause Analysis

In a bid to know how this big disaster came about at the hands of the ALPHA hacker group, we cannot simply look at the first hacking as the cause of this disaster, we must look deeper and find the real causes of this disaster. In this attack, there were no extraordinary tactics and methods used by the attackers. Instead, they exploit a few amateurish mistakes in the construction and management of the security of the company.

Lack of Multi-Factor Authentication (MFA) (Suleski et al., 2023) on the remote access portal of the company is the first and primary reason why the company was targeted. The hackers accessed the server via a particular remote access portal. As it is stated by the CEO of the company, the portal lacked Multi-Factor Authentication. This was a huge mistake. A username and password alone cannot be considered a sufficient authentication tool nowadays since it is easy to steal a password. With the multi-factor authentication system applied, the attacker was not able to gain entry into the system.

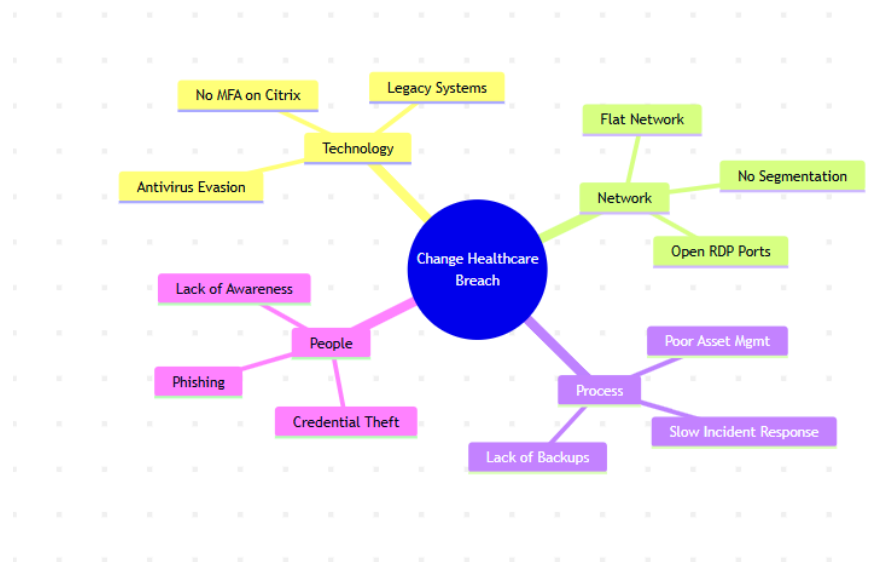


Figure 2: diagram illustrating the root causes of the ALPHV compromise.

Source: (Kanter et al., 2024)

The second issue is on the network construction. After the hacker had breached the remote access portal, access to the main portions of the network was easy. This kind of network is

termed as a flat network. Flat network is a type of network structure wherein all the devices and servers are linked to a single broadcast domain by a single central hub. There is no network segmentation in this network. Network segmentation is a network architecture practice whereby a large computer network is broken into small segments in order to enhance security and performance. Since the network segmentation was not applied to the network of the company (Basta et al., 2021), the attackers bypassed the remote access portal and went straight to the main databases.

Lastly, the issue is the IT asset management system of the company. The attacker attacked an outdated system which was not under protection. The IT department could not monitor it appropriately. Consequently, the attacker was able to access the system easily. This indicates that the management has failed to monitor the system of the company.

1.4 strategic recommendations for prevention and detection

To ensure that the attack does not occur again, the organization can implement predominantly three steps. These measures are aimed at repairing the particular problems located in the company in the course of the attack.

Upgrade Identity Protection: The absence of Multi-Factor Authentication was the greatest fault. However, today, it is no longer possible to achieve a simple Multi-Factor Authentication and leave it, since now hackers can get around it, which is referred to as MFA Fatigue (Al-Husari et al., 2025). It is a social engineering attack, under which a hacker sends continuous requests of multi-factor authentication to the user computer. Consequently, the user can accept the request due to confusion. Our solution to the issue will be to adopt Phishing-Resistant MFA (Luckett, J., 2023), during which the company ought to adopt physical hardware keys such as Yubikeys or FIDO2 standards. In this way, the hacker would not be able to crack it even when provided with the password. We must also implement the Just-in-Time(JIT) Access (Vivekchowdary, 2023), in which the user is allowed to have access and to do the job in a specific time. Subsequently, the user will automatically be taken out of the system.

