

Strategic Cyber Threat Analysis and Emulation

Keval Mahendra Motivaras

Student I'D- 2515743

December 14, 2025

Executive Summary

Smart cyber attackers are becoming increasingly targeted by pharmaceutical, healthcare, and research organisations with intentions to steal ideas, break important services, or gain a competitive advantage. To examine such threats, this report examines a real cyberattack and a red-team test. It demonstrates the functioning of Advanced Persistent Threats (APTs) and how companies can enhance their security.

Task 1 investigates a real case of failure in the healthcare sector as the WannaCry ransomware attack. The analysis of the attack steps against the ATT&CK framework of MITRE reveals how numerous tactics and tricks, such as using unpatched software, traversing the network, and locking files, led to huge problems. The findings demonstrate that WannaCry managed to achieve its success not due to a single defect, but due to the issues of patch management, network design, and internal detection.

Task 2, Operation IP Shield, is a simulation of red-team testing on Cureton Pharmaceutical Company (CPC) based on those lessons. By serving as a thief in disguise, the test demonstrated that sensitive research information could be stolen unnoticed, by using trusted paths and lax monitoring. The test revealed major areas of weakness particularly in the area of what the logged-in users were doing, how the system identified the insiders, and how data access was perceived. In general, the report indicates the necessity of APT-oriented defence. Securing valuable research assets needs to have controls based on identity, enhanced look-inside visibility, network separation, and post-hoc-attacker-follow-up detection, as opposed to network perimeter. Through the integration of the realistic threat research and practical experience, the report provides easily comprehensible measures to reduce the risks and harm of developed cyber spy attacks on pharma and healthcare organizations.

Introduction

There is a shift in the global cyber threat over the last few years. Smart cyber attackers are targeting companies in the pharmaceutical sector, the healthcare sector as well as research. They contain valuable ideas, important services, and confidential data, thus APT actors are interested in them. The pharmaceutical companies invest a significant amount of money in research that is over a period of many years and hence their ideas have considerable value financially or politically. Hospital organizations have complicated computer systems to assist patients and when any of them become compromised, it might pose a direct threat to individuals and halt treatment. Research institutions assist a nation in innovating and remaining safe hence spies and spies are interested in robbery (He et al., 2021).

Attackers of APTs of such locations do not pose a threat only to money. Theft of pharmaceutical research would damage the competitive advantage of a company and sluggish its products. Health-related cyber issues are capable of halting the operation of doctors and nurses and putting the patients at risk. Nationally, any theft of research and health information over the long term may result in individuals losing confidence in the system, and the disorganization of the rules as well as the harm to the tech leadership of the nation. As such, securing these locations must not merely be offered a firewall barrier but rather a clear understanding of the intentions of the attackers as well as the ability of detecting and preventing covert, long term attacks (Buckley et al., 2013).

There are two sections of this report. Task 1 provides a strategic overview of a real advanced attack on the health sector. It aligns the actions of the attacker with the MITRE ATT&CK framework to identify the primary tactics and tricks as well as failures in systems. Task 2 utilizes this appearance to carry out a realistic red-team test, simulating an APT assault in a pharmaceutical research environment. It is a test that is used to determine the performance of detection and defenses that are weak. The report takes one framework of MITRE ATT&CK and employs red-team techniques to bridge between theory and practice. It concludes by summarizing the results of the two tasks in order to inform intelligent, smart security improvements (MITRE, 2023).

TASK 1: Strategic Threat Analysis – From Headlines to TTPs

1.1 Overview of the Selected Real-World Cyber Attack

1.1.1 Background of the Incident

The WannaCry ransomware attack of 2017 was one of the most significant and multi-faceted cyber-attacks on the healthcare and research field in the recent years. It gravely injured the UK National Health Service (NHS). Although the attack occurred several decades ago, it still is relevant due to its use of ingenious means of diffusion, exploitation of a vulnerability in the systems, and lessons to be learned over time in the healthcare industry of how to defend sensitive research and intellectual property. The breach demonstrated how fast cyber issues in health care may evolve to computer issues, patient safety, and national security concerns (NHS England, 2023).

The NHS became a victim of a global ransomware attack that affected more than 230,000 computers in 150 countries. Health care organizations were particularly vulnerable since they had been operating on old systems, network structure was simple and they could not afford to be out. This ensured that the industry was an easy target by criminals and even state-related attacks.

1.1.2 Target Organisation

The principal victim in this case is the UK National Health Service (NHS) which is one of the largest health systems in the world that is funded by the British Government. The NHS has a huge IT network which is distributed in hospitals, research laboratories and administration offices. A lot of NHS trusts continued to run old versions of Windows operating systems, such as Windows XP and unpatched windows 7, particularly those in clinical equipment and research databases (Collier, 2017).

NHS is characterized by a decentralized system of governance and therefore, cybersecurity responsibilities were disproportionate in the trusts. This had the effect of patching inconsistently and having a low visibility across the whole network. These flaws led to the scenario that one vulnerability could be rapidly and uncontrollably propelled.

