

Assignment

by Daniel James

Submission date: 14-Jan-2026 07:20PM (UTC+0000)

Submission ID: 273301369

File name: 40166_Daniel_James_Assignment_712353_1630416001.docx (143.64K)

Word count: 6517

Character count: 42547



ETHICAL HACKING

Research into cybersecurity attacks and
penetration testing for a virtualised company
website

University of Wales Trinity Saint David
ACCA7033

Daniel James (2218766)
2218766@student.uwtsd.ac.uk

Contents

Abstract	2
1.0 Introduction	3
2.0 Background.....	5
2.1 Ransomware in Healthcare	5
2.2 Evolution of Modern Ransomware	5
2.3 MITRE ATT&CK as an Analytical Framework	6
3.0 Task 1 – Strategic Threat Analysis: Synnovis	7
3.1 Incident Overview	7
3.2 MITRE ATT&CK Mapping.....	8
3.3 Root Cause Analysis.....	10
3.4 Prevention and Detection Recommendations	11
4.0 Task 2 – Red Team Engagement.....	12
4.1 Scenario & Threat Model.....	12
4.2 Rules of Engagement.....	13
4.3 Threat Emulation Plan	13
4.4 Lab Environment Design	14
4.5 Attack Narrative	15
4.6 Detection Gap Analysis	15
4.7 Strategic Recommendations and Cost Benefit Analysis	16
5.0 Executive Brief.....	18
6.0 Conclusion	19
References	20

Abstract

Ransomware has emerged as one of the most disruptive cyber threats affecting the healthcare sector, with consequences that extend beyond technical compromise to patient safety, data protection, and organisational resilience. Modern ransomware campaigns increasingly operate as multi-stage intrusion activities, involving credential abuse, lateral movement, and data exfiltration prior to encryption. These characteristics challenge traditional security approaches that focus primarily on malware prevention rather than early-stage detection.

This report examines the 2024 ransomware attack against Synnovis, a pathology services provider supporting NHS England, as a real-world case study of modern ransomware activity. Using the MITRE ATT&CK framework, the incident is analysed to identify likely attacker behaviour, key root causes, and detection failures that would have enabled the attack to progress undetected. The analysis highlights the role of supply-chain dependencies, limited behavioural monitoring, and governance challenges in amplifying the impact of the incident.

Building on these findings, the report designs a threat-informed red team engagement to emulate realistic ransomware behaviour within a controlled environment. The engagement is used to assess detection gaps and organisational readiness across the full attack lifecycle. The findings demonstrate the value of adversary emulation in identifying weaknesses that may not be visible through traditional security testing and reinforce the importance of integrating cybersecurity into clinical and organisational management.

1.0 Introduction

The cyber threat landscape has shifted noticeably in recent years, moving away from more isolated attacks towards highly organised and persistent threats. One of the most damaging consequences of the shift has been the evolution of ransomware, which is no longer limited to encrypting files for financial gain. Instead, it commonly involves data exfiltration, service disruption, and public extortion tactics designed to maximise pressure on victim organisations. This impact is most apparent in the healthcare sector, where digital systems underpin critical services and failures can have direct consequences for patient safety [1], [2].

Healthcare organisations remain an attractive target for ransomware due to the combination of sensitive data, legacy systems, and urgency to restore services quickly. Rather than relying on a single vulnerability, modern ransomware typically progresses through a chain of well-established tactics and techniques. These often include phishing-based initial access, abuse of legitimate system tools, privilege escalation, and the use of infrastructure prior to encryption or data leakage [3]. Many of these activities are not inherently malicious in isolation, which allows the attackers to blend into normal network behaviour. In practice, this means that the failure is often not the absence of security controls, but the inability to detect attacker behaviour early enough to prevent escalation [4].

The 2024 ransomware attack against Synnovis, a pathology services provider supporting the NHS England, provides a clear example of how these weaknesses form in the real-world. The incident caused widespread disruption across multiple London hospital trusts, forcing a return to manual processes, the cancellation of procedures, and urgent appeals for blood donations. Beyond this operational impact, reports indicate that large volumes of sensitive patient and organisational data were exfiltrated and published, significantly increasing the long-term consequences of the attack [5]. This incident demonstrated how cybersecurity failures within healthcare settings can translate directly into risks to patient safety, ethical concerns around data handling, and a loss of the public's trust [6]. Articles following the attack also questioned the effectiveness of the existing cyber resilience and incident response capabilities across the NHS, suggesting that the issues could be systematic rather than isolated [7].

As attacks have become more sophisticated, offensive security practices have evolved in response. Traditional penetration testing, while valuable for identifying technical vulnerabilities, often fails to capture how real threat actors can operate over time. On the contrary, emulation and red team operations aim to address this gap by modelling attacker behaviour using structured frameworks such as the MITRE ATT&CK. This threat-informed approach focuses on replicating realistic tactics, techniques, and procedures, allowing for organisations to assess whether existing monitoring, detection, and

response capabilities are effective against credible attack scenarios rather than theoretical weaknesses [3], [4].