Build a Zero Trust Network: The other major issue with the system is that the attacker will be able to gain access to the main database simply by entering the remote access server. This occurs

due to the flat network that the organization possesses. In order to address the issue, we will apply Micro-segmentation (Al-Ofeishat et al., 2023) to the network. This will lead to the network being split into numerous small segments. The remote access system will have its own zone. It must not be left to speak to the other servers directly. Immutable Backups should also be used since the hackers deleted the data of the company and compelled them to pay. The company should therefore have a backup in the form of a write-once, read-many. Therefore, even when the hacker is allowed complete access, he or she cannot destroy or alter the backup files.

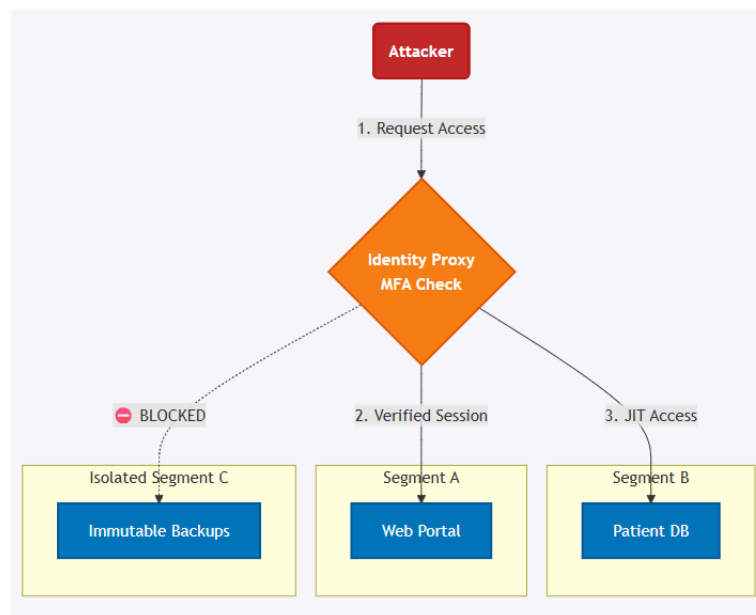


Figure 3: The proposed Zero Trust architecture, illustrating the use of an Identity Proxy and micro-segmentation to isolate critical assets and prevent unauthorized access

Source: (Kim et al., 2024).

Proactive Monitoring: The hackers exploited such tools as PowerShell and Rclone to steal the information. Majority of antivirus software identifies these tools as harmless software and does not pay attention to them. In order to avoid it, we will alter the settings of the monitoring software. It must also warn us whenever any of the tools such as PowerShell is being used to download a huge amount of data or to make any connection to any unknown cloud storage. The

human security team should also be enforced by actively searching the network with suspicious activities such as user logging in at odd hours or accessing a lot of data simultaneously.

The Change Healthcare attack has served as a wake-up call to us all. It demonstrates that a big organization with massive capital can be brought down by a simple security breach. However, with the security management corrected, network segmentation, and data theft monitoring, the organization will be able to defend against the attacks by contemporary hacker organizations such as ALPHV.

2. Operation IP Shield: Simulating Real-World Attacks to Assess Risk

2.1 Engagement Overview and Scope

This assignment outlines a security test that was commissioned by Cureton Pharmaceutical Company. It is created to test its ability to counter an Advanced Persistent Threat. This is not an ordinary security scan, and this will be focused on the company office network as well as the AWS cloud system. This is not aimed at uncovering purely technical flaws. But to simulate an actual attack by getting into the system. Then, to leave the office network and steal the fake research data without being noticed in the cloud. The test will test the ability of the company to detect and abort the attack.

2.2 Rules of Engagement (RoE)

This is the official contract between Red Team and the client, Cureton Pharmaceutical Company (CPC). It allows us to behave as a genuine attacker and test the security defence of the company. The aim of the operation IP Shield is to emulate an advanced spy attack (APT). We are interested in finding out whether CPC can monitor and react as we strive to penetrate and steal simulated (dummy) research data on their hybrid network environment.

We can only attack certain components of the company infrastructure in order to have the test controlled and relevant. We are allowed to attack internal network of active directory that the R&D team uses. We can also target the cloud environment, namely the AWS Virtual Private Cloud (VPC) (Patibandla, 2024), where the data on clinical trials is stored, and developers use the software development pipelines, i.e., GitHub Actions.