1.1.3 Threat Actor Attribution

According to intelligence agencies and cybersecurity researchers, the WannaCry campaign is attributed to the Lazarus Group that is affiliated to the North Korea government. Initially, WannaCry appeared to be interested in money due to its ransomware, however, as it was subsequently analysed, it possessed characteristics of state-sponsored attacks, including a poor money-making strategy yet an excellent hacking ability (Office of Public Affairs, 2018).

They possess sophisticated hacking tools and this is demonstrated by using a leaked NSA exploit named EternalBlue. Strong hacking in combination with random targets demonstrates how the state-provided tools may be utilized to initiate large-scale attacks that would result in severe damages.

1.1.4 High-Level Timeline of the Attack

On 12 May 2017, the WannaCry attack began. The computers with the virus started to encrypt files and make ransom requests. It propagated via a vulnerability of the SMB version 1, with a program named EternalBlue. Once in a network, WannaCry replicated itself, and it did not require people to perform any action (Kaspersky, 2024).

It took hours before numerous NHS trusts were out of system. Medical systems, booking systems, and diagnostic machines were stopped. A security researcher later that day triggered a hidden kill-switch domain which slowed the propagation. It is too late, however, to inflict the harm.

1.1.5 Impact and Strategic Significance

The attack hurt the NHS badly. A thousand and five hundred appointments were cancelled. Patients were forced to be taken elsewhere by the emergency rooms. Physicians were forced to work on paper rather than on computers. There was no stolen big data but the disorder still threatened patients. This was among the worst cyber attacks on health care.

In the case of pharmaceutical research companies, such as Cureton Pharmaceutical Company, which make medicines and conduct research, WannaCry demonstrates the risks of incompetent computer security, old systems, and failure to identify attacks, which allow powerful threats to ruin valuable work. CPC does not fear closing its services, but rather people stealing its research. These issues that were detrimental to the NHS may enable an attacker to steal research data as opposed to locking the system to demand money (Gregory, 2020).

1.2 MITRE ATT&CK Campaign Mapping

1.2.1 Attack Chain Narrative

The WannaCry case may be regarded as a rapid-paced attack campaign that best fits the MITRE ATT&CK Enterprise Matrix. It was more of a worm that distributed ransomware, rather than a standard hack that is executed using a keyboard. The attack commenced with a ransomware system that was to propagate automatically across windows networks. WannaCry did not rely on

any trickery since it was able to gain entry and execute itself through the known vulnerability of the Windows Server Message Block protocol (SMBv1) by way of the EternalBlue exploit. When a system had the said flaw, the malware executed automatically without the user taking any action, and it propagated rapidly in areas where there was no proper patching, network segregation, and tracking (MITRE ATT&CK, 2024).

Once the first machine was infected, WannaCry searched other machines that had SMB services and, using the same exploit, transferred sideways. This worm-like contagion made a single computer attacked to become an organization wide issue within a few hours particularly in large, distributed networks like in hospitals. The last phase was destruction: the viral software coded numerous files and closed down services. WannaCry was not based on a complicated command-and-control structure to organize, and its self-reliant design allowed it to continue spreading even without continuous attacker assistance. It demonstrates that malware is a simple program that can still lead to a considerable issue when the systems are exposed (Gregory, 2020).

1.2.2 MITRE ATT&CK Technique Mapping

Initial Access – Exploit Public-Facing Application (T1190)

The initial infection entry mode by WannaCry can be illustrated as T1190 (Exploit Public-Facing Application). It demonstrates how the malware took advantage of vulnerability in an open network service. To gain access into computers that had not installed Microsoft security update, the attackers exploited SMBv1 vulnerability (EternalBlue). Although SMB is not necessarily online SMB can be accessed within a company intranet and lack of network segregation exposed it. This method was successful due to patching being not uniform, the existence of old systems, and additional protective measures such as intrusion prevention or heavy isolation were frequently absent (MITRE ATT&CK, 2018).

Execution – Command and Scripting Interpreter (T1059)

WannaCry then began to execute itself in T1059 (Command and Scripting Interpreter) following the exploit. This demonstrates that it is possible to execute malicious code using Windows native means of executing programs. The program automatically started as soon as the exploit was successful and it began to encrypt files as well as spread without the user being required to do anything. It was successful because antivirus programs and controls against rules that prevent or block programs did not work since regular antivirus could not identify it at the earliest moment, as the malware has not yet produced the signatures and heuristics required to identify the new malware.

Persistence – Boot or Logon Autostart Execution (T1547)

WannaCry is T1547 (Boot or Logon Autostart) persistently used. The persistence tools allow the malware to continue running even after a reboot which is important when admins restart it to stop it. It is effective because most locations do not monitor startup changes and can find it difficult to view registry or service changes on lots of devices (Startup, 2025).

Privilege Escalation – Exploitation for Privilege Escalation (T1068)

WannaCry can be executed with a high level of privileges, which aligns with T1068 (exploit higher rights with the help of a vulnerability). Although the first attack as a result already granted it so much control, the bigger issue is that even loosely secured systems allowed it to acquire even more rights within a short period of time. The high rights they gave allowed it to lock files indefinitely and be propagated further. This was effective in situations where the system did not impose the rule of least privilege, did not segregate privileged duties effectively, and had weak application security controls.