The assignment adopts a threat-informed offensive security approach, grounded with real-world evidence. The first part of this report provides a strategic analysis of the Synnovis NHS England ransomware attack, mapping the adversary's activity to the MITRE ATT&CK framework, identifying key root causes, and suggesting recommendations aimed at improving prevention and detection. The second part applies these insights through a simulated red team engagement against a hybrid pharmaceutical environment, emulating an advanced persistent threat actor to test organisational resilience, identify detection gaps, and assess business risk. Together, these sections demonstrate how adversary emulation can be used to support more realistic, effective, and ethically informed cybersecurity within healthcare and research environments.

2.0 Background

Ransomware represents one of the most significant cyber threats affecting organisations, with particularly severe consequences in healthcare environments. The combination of sensitive clinical data, legacy infrastructure, and the requirement for continuous service availability makes healthcare organisations more vulnerable to disruption. This section provides contextual background on ransomware in healthcare, the evolution of modern ransomware campaigns, and the relevance of behaviour-based analytical frameworks, establishing a foundation for the subsequent analysis of the Synnovis NHS England incident.

2.1 Ransomware in Healthcare

Healthcare organisations are frequently targeted by ransomware actors due to the high value of medical data and the prevalence of legacy systems that are difficult to patch or replace [1], [2]. Electronic health records, diagnostic data, and personally identifiable information offer both direct financial value and leverage for extortion, while ageing infrastructure increases the attack surface available to adversaries.

Unlike many other sectors, ransomware incidents in healthcare directly affect patient care rather than solely financial or operational outcomes. Report impacts include cancelled procedures, delayed diagnoses, and reduced access to critical services, creating strong incentives for rapid system restoration that attackers actively exploit [2]. As a result, healthcare organisations face heightened pressure during incidents, increasing both operational risk and ethical responsibility.

From a defensive perspective, detecting ransomware activity in healthcare environments remains challenging. Modern attackers frequently rely on credential abuse and legitimate administrative tools rather than overtly malicious payloads, allowing activity to blend into normal operational behaviour. Research consistently links detection failures to insufficient visibility, limited logging, and monitoring approaches that are not aligned with known attacker tactics and techniques [3], [4]. These challenges highlight the need for detection strategies that extend beyond malware prevention.

2.2 Evolution of Modern Ransomware

Contemporary ransomware operations have evolved from opportunistic attacks into carefully planned intrusion campaigns that prioritise stealth, persistence, and impact. Modern ransomware groups typically conduct extended reconnaissance, privilege escalation, and lateral movement before deploying encryption mechanisms, allowing them to identify high-value systems and exfiltrate sensitive data in advance [4].

A defining characteristic of modern ransomware is the use of double or multi-stage extortion techniques, where the attackers will not only encrypt data, but also extract sensitive and threaten to publish if ransom demands are not met. Some groups further

escalate pressure through distributed denial-of-service attacks or direct communication with the organisation's customers, partners, or regulators. Research indicates that this multi-layered extortion strategy significantly increases the likelihood of ransom payment, particularly in sectors such as healthcare where data confidentiality and service continuity is critical [4].

From a technical perspective, modern ransomware campaigns increasingly abuse legitimate system tools and built-in administrative functionality rather than relying on custom malware alone. The use PowerShell and Windows management utilities allows attackers to blend malicious activity into normal operation. This approach reduces the effectiveness of signature-based detection tools and complicates incident response, as malicious actions may appear indistinguishable from routine administrative tasks [8].

2.3 MITRE ATT&CK as an Analytical Framework

As ransomware has evolved into a multi-stage intrusion model, analytical frameworks that solely focus on individual vulnerabilities or payload execution have become insufficient. Behaviour based frameworks such as MITRE ATT&CK provide a structured method for analysing adversary activity across the full attack lifecycle, grounded in real-world observations.

MITRE ATT&CK categorises attacker behaviour into tactics, techniques, and procedures (TTPs), capturing stages including initial access, credential abuse, lateral movement, command and control, and data exfiltration. This lifecycle orientated perspective aligns closely with the behaviour of modern ransomware groups, where the most damaging activity often occurs well before encryption is deployed [4].

Both academic research and industry practice demonstrate that mapping ransomware to ATT&CK reveals consistent behavioural patterns across campaigns, supporting its use for both defensive assessment and offensive security testing [4], [8]. Its applicability to adversary emulation and detection gap analysis justifies its use as a primary analytical framework throughout this report, supporting both incident analysis in Task 1 and red team engagement in Task 2.

3.0 Task 1 – Strategic Threat Analysis: Synnovis

While the previous sections have established the broader context of ransomware in healthcare and the evolution of modern attack techniques, this section applies those concepts to a real-world incident. Task 1 presents a strategic threat analysis of the 2024 ransomware attack against Synnovis, a pathology services provider supporting NHS England. Drawing on official statements, clinical reporting, and professional commentary, the incident is examined to understand its operational impact, strategic significance, and ethical implications. This analysis provides the foundation for mapping adversary behaviour to the MITRE ATT&CK framework and identifying the factors that enabled the attack to succeed.