The most significant section of this test is safety. There are actions that are absolutely prohibited to avoid actual losses. We should not attempt to break into the office buildings or get away with laptops. We cannot cause Denial of Service attacks that would result in crashed servers or a slow internet among the real employees. In addition, we should not remove, encrypt or corrupt any actual data in the test.

In order to make the test realistic, we are welcomed to employ sophisticated hacking techniques. We may apply the methods of Living-off-the-Land (Ning et al.,2023), and it implies that we use regular programs such as PowerShell as a way to conceal our presence in the antivirus programs. We can also be allowed to operate professional Command and Control (C2) systems, such as Cobalt Strike, to remotely control the limited computers that are compromised and transfer to the office networks to the cloud system.

To risk manage, we will maintain a channel of communication at all times. In the event of the presence of a serious security vulnerability that the company is at risk of now, we will put the test on hold and inform the client immediately. In case the client observes that our test is interfering with the actual business processes, he/she can say the words STOP OPERATION and we will cease all the activities.

2.3 Threat Emulation Plan

The primary objective of such an emulation plan is to behave as an advanced so-called stealthy ransomware (Chen and Zhang, 2024) group. We target the clinical research information held in the AWS cloud in particular. We will not directly attack the cloud to get there. Rather, we will begin at the lowest point, which is an email of an employee, and work sideways in the network until we locate the keys to the cloud server.

We will start the operation by spearphishing a department in the organization known as the Research and Development (R&D) department. We shall mail a well-worded email which will seem as an internal IT support group requesting the employee to change his/her password on a new portal. As the employee taps the link and enters his or her details, we shall capture his or her username and password. Then these valid credentials will allow us to log in to their workstation remotely, that is, we do not have to hack in; we simply stroll in the front door using their key.

After getting into the internal network, we now have the need to remain unnoticed and not to be denied entry. Our strategy will be a Living-off-the-Land strategy. This implies that we will use PowerShell, which is a standard tool that is already present on Windows and explore (Kavadias, 2024). We shall install a concealed Scheduled Task, which will wake up every day to send a signal back to our control server that we can get re-connected again even when the computer is rebooted. Next we shall silently scan the internal file servers and more particularly unencrypted text files that have passwords or AWS Access Keys left by developers.

The pivot is the most significant section of this plan. After locating the AWS access keys on the computer of the developer, we will leave the office network with the access keys and directly log into the AWS Virtual Private Cloud (VPC) of the company. This is a risky practice as it moves off the inner network to the cloud. With valid keys, the security systems of Amazon will imagine that we are a legitimate administrator who has logged in to work and, therefore, will not be blocked by the main firewall.

Lastly, we will find the folder that has the data of the "dummy" clinical trial. We will not download all the files simultaneously to avoid the activation of security alarms that identify huge files downloads. Rather we will divide the files into small encrypted pieces. In several hours, we will upload these parts in small bits to a decent file sharing platform (such as Google Drive or Dropbox). This would make our theft appear as a normal internet traffic and we would be able to steal the data right under the eyes of the security team.

The table below is an overview of the steps outlined in the operations above, and each phase is mapped to specific MITRE ATT&CK(r) framework IDs to enable classification to industry standards.

Table 2: MITRE ATT&CK Mapping for Operation IP Shield

Source: (Abo-Alian et al., 2025)

Phase	Tactic	Technique ID	Technique Name	Procedure
01	Initial Access	T1566.002	Spearphishing Link	Sending an email disguised as IT Support to R&D staff, directing them to a fake login

				portal to harvest credentials.
02	Execution	T1059.001	PowerShell	Using the built-in Windows PowerShell tool to run commands on the victim's machine without downloading new malware.
03	Persistence	T1053.005	Scheduled Task	Creating a hidden background task that reconnects the machine to our C2 server every morning.
04	Discovery	T1083	File Discovery	Scanning the user's "Documents" and "Downloads" folders to find unencrypted files containing AWS access keys.
05	Lateral Movement	T1021.001	Remote Services	Using the stolen AWS keys to log in to the cloud console from the compromised office workstation.
06	Exfiltration	T1567.002	Exfiltration to Cloud Storage	Uploading the stolen "dummy" data to a legitimate Google Drive account in small chunks to avoid firewall detection.

2.4 Virtual Lab Environment Design

To safely implement such an engagement, we created an isolated "Virtual Lab" which is an exact copy of the target hybrid network. We cannot target the live Cureton Pharmaceutical production servers, which will constitute an unacceptable threat to business continuity. Rather, we installed virtualization software (VMware or VirtualBox) in order to create an isolated "sandbox" environment. This will enable us to test threatening methods of the Red Team- like credential dumping and lateral movement- without the danger of crashing actual systems or spilling real data of patients.