Defense Evasion – Obfuscated/Encrypted File Payloads (T1027)

The malware also concealed the activity by employing a process known as T1027 or in other words by encasing its files in a difficult to read manner. Although the effects of the attack were felt when encryption commenced, hiding may postpone the early detection of the attack by signature controls. The method is most effective when organisations are primarily supported by antivirus signals rather than determining behavioural alterations, and when the threat-intelligence updates are not swift enough to identify new variations (Guo et al., 2025).

Lateral Movement – Exploitation of Remote Services (T1210)

The most outstanding operational aspect of the campaign was the Lateral Movement through T1210 (Exploitation of Remote Services). WannaCry used the same vulnerability repeatedly to scan the networks of hosts that were SMB enabled and to allow worm-like proliferation without human intervention. This was especially destructive in flat networks where eastwest traffic was not

restricted and important systems could be accessed through access to ordinary endpoints. In these types of environments, attacker sophistication is not a major driving force in facilitating lateral movement but the architectural exposure.

Credential Access – OS Credential Dumping (T1003)

It is also able to retrieve passwords on the infected computers even though it is not the primary mode of spread via the malware and tools. Weak passwords will enable the attackers to get control of more systems once the initial infection.

Discovery – Network Service Scanning (T1046)

WannaCry scanned network services (T1046) over internal computers with SMB. This assisted it in diffusing fast and reaching targets. It succeeded since most organizations lacked a benchmark of scans within the organization, did not scan between divisions, and did not warn them when SMB connections increased (Fortinet, 2025).

Command and Control – Application Layer Protocol (T1071)

In the case of command and control, WannaCry would be compared to T1071 which is an application layer protocol since it attempts to communicate with the network including checking the known kill-switch domain. Even some outgoing messages can be used to defend against this as they can be inspected by visualizing the logs of DNS and tracking outgoing traffic. WannaCry is more efficient when the outgoing traffic rules are loose and when monitoring is not optimally tuned so that it could detect strange domain queries.

Impact – Data Encrypted for Impact (T1486)

Lastly, WannaCry inflicted huge harm by encrypting files (T1486: Data Encrypted for Impact) and preventing the access to valuable systems. This had not only been effective because encryption is bad, but it was also effective because most firms did not have effective backups, tested methods of restoring information, or concrete strategies to act in response. In hospitals, it translated into cancelled appointments, interrupted operations as well as increased safety risks. Comprehensively, this mapping indicates that attackers with access the network via exploits and move fast within a network can inflict immense damage in the event that patches, network isolation, and detection solutions are feeble (Cloudflare, n.d.).

1.3 Root Cause Analysis

1.3.1 Patch Management and Legacy Systems

One of the primary reasons why the WannaCry attack occurred was that NHS was not good at patch updates. Microsoft had already implemented security patches to prevent the SMBv1 issue that was exploited by EternalBlue but not all computers had been patched when the attack began. This was due to the fact that most health care places operate on systems that cannot be easily stopped to undergo repairs. Individuals feared to damage patient care and the approval process took a long time and several NHS trusts were required to share the workload. This rendered patching to be slow or uneven. Also, a significant number of them ran outdated, unsuitable, windows XP that receives no security patches, thus remaining vulnerable eternally (NHS England, 2023).

1.3.2 Architectural Weaknesses and Network Design

One of the primary reasons why the WannaCry attack occurred was that NHS was not good at patch updates. Microsoft had already implemented security patches to prevent the SMBv1 issue that was exploited by EternalBlue but not all computers had been patched when the attack began. This was due to the fact that most health care places operate on systems that cannot be easily stopped to undergo repairs. Individuals feared to damage patient care and the approval process took a long time and several NHS trusts were required to share the workload. This rendered patching to be slow or uneven. Also, a significant number of them ran outdated, unsuitable, windows XP that receives no security patches, thus remaining vulnerable eternally (Microsoft Defender Security Research Team, 2017).

1.3.3 Human and Organisational Factors

The technical issues were aggravated by human and organizational problems. The board did not always regard cybersecurity as a major threat, and hence there was no adequate funding on qualified individuals, updated equipment, and long-term preparation. The responsibility of cybersecurity had been divided among numerous teams and trusts, and therefore, it was difficult to understand who did what and the standards did not occur everywhere. Additionally, non technical people did not know much about cybersecurity and hence did not see the need to rectify known issues immediately particularly when they were required to attend to everyday clinics.

1.3.4 Detection and Incident Response Failures

Lastly, there were no mature detection and response tools, which allowed the attack to proceed without much notice. Such aspects as abnormal SMB traffic, network scans, and mass encryption of files were not identified in real-time. Several NHS organisations lacked intrusion detection systems, central logging service using SIEM solutions, and endpoint detection and response (EDR) solutions that were able to identify unusual behaviour. Due to this fact, the reaction was largely reactive, and it was to restore the situation after the damage was already done. It demonstrates that numerous organisations were unprepared to detect and prevent sophisticated threats before they led to their extensive operational interference and damaged patient safety (Anjan Kumar Gundaboina, 2025).