3.1 Incident Overview

In early June 2024, Synnovis suffered a ransomware attack that resulted in widespread disruption to healthcare operations. Synnovis is in a joint venture with NHS foundation trusts like Guy's and St Thomas' NHS Foundation Trust and King's College Hospital NHS Foundation Trust. According to the information published in Synnovis' official Cyber Attack Information Centre, the attack was detected on the 3rd of June 2024, after which affected IT systems were taken offline as a part of initial containment and response measures [9]. The operational impact of this incident was immediate and severe. The loss of access to digital pathology systems forced hospitals across south-east London to revert to manual, paper-based processes for ordering and processing diagnostic tests. NHS England confirmed that this disruption led to the postponement of outpatient appointments and elective procedures, while critical services such as blood transfusions and diagnostic testing were significantly constrained. Due to the scale of the disruption, NHS England declared a critical incident and issued urgent appeals for blood donors, highlighting the direct impact of the cyberattack on patient care rather than solely administrative systems [10], [11].

Further reporting indicated that the attackers had exfiltrated a substantial volume of data from Synnovis systems prior to the encryption. According to The BMJ stated that sensitive patient and organisational data were later published on the dark web, suggesting that the use of a double-extortion ransomware model, where data theft is used alongside encryption to increase pressure on the victim organisation [5]. BBC News described the incident as one of the most significant and harmful cyberattacks to affect the NHS, emphasising the scale of the data exposure and the potential long-term consequences for affected patients [12].

Beyond the immediate technical and clinical consequences, the attack raised broader concerns regarding cyber resilience across the NHS and its supply chain. Analysis published by The Economist questioned whether existing cybersecurity controls and incident response capabilities were sufficient, noting that the reliance of multiple NHS trusts on a single third-party pathology provider significantly amplified the downstream

impact of the attack [13]. The article suggested that the severity of the disruption reflected systematic weaknesses in healthcare cybersecurity rather than an isolated failure confined to Synnovis alone [7]. The Synnovis attack also attracted ethical and governance scrutiny due to its implications for patient safety and confidentiality. An ethics briefing published after the attack highlighted that the disruption of diagnostic services, delays to urgent care, and potential exposure of sensitive medical data challenge fundamental principles of patient trust, autonomy, and non-maleficence. The authors argued that cybersecurity incidents of this nature should be treated as patient safety events rather than purely technical failures, reinforcing the ethical responsibility of healthcare organisations to maintain robust cyber resilience [6]. Following the reports of data exfiltration, the UK National Cyber Security Centre acknowledged the incident and issued guidance reinforcing the importance of mitigating secondary harm associated with data breaches, indicating that the attack was considered significant at a national cybersecurity level [14].

Overall, the Synnovis ransomware attack illustrates how modern ransomware campaigns can exploit technical, organisational, and supply-chain dependencies to produce widespread and sustained impact. The incident also prompted discussion at a parliamentary level, with written statements acknowledging the scale of the disruption and raising concerns regarding the resilience of healthcare digital infrastructure, further emphasising the national significance of the attack [15]. The incident therefore provides a suitable case study for strategic threat analysis, as it demonstrates characteristics commonly associated with contemporary ransomware operations, including service disruption, data exfiltration, and reputational pressure. Synnovis had later reported that a forensic investigation had been completed as a part of its recovery efforts; however, limited technical details were made publicly available, restricting independent assessment of the precise attack vectors used [16]. The following section builds on this overview by mapping the adversary's likely activity to the MITRE ATT&CK framework to analyse how the attack was conducted and where defence failures occurred.

3.2 MITRE ATT&CK Mapping

Although official technical details of the initial compromise have not been publicly disclosed, existing reporting and the characteristics of the attack suggest that the initial access was likely achieved through commonly observed ransomware vectors. Academic studies identifying phishing based credential theft and exploitation of exposed remote services as the most prevalent entry points for ransomware targeting healthcare organisations [3]. These techniques align with ATT&CK tactics such as Initial Access (TA0001), particularly the techniques such as Phishing (T1566) and valid account abuse (T1078). Given the scale of the attack and the lack of immediate detection, it is plausible that attackers gained access using legitimate credentials, allowing them to operate without triggering perimeter-based alerts.

Once initial access was established, the attackers likely focused on escalating privileges and moving laterally across the network to access critical systems. Research mapping ransomware campaigns to ATT&CK consistently identified privilege escalation (TA0004) and lateral movement (TA0008) as core stages in modern ransomware operations [4]. Techniques such as credential dumping (T1003) and remote service abuse (T1021) are commonly used to expand access and compromise additional systems. In healthcare environments, where Active Directory and shared infrastructure are widely used, successful lateral movement can rapidly amplify the impact of the intrusion [1].

To maintain access and coordinate activities, modern ransomware actors frequently establish persistence mechanisms and command-and-control channels prior to executing ransomware. ATT&CK tactics such as Persistence (TA0003) and Command and Control (TA0011) are commonly associated with the abuse of scheduled tasks (T1053) and remote access tools (T1219) [3]. The use of PowerShell and Windows management utilities allows attackers to blend malicious activity into normal administrative behaviour, reducing the likelihood of detection. Behavioural analysis of ransomware incidents indicates that such techniques are a significant factor in delayed detection and prolonged attacker dwell time [4].