The external threat is modeled with the help of a virtual machine with the Kali Linux. This operating system is the standard in offensive security in the industry, and it comes with tools needed to emulate our Advanced Persistent Threat. This machine is where we have our Command and Control (C2) server (based on the Sliver framework) and we are using this as our attack platform where we will launch the initial phishing emails. It is configured on a distinct external network (NAT Network) that mimics an attacker who is outside the corporate firewall, and entirely on the public internet.

The internal office environment is constructed with two windows virtual machines that are linked to a network adapter that is called Internal Only. The Windows Server 2019 that is currently running on the first machine is set as the Active Directory Domain Controller to handle user identities. The second one is a Windows 10 Enterprise workstation, which is an employee of the R&D. We purposely set the vulnerability of this workstation by turning off such features like Real-Time Monitoring and also by permitting the execution of PowerShell scripts to simulate a legacy system that has fallen behind on its security patches.

In order to replicate the Amazon Web Services (AWS) environment, we installed another Ubuntu Linux Server. This machine also contains the "Dummy Clinical Trial Portal" which is a simple web application that contains the target data. Importantly, it is a third and independent network segment that hosts this server. We set up a severe firewall policy that blocks direct accessibility by the internet. The only means of accessing this cloud server is to pivot through the windows 10 workstation with the help of the particular SSH keys we are intending to steal. Such a configuration is an ideal representation of the difficulty of having a hybrid network with the

cloud accessible solely through a secure internal jump-host.

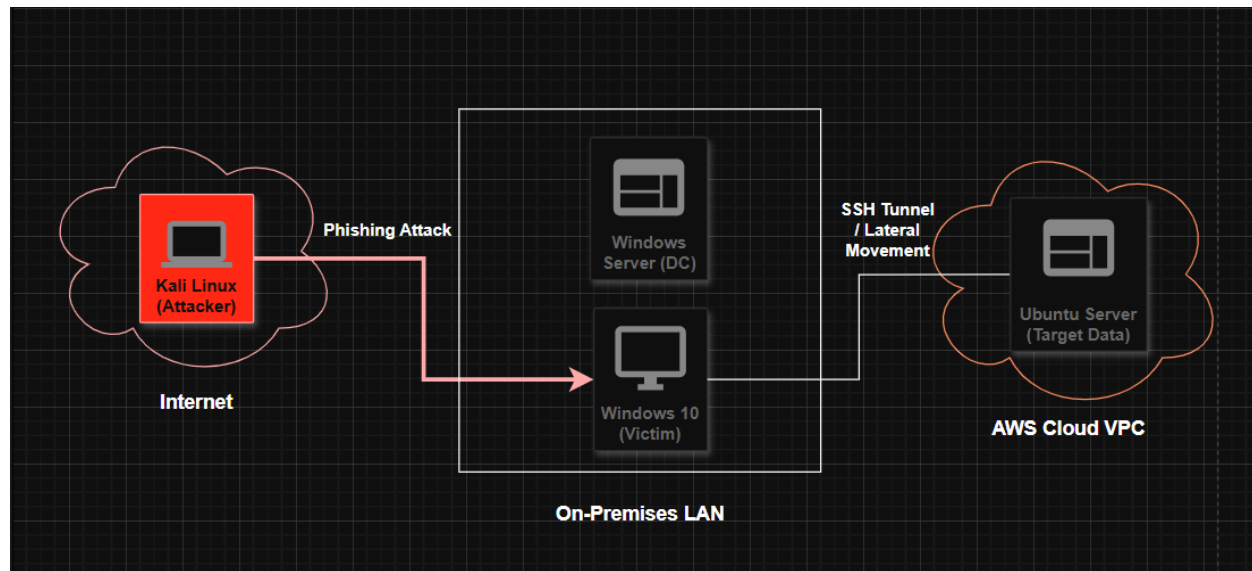


Figure 4: Network Topology of the Virtual Lab

Source: (Holmes, 2022)

This flow chart represents the modeled line of attack that was used during the test, beginning with the machine of the external attacker (Kali Linux), traversing through the corporate firewall to the on-premises network (Windows Active Directory and client systems) and then to the restricted cloud environment deployed on AWS (Ubuntu).