1.4 Strategic Prevention and Detection Recommendations

1.4.1 Strengthening Preventive Controls

CPC ought to emphasize the general security modification rather than rushed technological fixes. There must be a robust, risk-oriented patch system in place to ensure that all things are listed in the right order, prioritized, and repaired in due time. The old or unsupported systems are to be removed or blocked or extra controls put in place where feasible. In case patching is difficult, additional safety features such as network intrusion prevention must be implemented to make it more difficult and minimize the risk.

1.4.2 Enhancing Detection Capabilities

In detection, CPC must align itself with its monitoring plans with the MITRE ATT&CK framework in order to capture every phase of an attack. They should implement EDR that will monitor user and program activity to identify ransomware, users who access privileges that are not necessary to them, or network movement. Monitor the network traffic as well, to detect the curious SMB scans, unexpected connections within the network, and the strange data streams that may indicate the attacker stealing data (MITRE ATT&CK, 2024).

1.4.3 Architectural and Governance Improvements

In terms of design, CPC must apply network segmentation and Zero Trust concepts to prevent the mobility of attackers as well as minimize the harm in the event of a breach occurring. Administrative and internet-facing systems should not be mixed with research areas. On the policy-level, cyber security must be incorporated into major decisions, and the board controls, frequent red team exercises, and continual threat assessments must be performed to ensure intellectual property and research resources are secure in the long run (Palo Alto Networks, 2019).

TASK 2: Red Team Engagement – “Operation IP Shield”

2.1 Engagement Scenario and Objectives

2.1.1 Organisational Context

Cureton Pharmaceutical Company (CPC) is an organisation that engages in research pharmaceutical business that operates in a highly competitive and innovation-driven as well as highly regulated business environment. The company has the capability of generating, safeguarding, and selling its own research, including drug formulations, pre-clinical outcomes, and clinical trial information, which makes the company valuable. Cyber attacks that may target its intellectual property (IP) are an increased risk to CPC as it approaches a large new drug. The attacks are normally initiated by well organized groups such as state sponsored hackers and well financed corporate spies who are seeking economic or strategic benefits (Munday, 2024). The loss of research data in the pharma industry can lead to greater losses than the direct loss of money. It may destroy decades of investment, postpone regulatory permits and destroy stakeholder trust. Moreover, today research environments are combined with on-premises systems, cloud services and collaboration tools that form a vast attack surface that cannot be addressed solely with a perimeter security feature. Due to the knowledge of such threats, CPC engaged a red team, which tested its security against realistic and strategically motivated threats (Austin and Hayford, 2021).

2.1.2 Red Team Role and APT Emulation Objective

The mission of red team in operation IP shield was that it was to pretend to be a sneak thief attacker over time rather than attacking aggressively. The practice was arranged to resemble actual espionage operations, which revolve around remaining unnoticed, creating minimal commotion, and accessing familiar points of entry as opposed to direct assaults. The idea was to determine whether an attacker would be able to navigate through the network of CPC and locate useful research information, and steal it without detection (Post, 2025).

The primary objective of the exercise was to retrieve and access a phony research data sample which was carried in CPC internal system. Technical skills were not only counted as a measure of success but also the ability of the team to do this without the knowledge of the current security controls. This objective assists CPC to remain guarded against long-term cyber spying that may remain undetected until it results in a competitive or regulation loss.

2.2. Rules of Engagement (RoE)

2.2.1 Scope and Authorised Systems

The interaction was only within the simulated hybrid environment of CPC. It contained on-premise Active Directory domain that was a representation of the R&D network, an internal repository that was a simulation of cloud-based research storage, and a Kali Linux system that was a representation of attacker controlled infrastructure. Testing was not done against external, third, and production systems. The entire process remained behind the cage of the lab (soderholmd, 2024).

2.2.2 Permitted and Prohibited Techniques

Approved methods involved reconnaissance, simulation of credential-less access, internal discovery of resources, and utilisation of legitimate system functions, and adhering to the idea of living-off-the-land. Activities that were prohibited were denial-of-service attacks, destructive payloads, real malware deployment, or any other activity that might cause permanent damage to systems or data. These limitations were necessary to make the engagement ethical, legal, and in line with the academic assessment criteria.

2.2.3 Data Handling, Communication, and Ethics

The data that they saw were all fabricated research documents that were just to be tested. No actual personal, medical or secret information was utilized. They simply made the findings in order to have a better defense, and they did not conceal the work before the assessor. The work was in line with the ethical guidelines of safe security testing and academic honesty (Berger and Alperson, 2009).