A defining feature of the Synnovis incident was the confirmed exfiltration and publication of sensitive data, consistent with the Exfiltration (TA0010) and Impact (TA0040) tactics within the ATT&CK framework. Clinical reporting confirmed that patient and organisational data were stolen and later published on the dark web, strongly indicating the use of a double-extortion strategy [5]. ATT&CK techniques such as exfiltration over C2 channels (T1041) or web services (T1567) are commonly associated with ransomware groups employing this model [3]. The subsequent disruption of diagnostic services and the loss of system availability align with the impact techniques including data encryption (T1486) and service disruption (T1489). The mapping of this ransomware attack to the ATT&CK framework has been summarised in Table 1 below.

ATT&CK Tactic	Technique	ATT&CK ID
Initial Access	Phishing	T1566
Initial Access	Valid Accounts	T1078
Execution	PowerShell	T1059.001
Persistence	Scheduled Task	T1053
Privilege Escalation	Credential Dumping	T1003
Defence Evasion	System Binary Proxy Execution	T1218
Lateral Movement	Remote Services	T1021
Exfiltration	Exfiltration over C2 Channel	T1041
Exfiltration	Exfiltration over Web Services	T1567

Impact	Data Encrypted	T1486
Impact	Service Stop	T1489

Table 1 maps the likely adversary behaviour observed in the Synnovis ransomware incident to the ATT&CK framework.

The Synnovis ransomware attack exhibits behaviour consistent with modern ransomware campaigns mapped in the academic literature. The likely progression from initial access through privilege escalation, lateral movement, persistence, data exfiltration, and eventual service disruption closely mirrors ATT&CK aligned ransomware models described by Raj et al. [3] and Song et al. [4]. This mapping demonstrates that the most damaging aspects of the attack occurred well before ransomware was deployed, reinforcing the importance of early-stage detection and threat-informed defensive strategies. The following sections build on this analysis by examining the root causes and detection failures that allowed the adversary to progress through these stages largely unimpeded.

3.3 Root Cause Analysis

The Synnovis ransomware attack was not caused by a single technical failure, but by a combination of detection, architectural, and governance weaknesses that enabled the adversary to progress through multiple stages of the attack lifecycle. When viewed alongside established ransomware behaviour, the incident reflects broader challenges commonly observed in healthcare environments rather than an isolated anomaly. A key root cause was the apparent failure to detect malicious activity during the early stages of the intrusion. The confirmed exfiltration of sensitive data prior to service disruption strongly suggests that attacker behaviour went unnoticed for an extended period, indicating gaps in behavioural monitoring and ATT&CK-aligned detection.

Structural dependencies within the NHS pathology supply chain further amplified the impact of the attack. The compromise of a single third-party provider resulted in widespread disruption across multiple NHS trusts, highlighting insufficient resilience planning for supply-chain failure scenarios. This concentration of risk reflects an architectural and governance weakness rather than a purely technical shortcoming. Finally, organisational constraints common in healthcare, including legacy systems and competing operational priorities, likely reduced the effectiveness of preventative controls and incident response [1], [2]. Ethical analysis also indicated that cybersecurity incidents of this nature should be treated as patient safety events, reinforcing the need to integrate cybersecurity risk into clinical governance frameworks [6]. The Information Commissioner's Office also confirmed that it was making enquiries into the incident, highlighting the regulatory and data protection implications of the breach and reinforcing the importance of lawful handling of sensitive medical data within healthcare organisations [17].

3.4 Prevention and Detection Recommendations

This analysis of the Synnovis ransomware attack demonstrates the need for prevention and detection strategies that reflect modern attacker behaviour rather than reliance on isolated technical controls. Existing NHS England cybersecurity guidance emphasises the importance of resilience, incident preparedness, and third-party risk management; however, the scale of disruption observed in the Synnovis incident suggests a gap between policy guidance and practical implementation across complex healthcare supply chains [18]. The following recommendations directly address the root causes identified in Section 3.3 and are supported by current ransomware and healthcare cybersecurity research.

Firstly, organisations should prioritise early-stage, behaviour-based detection aligned with attacker tactics and techniques. Aligning logging and alerting capabilities with frameworks such as MITRE ATT&CK enables improved visibility across the attack lifecycle and supports earlier intervention. Secondly, supply-chain resilience must be strengthened to mitigate the systematic risk posed by third-party service providers. The Synnovis incident illustrated how the compromise of a single pathology provider could disrupt multiple NHS trusts simultaneously, highlighting the need for improved third-party risk management and architectural segmentation.

Cybersecurity should also be embedded within clinical governance and patient safety frameworks rather than treated solely as technical or compliance issues. Ransomware incidents in healthcare directly affect patient outcomes and ethical obligations, reinforcing the need to integrate cybersecurity risk into organisational decision-making and incident response planning. Finally, regular adversary emulation and incident response testing should be conducted to validate detection and response capabilities against realistic ransomware scenarios. Threat-informed red team exercises support continuous improvement and help ensure defensive controls remain effective against evolving threats.

Together, these recommendations emphasise a proactive and threat-informed approach to ransomware defence that addresses both technical and organisational vulnerabilities within a healthcare environment.