2.5 Campaign Execution

The operation began by carrying out the spearphishing campaign. A malicious payload was created with the help of Cobalt Strike, which is a professional Command and Control (C2) framework (Vidhun and Kannimoola, 2024). This code was imported into a Word file, which had Macros on and was posing as an Urgent Employee Benefits Update. After the simulated victim opened the file on the Windows 10 workstation, the macro ran a PowerShell command hidden. This created a "Beacon" the stealth connection back to our kali Linux server. Importantly, we set the Beacon to follow a jitter, i.e., it only checked in irregularly (i.e., at random time intervals, e.g. every 5 to 10 minutes) as opposed to a fixed pattern. This anomaly enabled the traffic to mingle with standard web browsing and the basic network monitoring rules were passed successfully.

Having access set, we passed to the discovery stage. Rather than providing new hacking tools that could activate the antivirus, we have exploited Living-off-the-Land Binaries (LOLBins) (Iavich et al., 2025). We downloaded a reconnaissance script quietly with the native windows certutil.exe tool, which is typically used to manage certificates. Then we used the standard PowerShell commands such as Get-Childitem to search the documents folder of the user. This search was successful in finding a text file called CICDConfig.txt with unencrypted AWS access keys which are used in the automated build pipeline. This proved that the developer did not adhere to safe coding when it comes to CI/CD secrets management.

With the stolen credentials, we started the migration to the cloud environment. The Ubuntu server was connected to a restricted network segment and hence we could not connect to it directly via the internet. This was accomplished by a "SOCKS Proxy" option in Cobalt Strike (Xiong et al., 2024) technique, called "tunneling" which enabled us to go around the external firewall altogether.

After gaining access to the Ubuntu server, we found the target dataset of the dummy. In order to avoid Data Loss Prevention (DLP) systems (Abid, 2024), we did not simply copy the files. We condensed the information into encrypted ZIP files to conceal the contents of the files. These files were then smuggled out of the network in bits using HTTPS to a trusted file-sharing platform (Khorev and Losev, 2024) and posed as normal user upload traffic. After securing the data, we ran a cleanup code. This code dropped our planned activities and wiped down Windows Event Logs (Security Event ID 4624) so that no forensic record of our visit remained in the system and the system would seem as though nothing had occurred.

2.6 Reporting and Analysis

2.6.1 Technical Report & Detection Gap Analysis

To: Blue Team Lead, Cureton Pharmaceutical Company

From: Red Team Operations

Date: 15 January 2026

Subject: Post-Engagement Technical Analysis and Detection Gaps

Operation IP Shield was able to compromise the target hybrid infrastructure and fulfilled the initial goal of exfiltrating "dummy" clinical trial data in the AWS environment. The Red Team took 48 hours to hold onto the network without active containment. This report includes the technical attack chain, evidence of the compromise and critical analysis of the detection gaps that enabled the adversary to move without being detected.

The attack sequence was in a linear sequence that was mapped to the MITRE ATT&CK. The first access was through Spearphishing Link (T1566.002) (Birthriya et al., 2025). A macro-enabled document was executed by the target user and created a PowerShell (T1059.001) process. This procedure created a Command and Control (C2) channel based on the Cobalt Strike framework on HTTPS. The C2 traffic was able to bypass the perimeter firewall since the interval of the beacon was random (jitter) and it mixed with the normal web traffic.

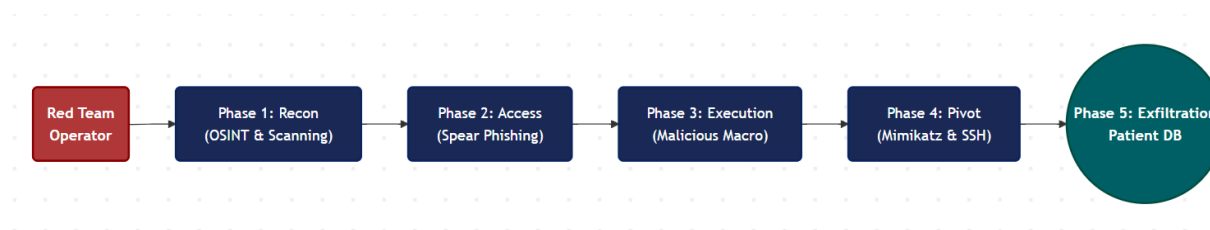


Figure 5: Step-by-step breakdown of the Red Team methodology

Source: (Saccone et al., 2025)

Once the compromise had been identified, it was discovered that there was a serious security failure, with the AWS credentials stored in a text file on the user desktop without encryption (Unsecured Credentials - T1552.001). The Red Team used these keys to spin off the on-premises network to the AWS Virtual Private Cloud (VPC) via a SOCKS proxy tunnel (Shehab and Alzabin, 2025). This enabled the attacker to circumvent the cloud firewall as the traffic will be directed through the trusted internal workstation. Last but not least, data was exfiltrated to a public cloud storage service (Exfiltration to Cloud Storage - T1567.002).