2.3 Threat Emulation Plan

2.3.1 Simulated Adversary Profile

The attacker in the Operation IP Shield was designed to appear as a state-sponsored Advanced Persistent Threat (APT) that is interested in stealing pharmaceutical research and intellectual property. This character is founded on actual spy organizations that do not require money at short term but long term strategic benefits. The counterfeit APT was said to be patient, cautious in security and able to remain silent and fit within normal business operations. The attacker relied primarily on inbuilt system tools, genuine user credentials, and authorized access routes, rather than creating its malware or performing blatant attacks. This is referred to as living-off-the-land. It has been designed that way in order to increase the difficulty of being detected by the regular security and that would resemble the tactics used in advanced espionage missions against research organisations (Baker, 2025).

2.3.2 Campaign Objectives and Attack Phases

The primary objective of the campaign was to locate, enter, and steal in the sensitive research data in the CPC R&D facility without raising any security alarm. To do, they prepared the work with distinct steps, which simulate a realistic APT attack. The sequencing was as follows: First they map the resources available within the system; they get initial access to it through a hacked device; they find shared research repositories and they end by harvesting and feigning to distribute out fake research data via valid file access programs. All these phases were aimed at determining whether CPC could identify any evidence of a violation rather than a blatant malicious activity, and gauge the willingness of the organization to deal with the threats of stealthy spying (Sasi et al., 2023).

2.3.3 MITRE ATT&CK Mapping Overview

2.4. Environment Design and Lab Architecture

2.4.1 Hybrid Environment Description

The lab was developed to replicate the manner the systems at Cureton Pharma are configured, particularly the sections that guard the inventions of the organization. The lab contains an on-premises Active Directory domain which displays the research network. It contains a domain controller that registers users and has identities and a workstation which is a domain member as is the case with an employee computer. This demonstrates the way the researchers access common resources by using company passwords (Microsoft, 2025).

They also created a common folder to simulate the cloud or hybrid data storage of the company. This demonstrates that sensitive files can be accessed both in the office and in the cloud. The attacker machine was modeled with Kali Linux software and was functioning as an outsider who has already bypassed the outer defenses, like a long-term attacker. The machines were all connected to a personal virtual network within the lab meaning that testing remains safe and can be replicated repeatedly. Figure 01 illustrates the conceptual hybrid architecture used during the engagement, including a simulated AWS VPC hosting a clinical trial data portal within a private subnet. The diagram highlights trust boundaries and assumed lateral movement paths between the on-premises R&D Active Directory environment and cloud-hosted research resources.

Figure 01- AWS VPC CONCEPTUAL ARCHITECTURE

2.4.2 Assumptions and Limitations

Since they were not able to create real cloud servers and test pipelines, they used simulation to fool the system rather than launching a full simulation. They also took clear notes on what they assumed and concentrated on how an attack is executed, trust relations and locations where it may remain unnoticed. These are the main points that they have been interested in. They also created a basic network map. It displays the trust lines and potential attack patterns, and one can easily interpret it without having to discuss the technical side (Iftikhar et al., 2023).

2.5 Attack Narrative (Execution)

2.5.1 Reconnaissance

The team began to scan the network and locate resources that they could get. To the attacker, internal file shares and folders were displayed on simple searches. This is equivalent to MITRE ATT&CK T1046, and indicates that small scans may identify significant targets when the network is not segregated (TcyberSec007, 2025).

2.5.2 Initial Access (Simulated)

The first entry was supposed to occur by a compromised internal workstation and this is a realistic case of phishing or reusing credential. This assumption is equivalent in T1078 (Valid Accounts), and is congruent with most real-world APT campaigns, where the initial compromise is never observed at the subsequent stage of detection.

2.5.3 Execution and Discovery

The attacker searched in directories with the use of built-in command-line tools and discovered a shared research folder containing fake data. Technique T1059 (Command-Line Interface) and T1083 (File and Directory Discovery) was used by the attacker in this step. Based on the normal system tools, the activity appeared normal and was not able to raise easy security alerts (MITRE ATT&CK, 2017).

2.5.4 Lateral Access to Research Data

The hacker accessed the shared research folder through trusted file-sharing techniques, which are equivalent to T1021 (Remote Services) and T1039 (Data from Network Shared Drive). The attacker was not faced with resistance and alert due to the fact that the permission on the folder was open and because of the weak monitoring.

2.5.5 Exfiltration (Simulated)

They proved the theft of data by transferring a counterfeit research file to the system of the attacker via a shared folder. It is a basic example, but it demonstrates that T1048 (Exfiltration Over Alternative Protocol) and can make the data leave a system without being noticed by perimeter defenses in case insiders are abused (Koval, 2022).

2.6 Detection Gap Analysis

The red team activity proved to be effective principally due to the fact that the actions of the attack left virtually no useful data in order to be detected and the limited available logs were not connected or followed closely to notice issues early. In the initial phases, the attackers searched the internal file systems and shared folders without triggering any alert and this signified a significant loophole in viewing within the traffic and user behavior on the network. Such techniques as File and Directory Discovery (T1083) and Data from Network Shared Drive (T1039) bypassed the existing controls, pointing to the fact that the security had been over-focused on the protection of the perimeter and the belief that the threats are external (Sharma, 2022).