4.0 Task 2 – Red Team Engagement

While Task 1 focused on analysing a real-world ransomware incident and identifying the factors that enabled the attack to succeed Task 2 applies these findings through the design of a threat-informed red team engagement. The purpose of this task is not to conduct a live attack, but to demonstrate how realistic adversary behaviour could be emulated in a controlled environment to assess organisational resilience, detection capability, and response effectiveness. Drawing directly on the tactics, techniques, and failures identified in the Synnovis NHS England ransomware attack, this section outlines a structured red team exercise aligned with modern ransomware operations and the MITRE ATT&CK framework. The engagement is designed to be ethically grounded, realistic, and focused on generating actionable insights rather than purely technical outcomes.

4.1 Scenario & Threat Model

The red team engagement is based on a hybrid pharmaceutical and healthcare research organisation that provides diagnostic services, clinical research support, and data processing for multiple external healthcare partners. This type of organisation was selected as it closely reflects the operational characteristics of observed in the Synnovis NHS England ransomware incident, including reliance on shared digital infrastructure, centralised service delivery, and the handling of sensitive medical and research data. As demonstrated in Task 1, such environments present attractive targets for financially motivated ransomware groups due to the potential for high operational impact and extortion leverage.

The assumed threat actor is a financially motivated ransomware group operating using a targeted intrusion model rather than opportunistic attacks. The adversary is expected to prioritise stealth, persistence, and reconnaissance, with the objective of maximising disruption and data exposure prior to ransomware deployment. This behaviour reflects patterns observed in modern ransomware campaigns analysed earlier in the assignment and provides a realistic basis for emulation.

Adversary behaviour within the scenario is modelled using the MITRE ATT&CK framework to ensure consistency with observed real-world attack techniques. The threat actor is assumed to exploit commonly abused techniques such as phishing based initial access, credential abuse, lateral movement within an Active Directory environment, and the misuse of legitimate administrative tools. These techniques were selected to test detection and response capabilities across multiple stages of the attack lifecycle rather than focusing solely on the final ransomware payload.

Overall, the scenario and threat model are designed to balance realism with the ethical and operational constraints, enabling meaningful assessment of organisational

resilience while remaining suitable for execution within a controlled laboratory environment.

4.2 Rules of Engagement

The red team engagement is conducted within a controlled laboratory environment to ensure that testing activity does not pose a risk to real patients, live services, or sensitive data. The scope of the engagement is limited to a simulated corporate network representing the target organisation's internal environment, including user workstations, an Active Directory domain, and internal servers used for file storage and research data processing. External-facing production systems, live clinical systems, and any systems containing real patient data are explicitly excluded from scope.

The testing activity is time-bound and conducted under predefined constraints to minimise disruption and maintain ethical oversight. Actions that could result in irreversible data loss, service disruption, or harm to individuals are prohibited. Therefore, the ransomware deployment is simulated rather than executed, with the impact assessed through controlled indicators such as access denial or simulated encryption events.

Finally, credential harvesting, lateral movement, and data exfiltration techniques are permitted only within the confines of the laboratory environment and for the purpose of evaluating detection and response capabilities. All activity is logged, and testing is conducted with the assumption that defensive monitoring is active throughout the engagement. These rules ensure that the exercise remains realistic while maintaining professional, ethical, and operational safeguards appropriate to healthcare-adjacent environment.

4.3 Threat Emulation Plan

The threat emulation plan is designed to replicate the behaviour of modern ransomware threat actors rather than focusing on a specific tool or exploit. The objective of the engagement is to assess whether defensive controls can detect and respond to realistic attacker activity across multiple stages of the intrusion lifecycle, informed by the behaviour observed in the Synnovis ransomware attack. Adversary activity is modelled using the MITRE ATT&CK framework, ensuring that selected techniques reflect real-world ransomware operations.

Initial access is assumed to occur through a phishing-based compromise or abuse of a valid account, representing one of the most common entry points for ransomware campaigns targeting healthcare and adjacent environments. This phase is intended to test the organisation's ability to detect anomalous authentication activity and suspicious user behaviour rather than perimeter exploitation alone. Following on from initial access, the threat actor is expected to perform a privilege escalation and lateral movement within the Active Directory environment. Techniques such as credential

harvesting, access to network shares, and movement via remote services are emulated to assess visibility across internal authentication flows. This stage reflects the reconnaissance and expansion phase commonly observed prior to ransomware deployment.

To maintain access and coordinate activity, the plan includes persistence and command-and-control behaviour through the misuse of legitimate administrative functionality. Emphasis is placed on techniques that blend into normal operational activity, testing whether behavioural monitoring can distinguish malicious use of systems tools from legitimate administration. Finally, the emulation includes data discovery and simulated exfiltration, followed by a controlled representation of an impact. Ransomware execution is not performed; instead, impact is assessed through simulated access denial and exfiltration indicators to evaluate detection, escalation, and response decision making without introducing risk.

Overall, this threat emulation plan prioritises realism, safety, and alignment with observed ransomware behaviour, enabling meaningful assessment of detection and response capabilities across the full attack lifecycle.

4.4 Lab Environment Design

The red team engagement is conducted within a simulated laboratory environment designed to reflect the core components of a typical healthcare corporate network while avoiding the risks associated with testing against live systems. The lab environment includes a small Active Directory domain, representative user workstations, and internal servers providing file storage and research data services. This configuration mirrors common enterprise architectures used within healthcare and pharmaceutical organisations and supports realistic emulation of attacker behaviour observed in modern ransomware campaigns.