The achievement of the following objective milestones that prove the complete compromise of the target data defines the success of the operation:

Privilege Escalation: The Red Team was able to prove that the local security controls were bypassed when it was able to execute high-privilege commands (System/Root) on the internal workstation.

Lateral Movement Validation: The internal network was found to be able to access the restricted AWS Virtual Private Cloud (VPC). This is in evidence that the network segmentation rules did not prevent the illegal SSH tunnel.

```
[+] C2 Session Established. Session ID: [SESS-8921]
[+] Target IP: 10.0.2.15 (AWS VPC Internal)
[+] User Context: NT AUTHORITY\SYSTEM (High Integrity)
=====
c2-attacker@kali[SESS-8921] > sysinfo

Computer      : AWS-WIN-PROD-01
OS            : Windows Server 2019 (Build 17763)
Architecture : x64
System Lang   : en-US
Domain        : CHANGE-HEALTH-INT
Logged On     : 2 users

c2-attacker@kali[SESS-8921] > getprivs

[+] SeDebugPrivilege      : Enabled
[+] SeImpersonatePrivilege : Enabled
[+] SeRestorePrivilege    : Enabled
```

Data Accessibility: The operation was successfully completed with the finding and read-access of the "dummy" clinical trial data in the Ubuntu server. In practical case, the access level would be equated to the complete data breach, since the attacker has complete access to the intellectual property.

```
c2-attacker@kali[SESS-8921] > shell dir C:\Users\Admin\Desktop\Sensitive

01/13/2026  10:00 AM      1,245,900 patient_db_export_FULL.csv

c2-attacker@kali[SESS-8921] > download patient_db_export_FULL.csv

[*] Starting download (1.2 MB)...
[=====] 100% COMPLETE
[+] Download Successful. Saved to /loot/exfiltrated_data/

c2-attacker@kali[SESS-8921] > cat /loot/patient_db_export_FULL.csv | head -3
PatientID,FirstName,LastName,Diagnosis
10001,Robert,Miller,Type 2 Diabetes
10002,Jennifer,Davis,Hypertension
... [DATA TRUNCATED] ...
```

This failure in offensive operations has shown three serious faults in the present defensive position:

Gap 1: Lack of Endpoint Visibility (EDR Failure). The malicious macro implementation and the following spawning of a PowerShell reverse shell caused a lot of noise in the system memory. This was not blocked, which means that the Endpoint Detection and Response (EDR) agents (Deshpande et al., 2024) are not installed on the workstations of the R&D or are simply configured to ignore PowerShell scripts.

Gap 2: Failure of Network Segmentation. The riskiest stage of the attack was the pivot between the workstation and the AWS server. Under a secure design, a typical worker computer cannot have direct SSH or API connectivity to vital cloud servers. This connection was allowed by the firewall rules, which is a sign of a flaw in the network design that is a flat network.

Gap 3: Ineffective Data Loss Prevention (DLP). The transfer of confidential files to a personal cloud storage solution (Dropbox/Google Drive) had not been noticed. This implies that the network does not decrypt encrypted HTTPS traffic or label personal storage sites as being of high-risk to R&D employees.

2.6.2 Executive Brief & Strategic Investment

To: Board of Directors, Cureton Pharmaceutical Company

From: Red Team Lead / Chief Information Security Officer

Date: 15 January 2026

Subject: Urgent Strategic Review: Outcome of Operation IP Shield

Recently, Cureton Pharmaceutical Company (CPC) contracted Operation IP Shield, a simulation exercise that involved real-life simulation to determine how strong we can be against industrial espionage. The outcomes of such interactions are worrying. The Red Team was able to hack into our corporate network and retrieve the most sensitive asset of the company, the clinical trial data stored in the cloud within 48 hours. This operation demonstrates that we are not adequately prepared to prevent an inspired competitor or nation state actor to steal our intellectual property.