Another issue was that the attackers provided valid credentials, which allowed them to move freely within the standard areas of trust. The events of logouts were accepted without verification of whether the usage was in line with the normal usage patterns. Such peculiar activities as a work station reading research material that it was not supposed to read went unnoticed. The absence of

user and entity behavior analytics (UEBA), the strategy of minimal logging of file access, and weak alert thresholds enabled the advanced persistent threat simulated to proceed without being detected. These vulnerabilities demonstrate that instead of preventing the first break-in, the organization was more concerned with preventing a compromise and identifying and preventing subtle activity, which is common in advanced espionage attacks (Microsoft, 2024).

2.7 Strategic Recommendations for CPC

CPC needs to pay attention to identity-based controls and internal visibility since when a hacker enters a system, he/she can retrieve sensitive information without hard work and without being noticed. To start with, restrict access to research files to authorized R&D employees only and make a regular review of such permissions. Include strong authentication such as phishing-resistant MFA to privileged accounts and sensitive data and policies that validate the device, location, and risk prior to access. Second, enhance surveillance through documenting all file access, use of shared-folders, and logins. Train on these logs to understand what normal activity should look like and raise suspicion of unusual patterns, like a new computer is accessing R&D shares, there was a huge spike in the number of data reads, or after-hours logins. Third, align detections to MITRE ATT&CK through the establishment of alerts concerning discovery (checking files and folders), collection (accessing shared drives), and exfiltration (seeking after the existence of staging areas or bizarre data transfer paths). Develop network segmentation such that R&D data is isolated with the rest of the workstations which slows down lateral mobility and limits damage. Such measures reduce the risk of the IP stealing and accelerate the reaction in case of an attack (Microsoft, 2024).

2.8 Cost–Benefit Analysis

Although improved identity controls, logging and segmentation require certain initial investment, the price is insignificant compared to the potential damage to pharmaceutical IP theft. A single infringement can be quite expensive: proprietary research can be lost, it can wipe out years of R&D investment, competitive advantage can be lost, regulatory approvals or product introductions can be slackened down. A minor data leak can allow the competitors to replicate the research focus, accelerate the development process, or to threaten the position of CPC on the market. CPC also has the indirect costs: incident response assistants, legal assistance, downtime, and reputation damage, which can damage partnerships, investor attraction and retention of employees. The risk may be exacerbated by regulatory issues in case of challenge on trial data, which results in audits and increased compliance (Ignacio De Leon and Jose Fernandez Donoso, 2017).

Conversely, the proposed improvements may be implemented in phases and controlled expenses. As an illustration, restrictive measures such as tightening permissions and MFA are inexpensive measures that reduce risk immediately. The logging and monitoring may be expanded in stages, initially securing the most valuable items such as R&D information and privileged accounts and progressing onwards. It is also possible to start segmentation with the most sensitive networks other than total redesign. These investments pay off when viewed as a business case: they reduce the likelihood and severity of a breach and increase the response time to breach and prevent it, as well as safeguard the primary value of CPC its research and IP (Takyar, 2023).

2.9 Executive Brief

The case of Operation IP Shield revealed that an intruder could infiltrate the research network of Cureton Pharmaceutical Company (CPC) and steal one of its research files without detection. It was conducted in the laboratory using a falsified data, however, the test demonstrates an actual threat that enables an attacker to quietly get access to sensitive research and steal valuable work without being noticed by the security departments at CPC at first (Sadeghpour and Vlajic, 2021). In case, this actually occurred, CPC would be in great trouble. It would be detrimental to the company because it would be losing its own research that would sluggish the development of new products and reduce profitability in the future. The theft that goes unnoticed also leads to the possibility of government investigations, bad publicity, and the lost confidence of investors and research partners.

There are three primary ways that leadership can mitigate these risks. First, become better who may log in to information and have access. Grant only the minimum required permissions, have strong multi-factor authentication which is difficult to phish, and maintain a tight rein over privileged accounts (MicrosoftGuyJFlo, 2024).

Second, monitor the network more attentively. Record comprehensive account of the log-ins and file movements and establish notification of anything suspicious. Lastly, re-architect the network such that research systems are isolated of the rest of the computer systems of the company. This

prevents the spread of a breach and limits the damage in case something terrible occurs. The three steps will reduce the possibility of concealed IP theft and protect CPC against advanced cyber attacks.

Conclusion

This evaluation covered severe cyber attacks on hospitals and pharmaceutical companies. It applied real-life analysis and practical test to demonstrate how clever attackers operate and how companies can defend themselves. Task 1 revealed that such attacks as WannaCry are not a piece of old news. They also instruct them that even weak systems like failure to repair software in time, basic network design, and missing access to what happens within the network can be scaled by attackers. Making the attack comparable to the MITRE ATT&CK map indicates the number of steps in the attack process that cooperate and create huge issues to the daily operations as well as long-term plans (Owens, 2020).