The environment is intentionally designed to be a simplified version of the network to focus on detection and response evaluation rather than infrastructure complexity. Centralised authentication, shared network resources, and standard administrative workflows are included to enable testing of credential abuse, lateral movement, and privilege escalation techniques. Logging and monitoring are assumed to be enabled across endpoints, authentication services, and network traffic to support analysis of detection coverage throughout the engagement.

To maintain ethical and operational safety, the lab does not contain real patient data or production services. All ransomware activity is simulated, and any destructive actions are represented through controlled indicators rather than actual data encryption or service disruption. While the environment does not replicate the full scale of a production healthcare network, it provides sufficient fidelity to evaluate how effectively

defensive controls detect and respond to realistic attacker behaviour across multiple stages of the intrusion lifecycle.

4.5 Attack Narrative

The attack narrative describes the progression of the emulated ransomware from the perspective of the threat actor, based on the techniques outlined in the threat emulation plan. The scenario begins with the compromise of a user account through a phishing-based credential theft, providing the attacker with an initial foothold within the internal network. At this stage, the attacker operates using legitimate credentials, allowing early activity to blend into normal user behaviour and reducing the likelihood of immediate detection. Following from the initial access, the attacker conducts internal reconnaissance to identify accessible systems, network shares, and privileged accounts. This phase includes attempts to escalate privileges and move laterally within the Active Directory environment by leveraging shared credentials and remote access mechanisms. The objective is to expand access while maintaining a low operational profile, reflecting the reconnaissance and preparation stages commonly observed in modern ransomware campaigns.

Once sufficient access has been established, the attacker focuses on persistence and coordination. Legitimate administrative tools are abused to maintain access and facilitate command-and-control activity, allowing the attacker to operate over an extended period without relying on overtly malicious code. During this phase, sensitive files located on the internal servers are identified, and simulated data exfiltration activity is performed to represent preparation for double extortion. The final stage of the narrative represents the impact phase of the attack. Rather than deploying live ransomware impact is simulated through controlled indicators such as restricted access to key resources and simulated encryption events. This approach enabled evaluation of detection, escalation, and response decision-making without causing irreversible damage. The narrative demonstrates how cumulative low-level activity can ultimately result in significant operational disruption if not detected early.

4.6 Detection Gap Analysis

The emulated attack narrative highlights several points at which attacker activity should reasonably have been detected but may have gone unnoticed due to limitations in monitoring, alerting, or response processes. These detection gaps reflect challenges commonly observed in modern ransomware incidents, including those identified during the analysis of the Synnovis NHS England attack in Task 1. The first significant detection gap occurs during initial access and early credential abuse. The use of valid credentials obtained through phishing allows the attacker to bypass many traditional perimeter controls. When monitoring is only limited to malware signatures or external intrusion attempts anomalous authentication attempts such as unusual login times, unfamiliar locations, or abnormal access patterns may not trigger alerts.

A second gap emerges during the lateral movement and internal reconnaissance. As the attack expands access within the Active Directory environment, repeated authentication attempts, access to shared resources, and movement between hosts should present opportunities for detection. However, if east to west traffic and internal authentication events are insufficiently monitored, these activities can blend into normal administrative behaviour, delaying response until later stages of the attack. The persistence and data exfiltration phases further expose detection weaknesses. The abuse of legitimate administrative tools and simulated exfiltration activity may not be flagged if logging is incomplete or if alerts are not mapped to meaningful attack indicators. This enables attackers to prepare for impact while remaining undetected.

Overall, the detection gaps identified emphasise the need for monitoring strategies aligned with attacker behaviour across the full intrusion lifecycle, rather than focusing solely on the final ransomware deployment. Addressing these gaps is critical to enabling earlier intervention and reducing the operational and clinical impact of the ransomware attacks.

4.7 Strategic Recommendations and Cost Benefit Analysis

The detection gaps identified during the red team engagement indicate the need for proportionate improvements that prioritise early-stage detection and organisational resilience. The following recommendations are directly aligned with the attacker behaviour emulated in Task 2 and the root causes identified in Task 1.

First, organisations should enhance behaviour-based monitoring of authentication events, privilege escalation, and lateral movement. These activities occur early in the attack lifecycle and offer high defensive value if detected properly. While improved logging and correlation may require moderate investment, the benefit of earlier intervention significantly outweighs the associated costs by reducing operational disruption and data exposure. Secondly, network segmentation and least-privilege access controls should be strengthened to limit the impact of credential compromise. These measures typically involve low-to-moderate implementation effort while providing substantial risk reduction in environments with shared infrastructure.

Finally, organisations should conduct regular threat testing including adversary emulation and incident response exercises, to validate detection capabilities and improve response coordination. Cybersecurity risks should also be integrated into the organisational and clinical governance frameworks to ensure appropriate oversight and accountability. These actions involve minimal financial cost but deliver significant long-term benefits in preparedness and resilience.