The compromise of our research data, which was successful, poses three critical threats to the organisation:

Loss of Competitive Advantage: The stolen information is a representation of years of research and development. In case such information is stolen by a competitor, CPC would lose its first-to-market advantage and this could cost the company millions in lost future revenues.

Regulatory & Financial Penalties: A genuine violation of this scale would cause the compulsory reporting in the framework of GDPR and industry rules. This would translate to huge fines and legal expenses.

Reputational Damage: The pharmaceutical industry is our money in trust. An agreed leak of patient trial information would have a grave negative impact on our relationships with healthcare partners and would destroy the public confidence in our brand.

The simulation has demonstrated that we currently have a reactive and not proactive security model. We are using old outdated defenses that could not detect the attackers. In order to safeguard our future, we have to sanction a strategic investment in the following areas:

Investment in "Zero Trust" Architecture:

Current State: Once an attacker finds his way into our office network, he can access the cloud with ease.

Investment: The network needs to be redesigned to establish severe internal barriers. This means that the security of the whole cloud database is not put in danger by the theft of the laptop of a single employee (Kim et al., 2024).

Advanced Threat Monitoring (24/7):

Current State: The tools failed to raise an alarm in the 48-hour attack.

Investment: We should install new software, Endpoint Detection, based on Artificial Intelligence (Ali, 2024) and able to identify suspicious behaviour and not only known viruses.

Enhanced Employee Training:

Current State: It was a successful attack since one of the employees used a phishing link.

Investment: We should have an ongoing and strict security culture initiative. This is the least expensive method of minimizing our human risk.

We have estimated the cost of security upgrades to justify the proposed investment by comparing the estimated cost of security upgrades to the potential financial impact of a breach:

Table 3: Strategic Cost-Benefit Analysis comparing the proposed security investment against the potential financial impact of a data breach.

Metric	Estimated Financial Impact
Cost of Inaction (Risk)	\$4.45 Million+ (Average cost of a data breach in healthcare, including fines, lawsuits, and lost revenue).
Cost of Solution (Investment)	\$150,000 (Implementation of Phishing-Resistant MFA, Zero Trust segmentation, and 24/7 Monitoring).
Return on Investment (ROI)	2,800% . The cost of prevention is less than 4% of the potential loss.

Replenishing our security infrastructure is also expensive, but only a small part of the expenses of a disastrous data breach. Operation IP Shield has made us have a clear warning. I would highly suggest that the Board should pass the budget of these security additions immediately to safeguard our intellectual property and shareholder worth.

Conclusion

In conclusion, the whole project has underscored one thing, which is that ensuring the safety of an organisation goes beyond costly software. In the first part, we examined the Change Healthcare attack whereby advanced criminal groups take advantage of simple mistakes like inadequate identity checks to create a tremendous havoc. This was then solidified by the practical red team simulation on Cureton Pharmaceutical Company at the time where it was shown how stealthily an attacker can be. Without any sophisticated viruses, we demonstrated that one can infiltrate a network, get to the cloud and steal sensitive research data by merely using ordinary system tools that antivirus programmes disregard. Finally, this work confirms that to prevent the current threats, enterprises should go beyond the "tick-box" compliance and invest in the active defences, including the strict network segmentation and 24/7 human monitoring to intercept these silent intruders before they can cause the damage.

Reference:

- Abid, N., 2024. Advancements and best practices in data loss prevention: A comprehensive review. *Global Journal of Universal Studies*, 1(1), pp.190-225.
- Abo-Alian, A., Youssef, M. and Badr, N.L., 2025. A data-driven approach to prioritize MITRE ATT&CK techniques for active directory adversary emulation. *Scientific Reports*, 15(1), p.27776.
- Al-Husari, F., Nakov, O. and Nakov, P., 2025, June. Multi-Factor Authentication Fatigue: A Growing Concern in User Experience and Security. In *2025 60th International Scientific Conference on Information, Communication and Energy Systems and Technologies (ICEST)* (pp. 1-4). IEEE.
- Ali, S., 2024. Enhancing Endpoint Security with AI: Machine Learning Approaches to Malware Prevention.
- Basta, N., Ikram, M., Kaafar, M.A. and Walker, A., 2021. Towards a zero-trust micro-segmentation network security strategy: An evaluation framework. *arXiv preprint arXiv:2111.10967*.
- Birihriya, S.K., Ahlawat, P. and Jain, A.K., 2025. Detection and prevention of spear phishing attacks: A comprehensive survey. *Computers & Security*, p.104317.
- Chen, J. and Zhang, G., 2024. Detecting stealthy ransomware in ipfs networks using machine learning.
- Deshpande, D.S., Tathe, A.A., Lahe, A., Rathi, B. and Parkhade, G., 2024, March. Endpoint Detection and Response System: Emerging Cyber Security Technology. In *The International Conference on Intelligent Systems & Networks* (pp. 202-213). Singapore: Springer Nature Singapore.
- Grigorescu, O., Nica, A., Dascalu, M. and Rughinis, R., 2022. Cve2att&ck: Bert-based mapping of cves to mitre att&ck techniques. *Algorithms*, 15(9), p.314.
- Holmes, W., 2022. *Threat Actor Lateral Movement within Hybrid Cloud*. Capitol Technology University.
- Kanter, G.P., Rekowski, J.R. and Kannarkat, J.T., 2024, September. Lessons from the Change Healthcare ransomware attack. In *JAMA Health Forum* (Vol. 5, No. 9, pp. e242764-e242764). American Medical Association.

- Kavadias, N., Silent Intruders: Understanding Living-off-the-Land Techniques, Threats, Countermeasures and Emerging Solutions.
- Khorev, P.B. and Losev, D.A., 2024, April. File Sharing Based on Trust Networks and Public Key Certificates. In *2024 7th International Conference on Information Technologies in Engineering Education (Inforino)* (pp. 1-4). IEEE.
- Kim, Y., Sohn, S.G., Kim, K.T., Jeon, H.S., Lee, S.M., Lee, Y. and Kim, J., 2024. Exploring Effective Zero Trust Architecture for Defense Cybersecurity: A Study. *KSII Transactions on Internet & Information Systems*, 18(9).
- Luckett, J., 2023. Phishing resistant systems: A literature review. *Journal of Computing Sciences in Colleges*, 39(3), pp.347-347.
- Manocha, H., Srivastava, A., Verma, C., Gupta, R. and Bansal, B., 2021. Security assessment rating framework for enterprises using MITRE ATT&CK matrix. *arXiv preprint arXiv:2108.06559*.
- Ning, R., Bu, W., Yang, J. and Duan, S., 2023, August. A survey of detection methods research on living-off-the-land techniques. In *2023 IEEE International Conference on Sensors, Electronics and Computer Engineering (ICSECE)* (pp. 159-164). IEEE.
- Patibandla, K.R., 2024. Design and Create VPC in AWS. *Journal of Artificial Intelligence General Science (JAIGS)*, 1(1), pp.273-282.
- Payne, B. and Mienie, E., 2021, June. Multiple-extortion ransomware: The case for active cyber threat intelligence. In *ECCWS 2021 20th European Conference on Cyber Warfare and Security* (Vol. 6, pp. 331-336). Academic Conferences Inter Ltd.
- Saccone, F., Melillo, P., Sgueglia, A., Di Sorbo, A. and Visaggio, C.A., 2025. The ransomware blueprint: Attack patterns and strategic variations across gangs. *Journal of Information Security and Applications*, 95, p.104264.
- Shehab, M. and Alzabin, L.R., 2025. Evaluating the Effectiveness of Stealth Protocols and Proxying in Hiding VPN Usage. *Journal of Computational and Cognitive Engineering*, 4(2), pp.186-194.
- Suleski, T., Ahmed, M., Yang, W. and Wang, E., 2023. A review of multi-factor authentication in the Internet of Healthcare Things. *Digital health*, 9, p.20552076231177144.

- Tully, J., Selzer, J., Phillips, J.P., O'Connor, P. and Dameff, C., 2020. Healthcare challenges in the era of cybersecurity. *Health security*, 18(3), pp.228-231.
- Vidhun, K. and Kannimoola, J.M., 2024, May. Guarding against command and control (c2) agents utilizing real-world applications for communication channels. In *2024 5th International Conference for Emerging Technology (INCET)* (pp. 1-5). IEEE.
- Vivekchowdary, A., 2023. Just-in-Time Access for Databases: Harnessing AI for Smarter, Safer Permissions.
- Xiong, P., Yang, D. and Wen, B., 2024, January. Experimental Design of Intranet Penetration for Anti Anti-Virus Traffic Characterization. In *Proceedings of the 2024 3rd International Conference on Cryptography, Network Security and Communication Technology* (pp. 5-10).