Operation IP Shield was a real test where task 2 utilized the lessons learned through Task 1. The test attempted to penetrate into the research field of Cureton Pharmaceutical Company. Without malware or new security vulnerabilities, the testers demonstrated that a determined attacker can obtain access to the system and steal research data. They did this through the legitimate access routes and exploitation of lax monitoring. The test also discovered key locations where the company could not notice or prevent the attacker, and it was also discovered that the greatest threat is what has to occur once the attacker is inside, not the first crash (Jha, 2023).

Combined, the two tasks emphasize the importance of the usage of APT-oriented defense strategies. The evaluation determines that good cybersecurity requires futuristic, data-intensive controls, continuous monitoring, and robust design to make valuable research safe in a world with increased attackers.

Reference List

- Anjan Kumar Gundaboina (2025). Endpoint Detection and Response (EDR) in Healthcare: Mitigating Threats on Critical Devices. *Journal of Technology and Systems*, [online] 7(4), pp.50–65. doi: <https://doi.org/10.47941/jts.2878>.
- Austin, D. and Hayford, T. (2021). Research and Development in the Pharmaceutical Industry. [online] Congressional Budget Office. Available at: <https://www.cbo.gov/publication/57126>.
- Baker, K. (2025). What is an Advanced Persistent Threat (APT)? | CrowdStrike. [online] Crowdstrike.com. Available at: <https://www.crowdstrike.com/en-us/cybersecurity-101/threat-intelligence/advanced-persistent-threat-apt/>.
- Berger, V. and Alperson, S. (2009). A General Framework for the Evaluation of Clinical Trial Quality. *Reviews on Recent Clinical Trials*, [online] 4(2), pp.79–88. doi: <https://doi.org/10.2174/157488709788186021>.
- Buckley, G.J., Gostin, L.O., Committee on Understanding the Global Public Health Implications of Substandard, Falsified, and Counterfeit Medical Products, Board on Global Health and Institute of Medicine (2013). Weaknesses in the Drug Distribution Chain. [online] Nih.gov. Available at: <https://www.ncbi.nlm.nih.gov/books/NBK202523/>.
- Cloudflare (n.d.). What was the WannaCry ransomware attack? [online] Cloudflare. Available at: <https://www.cloudflare.com/learning/security/ransomware/wannacry-ransomware/>.
- Collier, R. (2017). NHS ransomware attack spreads worldwide. *Canadian Medical Association Journal*, [online] 189(22), pp.E786–E787. doi: <https://doi.org/10.1503/cmaj.1095434>.
- Fortinet (2025). What is WannaCry? WannaCry Ransomware Attack Case Study. [online] Fortinet. Available at: <https://www.fortinet.com/resources/cyberglossary/wannacry-ransomware-attack>.
- Gregory, J. (2020). Articles WannaCry worm ransomware changed cybersecurity. [online] Ibm.com. Available at: <https://www.ibm.com/think/x-force/wannacry-worm-ransomware-changed-cybersecurity>.
- Guo, W., Xue, J., Liu, Z., Han, W. and Hu, J. (2025). MalGTA: Large language Model-based Guided Malware Tactical Analysis. [online] doi: <https://doi.org/10.21203/rs.3.rs-6226366/v1>.
- He, Y., Aliyu, A., Evans, M. and Luo, C. (2021). Healthcare cyber security challenges and solutions under the climate of COVID19: A scoping review. *Journal of Medical Internet Research*, [online] 23(4). doi: <https://doi.org/10.2196/21747>.
- Iftikhar, A., Qureshi, K.N., Shiraz, M. and Albahli, S. (2023). Security, trust and privacy risks, responses, and solutions for high-speed smart cities networks: A systematic literature review. *Journal of King Saud University - Computer and Information Sciences*, [online] 35(9), p.101788. doi: <https://doi.org/10.1016/j.jksuci.2023.101788>.

Ignacio De Leon and Jose Fernandez Donoso (2017). The Impact of IP Risk in the Development of IP Markets. Springer eBooks, pp.97–110. doi: https://doi.org/10.1007/978-3-319-54906-4_6.

Jha, S. (2023). Penetration Testing for Sensitive Data Exposure in Enterprise Networks: Everything You Need to Know! [online] WeSecureApp :: Securing Offensively. Available at: <https://wesecureapp.com/blog/penetration-testing-for-sensitive-data-exposure-in-enterprise-networks-everything-you-need-to-know/>.

Kaspersky (2024). What is WannaCry ransomware? [online] Kaspersky.com. Available at: <https://www.kaspersky.com/resource-center/threats/ransomware-wannacry>.

Koval, K. (2022). What Is Data Exfiltration? MITRE ATT&CK® Exfiltration Tactic | TA0010. [online] SOC Prime. Available at: <https://socprime.com/blog/what-is-data-exfiltration-mitre-attack/>.

Microsoft (2024). What Is User and Entity Behavior Analytics (UEBA)? | Microsoft Security. [online] Microsoft.com. Available at: <https://www.microsoft.com/en-us/security/business/security-101/what-is-user-entity-behavior-analytics-ueba>.

Microsoft (2025). Active directory domain services overview. [online] Microsoft. Available at: <https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/get-started/virtual-dc/active-directory-domain-services-overview>.