Table 2 demonstrates indicative costs for the recommended security controls which have been derived from publicly available industry benchmarks and national security guidance. Industry studies consistently demonstrate that healthcare cyber incidents

frequently result in multi-million-pound impacts once operational disruption, regulatory exposure, and reputational damages are considered [19]. UK national guidance similarly emphasises that investment into proactive detection and resilience measures is significantly more cost-effective than post-incident recovery [18]. In healthcare environments, the cost of cybersecurity failures extends beyond financial loss to include patient harm and ethical liabilities. This reinforces the justification for proactive investment in detection and resilience.

Security Improvement	Indicative Cost	Expected Risk Reduction
Behaviour based EDR tuning	£20 - £40 per endpoint / year	Earlier detection of credential abuse and lateral movement
SIEM log correlation and alerting	£15k - £30k / year	Improved visibility of multi-stage attacks
Network segmentation and least privilege	£10k - £25k	Reduced lateral movement and blast radius
Adversary emulation exercises	£5k - £15k annually	Identification of detection gaps
Governance & incident playbooks	Low direct cost	Faster, coordinated incident response

Table 2: Indicative cost-benefit comparison of recommended security controls.

5.0 Executive Brief

Recent ransomware attacks within the UK healthcare sector demonstrate a credible and immediate risk to patient safety, regulatory compliance, and service continuity. The 2024 Synnovis incident highlights how the compromise of a single third-party provider can result in widespread clinical disruption and reputational harm across multiple organisations. If similar weaknesses remain unaddressed, comparable organisations face a high likelihood of prolonged service disruption, regulatory investigations, financial loss, and loss of public trust. In healthcare environments, these impacts extend beyond operational inconvenience to include direct risks to patient outcomes and ethical responsibility. The recommended security improvements represent a proportionate and cost-effective investment when compared with the potential financial, clinical, and reputational consequences of a major ransomware incident.

This report examined the Synnovis incident to identify how modern ransomware attacks progress through multiple stages prior to deployment and why existing controls fail to detect attacker activity early. Using a threat-informed approach grounded in the MITRE ATT&CK framework, the analysis demonstrated that the most damaging phases of ransomware attacks typically occur during credential abuse, lateral movement, and data exfiltration, rather than at the point of encryption itself.

To apply these findings, a simulated red team engagement was designed to emulate realistic ransomware behaviour within a controlled laboratory environment. The engagement focused on testing detection and response capabilities across the full attack lifecycle while maintaining ethical and operational safeguards appropriate to healthcare systems. Analysis of the simulated attack highlighted key detection gaps during early-stage intrusion activity and internal network movement.

Based on these findings, the report recommends prioritising behaviour-based monitoring, strengthening segmentation and access controls, and integrating cybersecurity risk into organisational and clinical governance frameworks. Collectively, these actions provide a cost-effective means of reducing the likelihood and impact of ransomware incidents while supporting patient safety and operational continuity.

6.0 Conclusion

This report examined the evolving nature of ransomware within the healthcare sector, using the 2024 Synnovis NHS England attack as a case study to analyse how modern ransomware campaigns operate and why they remain difficult to detect. Through a strategic threat analysis grounded in the MITRE ATT&CK framework, the report demonstrated that contemporary ransomware attacks are multi-staged in nature, with the most damaging activity often occurring during early phases such as credential abuse, lateral movement, and data exfiltration, rather than at the point of ransomware deployment itself.

The analysis identified that the impact of the Synnovis incident was driven by a combination of limited early-stage detection, structural dependencies within the healthcare supply chain, and the governance challenges common to complex healthcare environments. These factors enabled the attackers to operate undetected for an extended period and amplified the downstream consequences once systems were taken offline. Building on these findings, a threat informed red team engagement was designed to demonstrate how realistic adversary emulation can be used to assess detection capability, identify defensive gaps, and evaluate organisational readiness in a controlled and ethical manner.

Importantly, subsequent reporting indicated that disruption associated with the Synnovis ransomware attack may have contributed to a patient's death [20]. This underscores that cybersecurity incidents in healthcare can have direct clinical consequences rather than purely technical or financial impact. Collectively, the findings reinforce the need to treat cybersecurity as an integral component of patient safety, clinical governance, and organisational resilience, supported by proactive, behaviour-based detection and regular threat informed testing.

References

- [1] G. Kirubavathi, W. Regis Anne, and U. K. Sridevi, 'A recent review of ransomware attacks on healthcare industries', *Int J Syst Assur Eng Manag*, vol. 15, no. 11, pp. 5078–5096, Nov. 2024, doi: 10.1007/s13198-024-02496-4.
- [2] A. Shahzadi *et al.*, 'Safeguarding the healthcare sector from ransomware attacks: insights from a literature review', *PeerJ Computer Science*, vol. 11, p. e3073, Oct. 2025, doi: 10.7717/peerj-cs.3073.
- [3] A. Raj, V. Narayan, V. Muskan, A. Sani, P. Sharma, and S. S. Sarma, 'Modern ransomware: Evolution, methodology, attack model, prevention and mitigation using multi-tiered approach', *Security and Privacy*, vol. 7, no. 6, p. e436, Nov. 2024, doi: 10.1002/spy2.436.
- [4] Z. Song, Y. Tian, and J. Zhang, 'Similarity Analysis of Ransomware Attacks Based on ATT&CK Matrix', *IEEE Access*, vol. 11, pp. 111378–111388, 2023, doi: 10.1109/ACCESS.2023.3322427.
- [5] I. Torjesen, 'NHS cyberattack: Data allegedly stolen from pathology lab published on dark web', *BMJ*, p. q1389, Jun. 2024, doi: 10.1136/bmj.q1389.
- [6] R. S. Berg and N. Michaux, 'Ethics briefing', *Journal of Medical Ethics*, vol. 50, no. 8, pp. 581–582, Aug. 2024, doi: 10.1136/jme-2024-110214.
- [7] 'Another wake-up call', *The Economist*, vol. 451, no. 9401, The Economist Intelligence Unit N.A., Incorporated, London, United Kingdom, p. 22, Jun. 15, 2024.
- [8] 'Britain's NHS reels from a ransomware attack', *The Economist (Online)*, The Economist Intelligence Unit N.A., Incorporated, London, United Kingdom, Jun. 13, 2024. Accessed: Jan. 12, 2026. [Online]. Available: <https://www.proquest.com/docview/3067293543/abstract/6F4FCAB52A6044D5PQ/1>
- [9] 'Cyber Attack Information Centre', Synnovis. Accessed: Jan. 12, 2026. [Online]. Available: <https://www.synnovis.co.uk/cyberattack-information-centre>
- [10] N. H. S. England, 'NHS England » Synnovis cyber incident'. Accessed: Jan. 12, 2026. [Online]. Available: <https://www.england.nhs.uk/synnovis-cyber-incident/>
- [11] N. E.- London, 'NHS England — London » Synnovis Ransomware Cyber-Attack'. Accessed: Jan. 12, 2026. [Online]. Available: <https://www.england.nhs.uk/london/synnovis-ransomware-cyber-attack/>
- [12] J. T. C. Correspondent and B. W. Service, 'London hospitals hackers publish stolen blood test data', BBC News. Accessed: Jan. 12, 2026. [Online]. Available: <https://www.bbc.co.uk/news/articles/c9ww90j9dj8o>
- [13] K. Welsh, 'Synnovis cyber-attack update', King's College Hospital NHS Foundation Trust. Accessed: Jan. 12, 2026. [Online]. Available: <https://www.kch.nhs.uk/news/synnovis-cyber-attack-update/>
- [14] 'NCSC statement following reports of a Synnovis data breach'. Accessed: Jan. 12, 2026. [Online]. Available: <https://www.ncsc.gov.uk/news/ncsc-statement-following-reports-of-a-synnovis-data-breach>
- [15] 'Written statements - Written questions, answers and statements - UK Parliament'. Accessed: Jan. 12, 2026. [Online]. Available: <https://questions-statements.parliament.uk/written-statements/detail/2025-11-12/hcws1046>
- [16] 'Synnovis completes forensic review following 2024 cyberattack — notifications under way', Synnovis. Accessed: Jan. 12, 2026. [Online]. Available:

<https://www.synnovis.co.uk/news-and-press/synnovis-completes-forensic-review-following-2024-cyberattack>

- [17] 'Statement in response to Synnovis cyber attack'. Accessed: Jan. 12, 2026. [Online]. Available: <https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2024/06/statement-in-response-to-synnovis-cyber-attack/>
- [18] N. H. S. England, 'NHS England » Cyber Security'. Accessed: Jan. 12, 2026. [Online]. Available: <https://www.england.nhs.uk/long-read/cyber-security/>
- [19] 'IBM: Cost of a Data Breach Report', *Computer Fraud & Security*, vol. 2021, no. 8, pp. 4–4, Jan. 2021, doi: 10.1016/S1361-3723(21)00082-8.
- [20] J. W. B. News, 'NHS ransomware attack contributed to patient's death', BBC News. Accessed: Jan. 12, 2026. [Online]. Available: <https://www.bbc.co.uk/news/articles/cp3ly4v2kp2o>

Assignment

GRADEMARK REPORT

FINAL GRADE

GENERAL COMMENTS

71 /100

PAGE 1

PAGE 2

PAGE 3

PAGE 4

PAGE 5

PAGE 6

PAGE 7

PAGE 8

PAGE 9

PAGE 10

PAGE 11

PAGE 12

PAGE 13

PAGE 14

PAGE 15

PAGE 16

GRADING FORM: L7 - (ETHICAL HACKING)

DANIEL JAMES

70.50

ENGAGEMENT WITH LIT (15)

Engagement with Literature Skills



Excellent, current academic and industry sources, well integrated and correctly referenced in IEEE style.

14

KNOWLEDGE & UNDERSTANDING (10)

Knowledge and Understanding Skills



Very strong conceptual understanding of ransomware, healthcare risk, and threat-informed defence.

9

COGNITIVE & INTELLECTUAL (40)

Cognitive and Intellectual Skills



Strong critical analysis and ethical reflection, particularly in Task 1. Task 2 shows good reasoning but less depth in detection gap critique.

30

PRACTICAL APPLICATION (30)

Practical Application Skills



Major weakness — limited practical execution. Task 2 lacks lab evidence, commands, or realistic attacker workflow.

14

TRANSFERABLE SKILLS (5)

Transferable Skills for Life and Professional Practice



Professional writing, cover page present, IEEE referencing used. Paragraphs not fully justified.

3.5