Microsoft Defender Security Research Team (2017). WannaCrypt ransomware worm targets out-of-date systems. [online] Microsoft Security Blog. Available at: <https://www.microsoft.com/en-us/security/blog/2017/05/12/wannacrypt-ransomware-worm-targets-out-of-date-systems/>.

MicrosoftGuyJFlo (2024). Require phishing-resistant multifactor authentication for Microsoft Entra administrator roles - Microsoft Entra ID. [online] Microsoft.com. Available at: <https://learn.microsoft.com/en-us/entra/identity/conditional-access/policy-admin-phish-resistant-mfa>.

MITRE (2023). Techniques - Enterprise | MITRE ATT&CK®. [online] attack.mitre.org. Available at: <https://attack.mitre.org/techniques/enterprise/>.

MITRE ATT&CK (2017). Command and Scripting Interpreter, Technique T1059 - Enterprise | MITRE ATT&CK®. [online] attack.mitre.org. Available at: <https://attack.mitre.org/techniques/T1059/>.

MITRE ATT&CK (2018). Exploit Public-Facing Application, Technique T1190 - Enterprise | MITRE ATT&CK™. [online] attack.mitre.org. Available at: <https://attack.mitre.org/techniques/T1190/>.

MITRE ATT&CK (2024). Matrix - Enterprise | MITRE ATT&CK™. [online] attack.mitre.org. Available at: <https://attack.mitre.org/matrices/enterprise/>.

Munday, J. (2024). The Threat of Intellectual Property (IP) Theft: Why Incident Response is Your Best Friend | Cybaverse. [online] Cybaverse.co.uk. Available at: <https://www.cybaverse.co.uk/resources/the-threat-of-intellectual-property-ip-theft-why-incident-response-is-your-best-friend>.

NHS England (2023). NHS England business continuity management toolkit case study: WannaCry attack. [online] www.england.nhs.uk. Available at: <https://www.england.nhs.uk/long-read/case-study-wannacry-attack/>.

Office of Public Affairs (2018). North Korean Regime-Backed Programmer Charged With Conspiracy to Conduct Multiple Cyber Attacks and Intrusions. [online] Justice.gov. Available at: <https://www.justice.gov/archives/opa/pr/north-korean-regime-backed-programmer-charged-conspiracy-conduct-multiple-cyber-attacks-and>.

Owens, B. (2020). How hospitals can protect themselves from cyber attack. Canadian Medical Association Journal, 192(4), pp.E101–E102. doi: <https://doi.org/10.1503/cmaj.1095841>.

Palo Alto Networks (2019). What is a zero trust architecture? [online] Paloaltonetworks.com. Available at: <https://www.paloaltonetworks.com/cyberpedia/what-is-a-zero-trust-architecture>.

Post, C.T. (2025). Cyber Threat Post. [online] Varutra.com. Available at: <https://varutra.com/ctp/posts/postDetails/VkpqVFVodS9iU2JsWU05YlhqMDI4QT09/Microsoft-Trust-Signing-Service-Exploited-to-Code-Sign-Malware> [Accessed 14 Dec. 2025].

Sadeghpour, S. and Vlajic, N. (2021). Click Fraud in Digital Advertising: A Comprehensive Survey. Computers, 10(12), p.164. doi: <https://doi.org/10.3390/computers10120164>.

Sasi, T., Lashkari, A.H., Lu, R., Xiong, P. and Iqbal, S. (2023). A Comprehensive Survey on IoT Attacks: Taxonomy, Detection Mechanisms and Challenges. Journal of Information and Intelligence, [online] 2(6). doi: <https://doi.org/10.1016/j.jiixd.2023.12.001>.

Sharma, A. (2022). TryHackMe — Red Teaming | Red Team Fundamentals | Part-1. [online] Medium. Available at: <https://medium.com/@ERBATMAN/tryhackme-red-teaming-red-team-fundamentals-f4e9a844cddd> [Accessed 14 Dec. 2025].

soderholmd (2024). Hybrid identity with Active Directory and Microsoft Entra ID in Azure landing zones - Cloud Adoption Framework. [online] learn.microsoft.com. Available at: <https://learn.microsoft.com/en-us/azure/cloud-adoption-framework/ready/landing-zone/design-area/identity-access-active-directory-hybrid-identity>.

Startup, I. (2025). Detection: Windows Boot or Logon Autostart Execution In Startup Folder. [online] Splunk Security Content. Available at:

<https://research.splunk.com/endpoint/99d157cb-923f-4a00-ae9-1f385412146f/> [Accessed 14 Dec. 2025].

Takyar, A. (2023). Data security in AI systems. [online] LeewayHertz - AI Development Company. Available at: <https://www.leewayhertz.com/data-security-in-ai-systems/>.

TcyberSec007 (2025). TryHackMe: Network Discovery Detection. [online] Medium. Available at: <https://medium.com/@tanwietayim.a09/tryhackme-network-discovery-detection-7700e598731a> [Accessed 14 Dec. 2025].

Appendix- Task 2 VM Work